MEĐUNARODNI NAUČNI SKUP „DANI ARČIBALDA RAJSA“
TEMATSKI ZBORNIK RADOVA MEĐUNARODNOG ZNAČAJA

INTERNATIONAL SCIENTIFIC CONFERENCE “ARCHIBALD REISS DAYS”
THEMATIC CONFERENCE PROCEEDINGS OF INTERNATIONAL SIGNIFICANCE

MEĐUNARODNI NAUČNI SKUP
INTERNATIONAL SCIENTIFIC CONFERENCE

„DANI ARČIBALDA RAJSA“

“ARCHIBALD REISS DAYS”

Beograd, 10-11. mart 2016.
Belgrade, 10-11 March 2016

TEMATSKI ZBORNIK RADOVA
MEĐUNARODNOG ZNAČAJA

THEMATIC CONFERENCE PROCEEDINGS
OF INTERNATIONAL SIGNIFICANCE

TOM III
VOLUME III

KRIMINALISTIČKO-POLICIJSKA AKADEMIJA
Beograd, 2016
ACADEMY OF CRIMINALISTIC AND POLICE STUDIES
Belgrade, 2016

Publisher
ACADEMY OF CRIMINALISTIC AND POLICE STUDIES
Belgrade, 196 Cara Dušana Street (Zemun)

Editor-in-Chief
DRAGANA KOLARIĆ, PhD
Academy of Criminalistic and Police Studies

Editors
ĐORĐE ĐORĐEVIĆ, PhD, Academy of Criminalistic and Police Studies
MILAN ŽARKOVIĆ, PhD, Academy of Criminalistic and Police Studies
DRAGAN RANĐELOVIĆ, PhD, Academy of Criminalistic and Police Studies
BOBAN MILOJKOVIĆ, PhD, Academy of Criminalistic and Police Studies
DANE SUBOŠIĆ, PhD, Academy of Criminalistic and Police Studies
SAŠA MIJALKOVIĆ, PhD, Academy of Criminalistic and Police Studies
OBRAD STEVANOVIĆ, PhD, Academy of Criminalistic and Police Studies
ZORAN ĐURĐEVIĆ, PhD, Academy of Criminalistic and Police Studies
TIJANA ŠURLAN, PhD, Academy of Criminalistic and Police Studies
NIKOLA MILAŠINOVIĆ, PhD, Academy of Criminalistic and Police Studies
DRAGOSLAVA MIĆOVIĆ, PhD, Academy of Criminalistic and Police Studies

Thematic Proceedings Reviewers
Full Professor OLIVIER RIBAUX, PhD
School of Criminal Justice, Faculty of Law, Criminal Justice and Public Administration,
University of Lausanne, Switzerland
Associate Professor GABOR KOVACS, PhD
Faculty of Law Enforcement, National University of Public Service, Hungary
Full Professor JOZEF METENKO, LLD
Academy of Police Force in Bratislava, Slovakia
Associate Professor SNEŽANA MOJSOSKA, PhD
Faculty of Security, University "St. Climent Ohridski", Macedonia
Associate Professor GEORGICĂ PANFIL, PhD
"Alexandru Ioan Cuza" Police Academy, Romania

Impression
200 copies

Print
PEKOGRAF, Belgrade

THE CONFERENCE AND THE PUBLISHING OF PROCEEDINGS
WERE SUPPORTED BY THE MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF SERBIA

© 2016 Academy of Criminalistic and Police Studies, Belgrade

ISBN 978-86-7020-358-7
ISBN 978-86-7020-190-3

Izdavač
KRIMINALISTIČKO-POLICIJSKA AKADEMIJA
Beograd, Cara Dušana 196 (Zemun)

Glavni i odgovorni urednik
prof. dr DRAGANA KOLARIĆ
Kriminalističko-policijska akademija

Urednici
prof. dr ĐORĐE ĐORĐEVIĆ, Kriminalističko-policijska akademija
prof. dr MILAN ŽARKOVIĆ, Kriminalističko-policijska akademija
prof. dr DRAGAN RANĐELOVIĆ, Kriminalističko-policijska akademija
prof. dr BOBAN MILOJKOVIĆ, Kriminalističko-policijska akademija
prof. dr DANE SUBOŠIĆ, Kriminalističko-policijska akademija
prof. dr SAŠA MIJALKOVIĆ, Kriminalističko-policijska akademija
prof. dr OBRAD STEVANOVIĆ, Kriminalističko-policijska akademija
prof. dr ZORAN ĐURĐEVIĆ, Kriminalističko-policijska akademija
prof. dr TIJANA ŠURLAN, Kriminalističko-policijska akademija
doc. dr NIKOLA MILAŠINOVIĆ, Kriminalističko-policijska akademija
doc. dr DRAGOSLAVA MIĆOVIĆ, Kriminalističko-policijska akademija

Recenzenti Zbornika radova
prof. dr OLIVIJE RIBO
Univerzitet u Lozani, Švajcarska
prof. dr GABOR KOVAČ
Policijska akademija, Nacionalni univerzitet za javnu službu, Mađarska
prof. dr JOZEF METENKO
Policijska akademija, Bratislava, Slovačka
prof. dr SNEŽANA MOJSOSKA
Fakultet bezbednosti, Univerzitet "Sv. Kliment Ohridski", Makedonija
prof. dr George Panfil
Policijska akademija "Aleksandru Joan Kuza"

Tiraž
200 primeraka

Štampa
PEKOGRAF, Beograd

ODRŽAVANJE SKUPA I ŠTAMPANJE OVOG ZBORNIKA PODRŽALO JE
MINISTARSTVO PROSVETE, NAUKE I TEHNOLOŠKOG RAZVOJA
REPUBLIKE SRBIJE

© 2016 Kriminalističko-policijska akademija, Beograd

ISBN 978-86-7020-358-7
ISBN 978-86-7020-190-3

INTERNATIONAL SCIENTIFIC CONFERENCE
"ARCHIBALD REISS DAYS"

THE HONORARY COMMITTEE

Mladen Bajagić, PhD, Acting Dean of the Academy of Criminalistic and Police Studies, President
Dragana Kolarić, LLD, Acting Vice Dean of the Academy of Criminalistic and Police Studies
Tijana Šurlan, LLD, Acting Vice Dean of the Academy of Criminalistic and Police Studies
Sima Avramović, LLD, Dean of the Faculty of Law, Belgrade
Zoran Stojanović, LLD, Full Professor, Faculty of Law, Belgrade
Ivica Radović, PhD, Dean of the Faculty of Security, Belgrade
Major-General **Goran Zeković**, Spec., Head of the Military Academy, Belgrade
Ambassador **Ljiljana Nikšić**, PhD, Head of the Department for Migration Policy and Diaspora, Ministry of Foreign Affairs of the Republic of Serbia
Academician **Dragoljub Živojinović**, Serbian Academy of Sciences and Arts
Jovan Ćirić, PhD, Director of the Institute of Comparative Law, Belgrade
Branislav Đorđević, PhD, Director of the Institute of International Politics and Economics, Belgrade
Momčilo Pavlović, PhD, Director of the Institute for Contemporary History, Belgrade

International members

Zvonimir Jovanović, President of the Serbian-Swiss Friendship Association "Dr. Archibald Reiss"
Olivier Ribaux, PhD, Director of the School of Criminal Justice, University of Laussane, Switzerland
Marcelo Aebi, PhD, Deputy Director of the School of Criminal Justice, University of Laussane, Switzerland
Barry Lituchy, PhD, University of California, Berkeley, Director of the Jasenovac Research Institute, USA
Wang Shiquan, PhD, President of the National Police University of China
Vladimir Tretyakov, LLD, Chief of the Volgograd Academy of the Russian Internal Affairs Ministry
José García Molina, PhD, Director of the National Police Academy, Ávila, Spain
Major Knut Thoresen, Researcher of the „Simon Wiesenthal" Centre, Norway
Hélène Martini, PhD, Director of the France's National Police College and President of the Association of European Police Colleges
Norbert Leitner, PhD, Vice President of the Association of European Police Colleges and Director of SIAK, Vienna, Austria
Major-General **Valeriy Vyacheslavovich Sereda**, LLD, Rector of the Lviv State University of Internal Affairs, Ukraine
Major-general **Vladimir Bachila**, LLD, Head of the Academy of the Interior Ministry of the Republic of Belarus
Gheorghe Popa, PhD, Rector of the Police Academy "Alexandru Ioan Cuza", Bucharest, Romania
Simon Carp, PhD, Rector of the Academy "Stefan cel Mare", Ministry of Interior of the Republic of Moldova
Piotr Bogdalski, LLD, Commandant-Rector of the Police Academy, Szczytno, Poland
Lucia Kurilovská, PhD, Rector of the Academy of Police Force, Bratislava, Slovakia
Jozef Meteňko, PhD, Academy of Police Force, Bratislava, Slovakia
Milorad Kojić, PhD, Centre for the Investigation of War, War Crimes and the Search for Missing Persons, Republika of Srpska
Duško Pena, MA, Director of the Police College, Republic of Srpska
Mile Šikman, PhD, MoI of the Republic of Srpska
Count Philippe Piccapietra, Honourable President of the the Serbian-Swiss Friendship Association "Dr. Archibald Reiss", Switzerland
Nedžad Korajlić, PhD, Dean of the Faculty for Criminal Justice, Criminology and Security Studies, University of Sarajevo, Bosnia and Herzegovina
Zoltán Rajnai, PhD, Bánki Donát Faculty, Óbuda University, Hungary
Andrej Sotlar, PhD, Dean of the Faculty of Criminal Justice and Security, Ljubljana, University of Maribor, Slovenia
Ivan Toth, PhD, Dean of the University of Applied Sciences Velika Gorica, Croatia
Oliver Bačanović, PhD, Dean of the Faculty of Security, Skopje, Macedonia
Dragan Radonjić, LLD, Dean of the Faculty of Law, Podgorica, Montenegro
Milica Pajović, Dean of the Police Academy, Danilovgrad, Montenegro

THE PROGRAMME COMMITTEE

Đorđe Đorđević, PhD, Academy of Criminalistic and Police Studies, President
Milan Žarković, PhD, Academy of Criminalistic and Police Studies
Dragan Ranđelović, PhD, Academy of Criminalistic and Police Studies
Boban Milojković, PhD, Academy of Criminalistic and Police Studies
Dane Subošić, PhD, Academy of Criminalistic and Police Studies
Saša Mijalković, PhD, Academy of Criminalistic and Police Studies
Obrad Stevanović, PhD, Academy of Criminalistic and Police Studies
Zoran Đurđević, PhD, Academy of Criminalistic and Police Studies
Nikola Milašinović, PhD, Academy of Criminalistic and Police Studies
Dragoslava Mićović, PhD, Academy of Criminalistic and Police Studies

MEĐUNARODNI NAUČNI SKUP
„DANI ARČIBALDA RAJSA"

POČASNI ODBOR

prof. dr **Mladen Bajagić**, v. d. dekana Kriminalističko-policijske akademije, predsednik
prof. dr **Dragana Kolarić**, v. d. prodekana Kriminalističko-policijske akademije
prof. dr **Tijana Šurlan**, v. d. prodekana Kriminalističko-policijske akademije
prof. dr **Sima Avramović**, dekan Pravnog fakulteta, Beograd
prof. dr **Zoran Stojanović**, redovni profesor Pravnog fakulteta, Beograd
prof. dr **Ivica Radović**, dekan Fakulteta bezbednosti, Beograd
general-major spec. **Goran Zeković**, načelnik Vojne akademije, Beograd
ambasador dr **Ljiljana Nikšić**, načelnik Odeljenja za migracionu politiku, dijasporu, socijalne sporazume i kulturu sećanja, Ministarstvo spoljnih poslova
akademik **Dragoljub Živojinović**, Srpska akademija nauka i umetnosti
dr **Jovan Ćirić**, direktor Instituta za uporedno pravo, Beograd
prof. dr **Branislav Đorđević**, direktor Instituta za međunarodnu politiku i privredu, Beograd
dr **Momčilo Pavlović**, direktor Instituta za savremenu istoriju, Beograd

Članovi iz inostranstva

Zvonimir Jovanović, predsednik Društva srpsko-švajcarskog prijateljstva „Dr Arčibald Rajs"
prof. dr **Olivier Ribaux**, direktor Fakulteta za kriminalistiku, Univerzitet u Lozani, Švajcarska
prof. dr **Marcelo Aebi**, zamenik direktora Instituta za kriminologiju, Lozana, Švajcarska
prof. dr **Barry Lituchy**, Univerzitet Berkli, direktor Institut za istraživanje zločina u Jasenovcu, SAD
prof. dr **Wang Shiquan**, predsednik Nacionalnog policijskog univerziteta Kine
prof. dr **Vladimir Tretjakov**, načelnik Volgogradske akademije Ministarstva unutrašnjih poslova Rusije
prof. dr José **García Molina**, direktor Nacionalne policijske akademije, Ávila, Španija
major **Knut Thoresen**, istraživač Centra „Simon Vizental", Norveška
Hélène Martini, predsednica Asocijacije evropskih policijskih koledža i direktorka Francuskog nacionalnog policijskog koledža
dr **Norbert Leitner**, potpredsednik Asocijacije evropskih policijskih koledža i direktor SIAK Policijske akademije, Beč, Austrija
general-major prof. dr **Valerij Vjačeslavovič Sereda**, rektor Državnog univerziteta unutrašnjih poslova, Lavov, Ukrajina
general-major doc. dr **Vladimir Bačila**, načelnik Akademije MUP R. Belorusije
prof. dr **Gheorghe Popa**, rektor Policijske akademije „Alexandru Ioan Cuza", Bukurešt, Rumunija
prof. dr **Simon Carp**, rektor Akademije "Stefan cel Mare", MUP R. Moldavije
prof. dr **Piotr Bogdalski**, komandant-rektor Policijske akademije, Ščitno, Poljska
doc. dr **Lucia Kurilovská**, rektor Policijske akademije, Bratislava, Slovačka
prof. dr **Jozef Meteňko**, Policijska akademija, Bratislava, Slovačka
dr **Milorad Kojić**, Republički centar za ratne zločine, Banja Luka, R. Srpska
mr **Duško Pena**, direktor Visoke škole unutrašnjih poslova, Republika Srpska
dr **Mile Šikman**, MUP Republike Srpske
grof **Philippe Piccapietra**, počasni predsednik Društva srpsko-švajcarskog prijateljstva „Dr Arčibald Rajs", Švajcarska
prof. dr **Nedžad Korajlić**, dekan Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, Univerzitet u Sarajevu, BiH
prof. dr **Zoltan Rajnai**, Fakultet Banki Donat, Univerzitet Obuda, Mađarska
prof. dr **Andrej Sotlar**, dekan Fakulteta bezbednosnih studija, Ljubljana, Univerzitet u Mariboru, Slovenija
prof. mr. sc. **Ivan Toth**, dekan Veleučilišta Velika Gorica, Hrvatska
prof. dr **Oliver Bačanović**, dekan Fakulteta bezbednosti, Skoplje, Makedonija
prof. dr **Dragan Radonjić**, dekan Pravnog fakulteta, Podgorica, Crna Gora
Milica Pajović, direktorka Policijske akademije, Danilovgrad, Crna Gora

PROGRAMSKI ODBOR

prof. dr **Đorđe Đorđević**, Kriminalističko-policijska akademija, predsednik
prof. dr **Milan Žarković**, Kriminalističko-policijska akademija
prof. dr **Dragan Ranđelović**, Kriminalističko-policijska akademija
prof. dr **Boban Milojković**, Kriminalističko-policijska akademija
prof. dr **Dane Subošić**, Kriminalističko-policijska akademija
prof. dr **Saša Mijalković**, Kriminalističko-policijska akademija
prof. dr **Obrad Stevanović**, Kriminalističko-policijska akademija
prof. dr **Zoran Đurđević**, Kriminalističko-policijska akademija
doc. dr **Nikola Milašinović**, Kriminalističko-policijska akademija
doc. dr **Dragoslava Mićović**, Kriminalističko-policijska akademija

PREFACE

Dear readers,

In front of you is the Thematic Collection of Papers presented at the International Scientific Conference "Archibald Reiss Days", which was organized by the Academy of Criminalistic and Police Studies in Belgrade, in co-operation with the Ministry of Interior and the Ministry of Education, Science and Technological Development of the Republic of Serbia, National Police University of China, Lviv State University of Internal Affairs, Volgograd Academy of the Russian Internal Affairs Ministry, Faculty of Security in Skopje, Faculty of Criminal Justice and Security in Ljubljana, Police Academy "Alexandru Ioan Cuza" in Bucharest, Academy of Police Force in Bratislava and Police College in Banjaluka, and held at the Academy of Criminalistic and Police Studies, on 10 and 11 March 2016.

The International Scientific Conference "Archibald Reiss Days" is organized for the sixth time in a row, in memory of the founder and director of the first modern higher police school in Serbia, Rodolphe Archibald Reiss, PhD, after whom the Conference was named.

The Thematic Collection of Papers contains 165 papers written by eminent scholars in the field of law, security, criminalistics, police studies, forensics, informatics, as well as by members of national security system participating in education of the police, army and other security services from Belarus, Bosnia and Herzegovina, Bulgaria, China, Croatia, Greece, Hungary, Macedonia, Montenegro, Romania, Russian Federation, Serbia, Slovakia, Slovenia, Spain, Switzerland, Turkey, Ukraine and United Kingdom. Each paper has been double-blind peer reviewed by two reviewers, international experts competent for the field to which the paper is related, and the Thematic Conference Proceedings in whole has been reviewed by five competent international reviewers.

The papers published in the Thematic Collection of Papers contain the overview of contemporary trends in the development of police education system, development of the police and contemporary security, criminalistic and forensic concepts. Furthermore, they provide us with the analysis of the rule of law activities in crime suppression, situation and trends in the above-mentioned fields, as well as suggestions on how to systematically deal with these issues. The Collection of Papers represents a significant contribution to the existing fund of scientific and expert knowledge in the field of criminalistic, security, penal and legal theory and practice. Publication of this Collection contributes to improving of mutual cooperation between educational, scientific and expert institutions at national, regional and international level.

The Thematic Collection of Papers "Archibald Reiss Days", according to the Rules of procedure and way of evaluation and quantitative expression of scientific results of researchers, passed by the National Council for Scientific and Technological Development of the Republic of Serbia, as scientific publication, meets the criteria for obtaining the status of thematic collection of papers of international importance.

Finally, we wish to extend our gratitude to all the authors and participants in the Conference, as well as to all those who contributed to or supported the Conference and publishing of this Collection, especially to the Ministry of Interior and the Ministry of Education, Science and Technological Development of the Republic of Serbia.

Belgrade, June 2016 *The Programme Committee*

TABLE OF CONTENTS

TOPIC V

Social, Economic and Political Flows of Crime - Manifestation, Measuring and Analysis

TOPIC VII

Cybercrime

TOPIC VIII

Innovative Techniques and Equipment in Forensic Engineering

Topic V

SOCIAL, ECONOMIC AND POLITICAL FLOWS OF CRIME – MANIFESTATION, MEASURING AND ANALYSIS

UDC: 378.6:343(494)

THE SCHOOL OF CRIMINAL JUSTICE, UNIVERSITY OF LAUSANNE: FROM R. A. REISS TO CURRENT CHALLENGES

Olivier Ribaux, PhD[1]
University of Lausanne, Faculty of Law, Criminal Justice and Public Administration, School of Criminal Justice

Abstract: Formerly called the *Institut de Police Scientifique*, the School of Criminal Justice (in French: *Ecole des Sciences Criminelles*), was founded by Rodolphe Archibald Reiss in 1909. He brought hence officially forensic science for the first time at an academic level. Since 1954, a professor of criminology broadened the fields covered.

The School has dramatically grown over the past 30 years. Recently, changes in the volume and variety of data generated by criminal activities accelerated developments. This numerical context provided incentive for expanding and restructuring the architecture of courses. Hence, without rejecting its traditions, the school promotes an interdisciplinary search for models linking forensic science, security studies, and criminology. This movement leads to innovative research, opens to emerging professions, and increases students' employability.

Keywords: education and training, traceology, forensic science, criminology.

INTRODUCTION

Rodolphe Archibald Reiss proposed in 1906 the creation of a position of professor of forensic photography, at the University of Lausanne, in Switzerland. The authorities were, however, hesitating and lacking enthusiasm: why creating something that did not exist in academic circles elsewhere at that time?

Considering the sustainability and the growth of the school he eventually founded, that conservatism is difficult to understand nowadays. It may have had its origins in a culture of public administrators concerned about minimising the risks of destabilising the system.

Such inertia in university systems is still a topical issue. This is paradoxical in relation to attitudes, such as creative thinking and innovation, implicitly expected from universities by the public. Traditional boundaries between academic disciplines are the main causes. The way ancients organised knowledge has determined the structure of universities, how communities are organised, and eventually ideal career paths.[2] Occasionally, scientific paradigms, vigorously defended by communities of well-established scholars, erect insurmountable barriers for innovative researchers until a change of generation occurs.[3]

Some movements do not accept this closure, in relation to the magnitude of contemporary complex problems the society is facing. For their adherents, collective and interdisciplinary endeavours are a prerequisite. Security studies, forensic science and criminology are particu-

1 E-mail: Olivier.Ribaux@unil.ch.
2 Fabiani, J.-L. (2013) "Vers la fin du modèle disciplinaire ?", Hermes, la Revue Vol. 67, special issue, Interdisciplinarité : entre disciplines et indiscipline, No. 3, pp. 90–94.
3 Kuhn, T. (1962) The Structure of Scientific Revolutions, University of Chicago Press Chicago.

larly concerned.[4] Indeed, concrete solutions necessitate multiplying perspectives from which common or related objects are investigated. New methods and instruments for solving real world crime-related or security problems must emerge from the destabilisation of the rigid pillars firmly anchored in traditions.

Interdisciplinary approaches are often hailed. They are rarely effectively implemented. Crossing chemistry, physics, mathematics, information sciences, medicine, social sciences, psychology and law, seems intractable in common settings.

This enterprise may demand a return to pioneering works in forensic science and criminology. By facing real-world problems, Reiss continuously broadened his vision. He started from the chemistry of how light acts on the matter, and the development of techniques in photography (and then forensic photography). An important turn occurred then: he developed a special interest for crime problems. This attitude culminated in his seminal book containing a strong criminological component.[5] Just before leaving Switzerland in 1914, he even advised the police of New York about its organisation and policing.[6] The social life of sciences and technologies was obviously one of his main concerns.

This paper provides an interpretation of the School of Criminal Justice's development, over the past thirty years. We argue that it has successfully lack discipline by bypassing standard delineation of sciences. It has considerably broadened its scope and the variety of its approaches to crime problems and security. It is incredibly solicited and its functioning attracts attention worldwide, both from professional and academic environments.

This paper starts by expressing a lively contemporary debate around the different visions of forensic science. The School of Criminal Justice will be situated within this agitated landscape. Its functioning will be explained. An interpretation of its position will be eventually proposed.

FORENSICS OR FORENSIC SCIENCE?

The American National Academy of Sciences has reported a very pessimistic and fragmented situation for forensic science in the US.[7] This document has generated many controversies, and still has a dramatic influence on the evolution of forensic activities, in the whole world. Methods and techniques used to provide evidence at court are presented as insufficiently scientifically validated. Limits of instruments and reliability thresholds are not well known or expressed. Laboratories, organised around specialities, are mostly not accredited and far too influenced by police structures and activities. Scientific independence is not guaranteed. The current forensic science setting is presented as exacerbating unconscious cognitive biases.[8] Only DNA, as a specific forensic discipline, succeeded in eluding criticisms.

Criminal Justice System, the report states, should react and augment structures of control: accreditation and certification schemes should be mandatory. Training and education programmes should be developed in universities. The development of a research culture in forensic science should be a priority.[9] Laboratories should be protected from police culture

4 Ribaux, O., F. Crispino, O. Delémont and C. Roux (2016) "The Progressive Opening of Forensic Science towards Criminological Concerns ", Security Journal, In press.
5 Reiss, R. A. (1911) Manuel de police scientifique (technique). Vols et homicides, Payot Alcan, Lausanne.
6 Reiss, R. A. (1914) Contribution à la réorganisation de la police, Payot, Paris.
7 NAS (2009) Strengthening Forensic Science in the United States: a Path Forward, National Research Council of the National Academies, National Academies Press, Washington D.C.
8 Dror, I. (2013) "The Ambition to be Scientific: Human Expert Performance and Objectivity", Science & Justice, Vol. 53, No. 2, pp. 81–82, http://www.sciencedirect.com/science/article/pii/S1355030613000245.
9 Mnookin, J. L., S. A. Cole, I. E. Dror, B. A. J. Fisher, M. Houck, K. Inman, D. H. Kaye, J. J. Koehler,

and moved away from their structures. Communication of forensic scientists with justice systems should be readjusted.

To what point reforms have been effectively implemented now is an open debate. The strength of this stream is, however, evident when considering academic debates, the structure of forensic conferences, the focus of forensic science associations, or funding schemes.

The biggest merit of this report is the lively debate it has sparked. It, however, recognises almost no own epistemology to forensic science, mainly viewed from the eye of legal figures. The discipline is rather called *forensics,* insisting that the forensic science disciplines are a patchwork of fundamental sciences' applications such as chemistry, physics, biology, biochemistry or engineering, and obviously medicine. The importance of information sciences is always much more recognised in this context.[10] These disciplines are the main drivers of forensic activities.

In summary, the efforts called for are significant, and mostly desirable, but they remain essentially in line with the dominant *forensics* stream. Hence, the debate raised by the report has not caused a demand for a paradigm shift, as it may be occasionally suggested.[11]

THE SCHOOL OF CRIMINAL JUSTICE FACING THE FORENSICS CRISIS

The NAS report has necessarily found an echo at the Sl. The reason the institution exists is based on the recognition of a discipline called forensic science. If forensic science is reduced to forensics and contains almost no own epistemology, no reason remains to keep under the same roof such scattered activities. The only possible path would be to close the gates of the School, and replace it by prolonging chemistry, computer science, biochemistry and physic departments in other universities. This is the dominant model adopted all around the world promoted by the *forensics* view.

For instance, in the UK, the number of courses having added the term "forensic" in their original definition based on natural sciences, has dramatically grown. Media and TV series have reinforced the popularity of forensic science, and, hence, this movement. It offers fantastic opportunities for some chemistry departments to appropriate it for retaining branches deserted by the students.[12]

What is the position of professors and researchers at the School of Criminal Justice in the face of this crisis, which could potentially lead to its disaggregation?

Of critical importance are the liberty of thought, and the independence of its researchers. They are the main fundamental values defended by the whole University. The institution has a very democratic functioning, which promotes debates and the development of a variety of positions on the same subjects. The management of the School is responsible for proposing to its Council a general strategy, and for running administratively the institution. Its abso-

G. Langenburg, D. M. Risinger, N. Rudin, J. Siegel and D. A. Stoney (2011) "The Need for a Research Culture in the Forensic Science", UCLA Law Review, Vol. 58, No. 3, pp. 725–779.

10 Roux, C., J. Robertson, B. Talbot-Wright, O. Ribaux and F. Crispino (2015) "The End of the (Forensic Science) World as We Know It? – The Example of Trace Evidence", Philosophical Transactions B, Vol. 370, 20140260.

11 Black, S. and N. N. Daeid (2015) "Time to think differently: catalysing a paradigm shift in forensic science", Philosophical Transactions B, Vol. 370, 20140251.

12 Mennell, J. (2006) "The future of Forensic and Crime Scene Science: Part II. A UK Perspective on Forensic Science Education", Forensic science international, Vol. 157, Supplement, S13-S20, http://www.sciencedirect.com/science/article/pii/S0379073805006948.

lute priority consists, however, in preserving the independence and autonomy of its researchers. This is hence not surprising that a broad spectrum of opinions has internally developed around conceptions and visions of forensic science and criminology. Individual agendas and priorities may diverge considerably. The coherency of the whole is not an objective, and may even be undesirable. The developments of various viewpoints do not contradict an almost unanimous respect to the institution, which constitutes the strong cement. This is an important nuance which even constitutes a postulate.

Worldwide, key players and stakeholders recognise the Lausanne school of thought: does it mean something internally?

We argue that, across the diversity of conceptions, fundamental tenets provide sense to the existence of the School, beyond the sole motivation to make it exist.

Some commentators officially disagree with the Lausanne interdisciplinary endeavour and the programme it provides.[13] Paradoxically, the School seems to attract the interests of external stakeholders. It is incredibly and increasingly solicited. *Ceteris paribus*, the "place to be" in forensic science definitely seems to be Lausanne.

As Stuart Kind, a previous director of research of the forensic science service in Aldermaston (UK), noticed[14]: Lausanne is the place where the *thing* started. But what is this *thing*?

LAUSANNE CULTURE OF FORENSIC SCIENCE

The international and internal esteem gained by previous directors of the school have played a great role in creating and maintaining internal cohesive forces. It started with its founder, Rodolphe Archibald Reiss, and continued with professors Marc Bischoff, Jacques Mathyer, and eventually Pierre Margot. It is under the management of this latest director, spanning twenty-nine years, that the School has experienced its biggest expansion. It has diversified its activities, and has prepared a new generation of academicians in forensic science. He has largely influenced most of current professors' careers. They would have even never existed without him.

Pierre Margot provided a sharp and vigorous response to the NAS report,[15] as well as proposals, members of the School would probably not contest.[16] He presents forensic science as a discipline:

- studying its own object (the trace, vestige of a litigious activity);
- resting on a methodology for extracting relevant information from the trace, in function of problems to be faced (reconstructing specific events, identifying a person or an object, evaluating the evidential value of traces in the circumstances of the case, linking cases);
- developing a scientific programme (building frameworks, collecting specific types of data);
- underlying many occupational activities related to a new set of professions.

13 Cole, S. (2013) "Response Forensic Science Reform: Out of the Laboratory and into the Crime Scene", Texas Law Review, Vol. 91, pp. 124–136; Risinger, D. M. (2013) "Reservations about Likelihood Ratios (and Some Other Aspects of Forensic 'Bayesianism')", Law, Probability and Risk, Vol. 12, No. 1, pp. 63–73.
14 Kind, S. S. (1984) "La science dans l'enquête criminelle", Revue Internationale de Criminologie et de Police Technique, Vol. 37, pp. 92–101.
15 Margot, P. (2011a) "Commentary on the Need for a Research Culture in the Forensic Sciences", UCLA Law Review, Vol. 58, No 3, pp. 795–801.
16 Margot, P. (2011b) "Forensic Science on Trial – What Is the Law of the Land?", Australian Journal of Forensic Sciences, Vol. 43, No. 2, pp. 89–103.

This view is based on the well-known and widely embraced Locard's postulate:

"The truth is that none can act with the intensity induced by criminal activities without leaving multiple traces of his path. [...] The clues I want to speak of here are of two kinds: Sometimes the perpetrator leaves traces at a scene by their actions; sometimes, alternatively, he/she picked up on their clothes or their body traces of their location or presence."[17]

For Margot, the "object of forensic science or its primitive source of information" is hence the *trace*.

"(…) the trace, which, by definition, is a pattern, a signal or material transferred during an event (often unknowingly by the actors of the event). It is the remnant (the memory) of the source (identity – who, with what?) and of the activity (what, how, when, why?) that produced it."[18]

A methodology for extracting information from the trace is depicted in Figure 1.

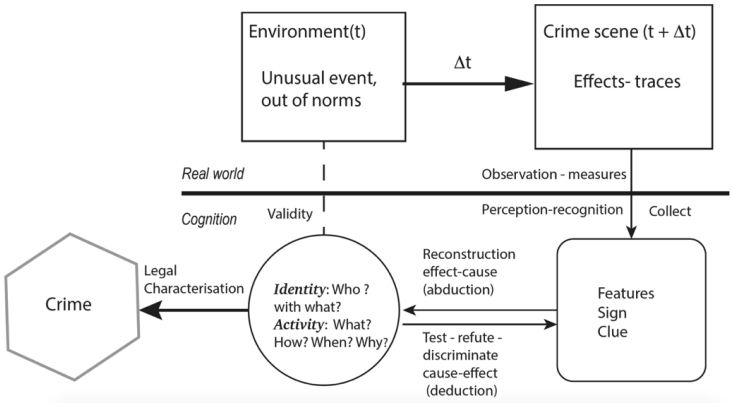


Figure 1: *The forensic science process. The identity of objects and persons, elements of the activity, as well as the legal characterisation are reconstructed by abduction from the detection, the collection, and the interpretation of traces.*

The detailed definitions and constitutive elements of the paradigm can be found in Margot's paper.[19] It starts from the trace, and inverses the usual focus on core sciences' technologies, to the specific problem under scrutiny.

Obviously, part of forensic science consists of developing new technologies. They are, however, carefully designed in order to extend human perceptions under the circumstances and the constraints of investigations. Moreover, this definition does not mean that fundamental sciences have no relevancy, but the attention must focus on problem solving. Fundamental sciences and derived technologies must serve the resolution of problems, not the other way round!

Forensic science claims hence for the existence of a forensic generalist. It is handling forensic issues in the course of investigations, from the crime scene to the court.

The event of interest is unique, and not reproducible due to the asymmetry of time. Its (partial) reconstruction, by analysing and interpreting fragmented traces detected and seen at the scene, is thus the methodological focus of forensic science.

17 Locard, E. (1920) L'enquête criminelle et les méthodes scientifiques, Flammarion, Paris.
18 Margot, P. (2011b) "Forensic Science on Trial – What Is the Law of the Land?", Australian Journal of Forensic Sciences, Vol. 43, No. 2, p. 91.
19 Margot, P. (2011b) "Forensic Science on Trial – What Is the Law of the Land?", Australian Journal of Forensic Sciences, Vol. 43, No. 2, pp. 89–103.

- There is no way to ensure that, if a trace exists, it will be found, whatever the deployment of resources (there is no way to know where is dispersed each piece of material exchanged in the course of an event of interest);

- traces collected are hence not *sample,* which has a well-defined statistical meaning, but *specimen*. This is because there is no way to affirm that they are representative of the set of existing traces generated in the event;

- relevant traces have to be detected and seen on the basis of assumptions about possible scenarios. These hypotheses are developed from knowledge about the crime situation, analogies with previous events encountered or interpretations of the specific immediate physical and social environment;[20]

- methods and techniques engaged at the scene or in laboratories for extracting characteristics from the trace serve the resolution of the specific problem at hand. They must be rationally chosen, in sequence, in function of the interpretation of the situation, knowledge about their potential, resources available, as well as the various aims of an investigation at different stages (*e.g.* detecting a trace, finding suspects, explaining an aspect of the event);

- the uncertain information extracted from fragmented traces supports mainly two levels of interpretation: the identification of persons or objects,[21] or the description of elements of the activity. Most often than not, these interpretations must be relevant from a legal perspective;

- traces are eventually evaluated for a court. Uncertainties must be managed and presented in logic, balanced, robust, and transparent way.[22] They serve, however, also to orient many other decisions in the course of an investigation;

- the information extracted from traces encourages going beyond the sole reconstruction of single events: crime repetitions can be detected through the systematic comparison of traces.

Forensic science does not exist in isolation. It is, in priority, serving legal systems. It is hence highly influenced by legal settings and reasoning. Some of the mentioned aspects incite, however, going even further: reconstruction means eliciting mechanisms behind each crime. Linking traces means deciphering crime systems. Ways of disrupting or preventing those mechanisms can also emerge from the analysis and use of traces.

Forensic science concentrates then also on the study of crime itself, and ways the society reacts to it, *i.e.* criminology. In other words, it can take some autonomy from law enforcement and justice systems to contribute to security studies (e.g. policing, intelligence, prevention) and many other areas in criminology (e.g. evaluating drug consumption through wastewater analysis).[23] There was very soon a realisation that criminology and security studies should complete curricula at Lausanne: forensic science and criminology are not so distinct as cur-

20 Ribaux, O., A. Baylon, E. Lock, C. Roux, O. Delémont, C. Zingg and P. Margot (2010) "Intelligence-led Crime Scene Processing. Part II: Intelligence and Crime Scene Examination ", Forensic Science International, Vol. 199, pp. 63–71, doi:10.1016/j.forsciint.2009.10.027.

21 Kirk, P. L. (1963) "The Ontogeny of Criminalistics", The Journal of Criminal Law, Criminology and Police Science, Vol. 54, pp. 235–238.

22 Biedermann, A. and F. Taroni (2012) "Bayesian Networks for Evaluating Forensic DNA Profiling Evidence: A Review and Guide to Literature", Forensic Science International: Genetics, Vol. 6, No. 2, pp. 147–157, http://www.sciencedirect.com/science/article/pii/S1872497311001359; Biedermann, A. (2015) "The Role of the Subjectivist Position in the Probabilization of Forensic Science", Journal of Forensic Science and Medicine, No. 1, pp. 140–148.

23 van Nuijs, A. L. N., S. Castiglioni, I. Tarcomnicu, C. Postigo, M. L. de Alda, H. Neels, E. Zuccato, D. Barcelo and A. Covaci (2011) "Illicit drug consumption estimations derived from wastewater analysis: A critical review", Science of The Total Environment, Vol. 409, No. 19, pp. 3564–3577, http://www.sciencedirect.com/science/article/pii/S0048969710005450; Béen, F. (2014) "Population Normalization with Ammonium (NH4-N) in Wastewater-Based Epidemiology: Application to Illicit Drug Monitoring", Submitted.

rent conceptions and implementation of academic programmes may let perceive. They can cross-fertilise each other.[24]

Another evolution is critical. The Volume of traces available, their Variety, the Velocity at which they have to be treated and they change, their questioned Validity, as well as the Value they represent constitute the 5Vs scheme that define big data spaces. Order of magnitude is changing, in particular due to the necessity to investigate numerical spaces. The nature, extent and scale of problems to solve and traces to treat radically change. The core notion of trace becomes more and more central, and allows a natural expansion of forensic science frameworks. Such a global vision is necessary for avoiding that security systems unproductively jump from one technology to another one for exploring big data spaces. This is one of the main concerns of organisations (academic or not) dealing with security, criminology or forensic science.

COURSES AT THE SCHOOL OF CRIMINAL JUSTICE

This paradigm orients educations and training programs from the School of Criminal Justice (Figure 2).

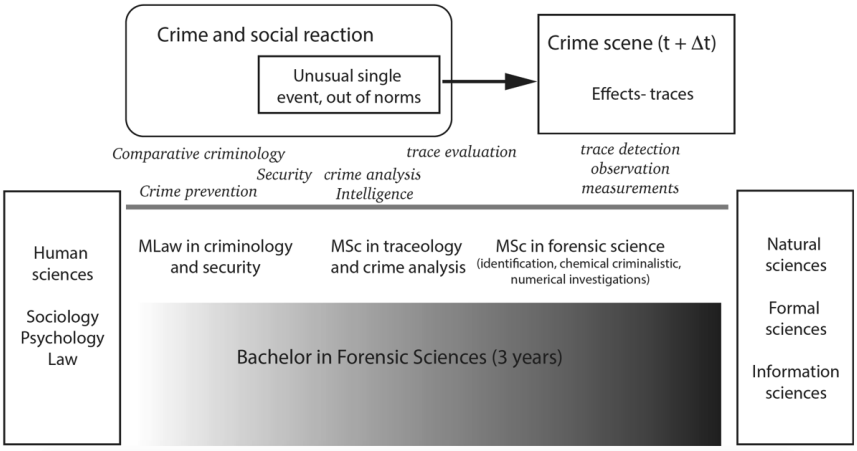


Figure 2: *The architecture of courses at the School of Criminal Justice, of Lausanne. It is strongly influenced by natural, formal and information sciences. It, however, provides streams that conduct students to more criminological path or to security studies. Around half of the students orient their career towards new professions outside traditional forensic science settings (i.e. laboratories or crime scene departments).*

The initial year of education in forensic science at the University of Lausanne is not tremendously distinct from the first year in other fundamental science courses. It consists mainly of a solid basis in mathematics, information sciences, physics, biochemistry, and chemistry. These branches are completed by an introduction to forensic science, to law, and to criminology. From the second year, awareness of students to the discipline of forensic science is increased. Modules such as trace evidence, fingermarks, shoemarks or toolmarks detections, biological marks, firearms investigation or illicit drugs are delivered at this stage of the studies. More transversal approaches are treated in specific classes such as crime scene investigation, forensic intelligence, fire investigation or statistical evaluation of traces. Methodological and

24 Ribaux, O., F. Crispino, O. Delémont and C. Roux (2016) "The Progressive Opening of Forensic Science towards Criminological Concerns", Security Journal, In press.

technological disciplines complete the program (microscopy, image processing and photography, or separation methods in analytical chemistry).

One single master in forensic science proposes three orientations: they relate either to the study of identification processes of objects and persons, of forensic chemistry, as well as of numerical identification and investigation processes. A new master is organised jointly with the University of Montreal and its School of Criminology. It is called traceology and crime analysis. Students of Lausanne spent one semester in this esteemed School. Eventually, a master in criminology and security complete the transversal coverage of the disciplines.

More than one hundred students enter each year the bachelor in forensic science. This first year is very demanding, as only around forty students reach the second year. Masters are populated by around seventy students in forensic science, fifteen in traceology, and eighty in criminology and security. In the context of the Bologna system, mobility is promoted. New students coming with different backgrounds join the master's courses. From their side, Lausanne's students are travelling all over Europe in criminology. In forensic science, agreements cover mostly selected programmes in Canada, the UK, Australia or China. More than one hundred PhD students are carrying out research in forensic science or criminology at the School. Almost half of them realises their research while working in a professional forensic environment in many different countries.

In whole, the School has experienced an increase of 40% of its students from 2008. Around 30% of the students come from a foreign country.

CONCLUSION

Based on its historical solid foundations, the School of Criminal Justice of the University of Lausanne adapts in the face of a changing environment. These evolutions follow a conception of a science focused on the study of traces, vestiges of a litigious activity. Rather than seeing criminology, security studies and forensic science as separated disciplines, the School suggests overlapping and continuity. Novelty will mainly come from the many links to be easily built within the framework and the autonomy provided by the organisation to the professors and researchers of the School. The transversal view promoted has already stimulated the emergence of original and innovative approaches to the study of new forms of crimes, and of the behaviours of figures/actors[25]. Fundamental works feed the debate around the epistemology of forensic science[26] and criminology[27], or of both. PhD researches regularly lead

25 Pazos, D., P. Giannasi, Q. Rossy and P. Esseiva (2013) "Combining Internet Monitoring Processes, Packaging and Isotopic Analyses to Determine The Market Structure: The Example of Gamma Butyrolactone.", Forensic Science International, Vol. 230, No 1–3, pp. 29–36; Béen, F. (2014) "Population Normalization with Ammonium (NH4-N) in Wastewater-Based Epidemiology: Application to Illicit Drug Monitoring ", Submitted; Baechler, S., M. Morelato, O. Ribaux, A. Beavis, M. Tahtouh, P. Kirkbride, P. Esseiva, P. Margot and C. Roux (2015) "Forensic intelligence framework. Part II: Study of the main generic building blocks and challenges through the examples of illicit drugs and false identity documents monitoring", Forensic Science International, Vol. 250, pp. 44–52; Ressnikoff, T., O. Ribaux, A. Baylon, M. Jendly and Q. Rossy (2015) "The Polymorphism of Crime Scene Investigation: an Exploratory Analysis of the influence of Crime and Forensic Intelligence on decisions made by Crime Scene Examiners", Forensic Science International, Vol. 257, pp. 425–434.

26 Crispino, F., O. Ribaux, M. Houck and P. Margot (2011) "Forensic Science – A True Science ?", Australian Journal of Forensic Sciences, Vol. 43, No 2, pp. 157–176; Roux, C., F. Crispino and O. Ribaux (2012) "From Forensics To Forensic Science", Current Issues in Criminal Justice, Vol. 24, No. 1, pp. 7–24; Biedermann, A. (2015) "The Role of the Subjectivist Position in the Probabilization of Forensic Science", Journal of Forensic Science and Medicine, No. 1, pp. 140–148.

27 Aebi, M. F., A. Linde and N. Delgrande (2015) "Is There a Relationship Between Imprisonment and Crime in Western Europe?", Eur J Crim Policy Res, Vol. 21, pp. 425–446.

to the development of systems deployed in operational environments[28]. Security policies are frequently supported through deliverable provided by the School along a broad spectrum of dimensions. The participation of the School in police training is still increasing. Employability of students has shown to improve through the creation of new professions, in phase with the vision underlying the development of the School.

The diversity of the courses, overlapping and connexions increase complexity. It makes the management of the School delicate. Its size and its coverage should probably not grow beyond a certain threshold, despite many opportunities and temptations. Improving possibilities to enter the master in criminology and security from the bachelor seems an important aspect of the development. This master is currently populated by a vast majority of students entering with a bachelor in psychology, social sciences or political sciences. Developing criminological aspects of the bachelor in forensic science will provide more harmony within the whole education architecture and less heterogeneity across the students.

The development of virtual worlds will evidently bring new students in the dedicated course at the School. The size of the flow is unpredictable, but vigilance is necessary in order to adapt resources.

Eventually, the size of certain partners (occasionally a whole University or even a government) creates an asymmetry difficult to manage for a relatively modest School. Protecting members of the School who may feel overwhelmed by such pressure, while maintaining an open attitude is a managerial challenge.

In summary, Lausanne seems to provide an artisanal highly demanded product, which is contradicting with all management theories, dominant streams, and industrial processes. The whole edifice will remain sustainable only if internal cohesive forces stay sufficiently strong to resist to attractive external calls. They mostly come from fundamental disciplines willing to prolong and invigorate their own branches.

Developing, stimulating, and maintaining an internal epistemological debate is probably the core mission of the management of the School in order to achieve its adaptation without endangering its existence.

REFERENCES

1. Aebi, M. F., A. Linde and N. Delgrande (2015) "Is There a Relationship Between Imprisonment and Crime in Western Europe? ", *Eur J Crim Policy Res,* Vol. 21, pp. 425–446.
2. Baechler, S., M. Morelato, O. Ribaux, A. Beavis, M. Tahtouh, P. Kirkbride, P. Esseiva, P. Margot and C. Roux (2015) "Forensic intelligence framework. Part II: Study of the main generic building blocks and challenges through the examples of illicit drugs and false identity documents monitoring", *Forensic Science International,* Vol. 250, pp. 44–52.
3. Béen, F. (2014) "Population Normalization with Ammonium (NH4-N) in Wastewater-Based Epidemiology: Application to Illicit Drug Monitoring", Submitted.
4. Biedermann, A. (2015) "The Role of the Subjectivist Position in the Probabilization of Forensic Science", *Journal of Forensic Science and Medicine,* No 1, pp. 140–148.
5. Biedermann, A. and F. Taroni (2012) "'Bayesian Networks for Evaluating Forensic DNA Profiling Evidence: A Review and Guide to Literature", *Forensic Science International: Genetics,* Vol. 6, No. 2, pp. 147–157, http://www.sciencedirect.com/science/article/pii/S1872497311001359.

28 Rossy, Q. and O. Ribaux (2014) "A Collaborative Approach for Forensic Science and Investigation Using Criminal Intelligence Analysis and Visualisation", Science and Justice, Vol. 54, No. 2, pp. 146–153.

6. Black, S. and N. N. Daeid (2015) "Time to think differently: catalysing a paradigm shift in forensic science", *Philosophical Transactions B,* Vol. 370, 20140251.

7. Cole, S. (2013) "Response Forensic Science Reform: Out of the Laboratory and into the Crime Scene", *Texas Law Review,* Vol. 91, pp. 124–136.

8. Crispino, F., O. Ribaux, M. Houck and P. Margot (2011) "Forensic Science – A True Science ?", *Australian Journal of Forensic Sciences,* Vol. 43, No. 2, pp. 157–176

9. Dror, I. (2013) "The Ambition to be Scientific: Human Expert Performance and Objectivity", *Science & Justice,* Vol. 53, No. 2, pp. 81–82, http://www.sciencedirect.com/science/article/pii/S1355030613000245.

10. Fabiani, J.-L. (2013) "Vers la fin du modèle disciplinaire?", *Hermes, la Revue,* Vol 67, special issue, Interdisciplinarité: entre disciplines et indiscipline, No. 3, pp. 90–94.

11. Kind, S. S. (1984) "La science dans l'enquête criminelle", *Revue Internationale de Criminologie et de Police Technique,* Vol. 37, pp. 92–101.

12. Kirk, P. L. (1963) "The Ontogeny of Criminalistics", *The Journal of Criminal Law, Criminology and Police Science,* Vol. 54, pp. 235–238.

13. Kuhn, T. (1962) *The Structure of Scientific Revolutions*, University of Chicago Press Chicago.

14. Locard, E. (1920) *L'enquête criminelle et les méthodes scientifiques*, Flammarion, Paris.

15. Margot, P. (2011a) "Commentary on the Need for a Research Culture in the Forensic Sciences", *UCLA Law Review,* Vol. 58, No. 3, pp. 795–801.

16. Margot, P. (2011b) "Forensic Science on Trial - What Is the Law of the Land?", *Australian Journal of Forensic Sciences,* Vol. 43, No. 2, pp. 89–103.

17. Mennell, J. (2006) "The future of Forensic and Crime Scene Science: Part II. A UK Perspective on Forensic Science Education", *Forensic science international,* Vol. 157, Supplement, S13-S20, http://www.sciencedirect.com/science/article/pii/S0379073805006948.

18. Mnookin, J. L., S. A. Cole, I. E. Dror, B. A. J. Fisher, M. Houck, K. Inman, D. H. Kaye, J. J. Koehler, G. Langenburg, D. M. Risinger, N. Rudin, J. Siegel and D. A. Stoney (2011) "The Need for a Research Culture in the Forensic Science", *UCLA Law Review,* Vol. 58, No. 3, pp. 725–779.

19. NAS (2009) *Strengthening Forensic Science in the United States: a Path Forward*, National Research Council of the National Academies, National Academies Press, Washington D.C.

20. Pazos, D., P. Giannasi, Q. Rossy and P. Esseiva (2013) "Combining Internet Monitoring Processes, Packaging and Isotopic Analyses to Determine The Market Structure: The Example of Gamma Butyrolactone", *Forensic Science International,* Vol. 230, No. 1–3, pp. 29–36.

21. Reiss, R. A. (1911) *Manuel de police scientifique (technique). Vols et homicides*, Payot Alcan, Lausanne.

22. Reiss, R. A. (1914) *Contribution à la réorganisation de la police*, Payot, Paris.

23. Ressnikoff, T., O. Ribaux, A. Baylon, M. Jendly and Q. Rossy (2015) "The Polymorphism of Crime Scene Investigation: an Exploratory Analysis of the influence of Crime and Forensic Intelligence on decisions made by Crime Scene Examiners", *Forensic Science International,* Vol. 257, pp. 425–434.

24. Ribaux, O., A. Baylon, E. Lock, C. Roux, O. Delémont, C. Zingg and P. Margot (2010) "Intelligence-led Crime Scene Processing. Part II: Intelligence and Crime Scene Examination", *Forensic Science International,* Vol. 199, pp. 63–71, doi:10.1016/j.forsciint.2009.10.027.

25. Ribaux, O., F. Crispino, O. Delémont and C. Roux (2016) "The Progressive Opening of Forensic Science towards Criminological Concerns", *Security Journal*, In press.

26. Risinger, D. M. (2013) "Reservations About Likelihood Ratios (and Some Other Aspects of Forensic 'Bayesianism')", *Law, Probability and Risk,* Vol. 12, No. 1, pp. 63–73.
27. Rossy, Q., S. Ioset, D. Dessimoz and O. Ribaux (2013) "Integrating Forensic Information in a Crime Intelligence Database", *Forensic Science International,* Vol. 230, pp. 137–146.
28. Rossy, Q. and O. Ribaux (2014) "A Collaborative Approach for Forensic Science and Investigation Using Criminal Intelligence Analysis and Visualisation", *Science and Justice,* Vol. 54, No. 2, pp. 146–153.
29. Roux, C., F. Crispino and O. Ribaux (2012) "From Forensics To Forensic Science", *Current Issues in Criminal Justice,* Vol. 24, No. 1, pp. 7–24.
30. Roux, C., J. Robertson, B. Talbot-Wright, O. Ribaux and F. Crispino (2015) "The End of the (Forensic Science) World as We Know It? – The Example of Trace Evidence", *Philosophical Transactions B,* Vol. 370, 20140260.
31. van Nuijs, A. L. N., S. Castiglioni, I. Tarcomnicu, C. Postigo, M. L. de Alda, H. Neels, E. Zuccato, D. Barcelo and A. Covaci (2011) "Illicit drug consumption estimations derived from wastewater analysis: A critical review", *Science of The Total Environment,* Vol. 409, No. 19, pp. 3564–3577, http://www.sciencedirect.com/science/article/pii/S0048969710005450.

UDC: 343.14:343.62-055.2
343.14:343.54/.55-055.2

THE PROBLEM OF THE INCRIMINATION EVIDENCE IN THE GENDER VIOLENCE PURSUIT

Ramiro Herranz Latorre[1]
National Police Academy, Legal Sciences Department, Ávila

Abstract: In 2004 in Spain, the Integrated Law against Gender Violence was enacted. The gender violence is the most brutal symbol of inequality in our society. This law aims to provide a comprehensive, integrated and multidisciplinary response to violence against women as well as formulate its prevention. The law establishes the need for an adequate training of healthcare, police and legal practitioners.

More than a decade after, the figures of deceased women are still staggering, reaching up to 750. A serious procedural problem accompanies this situation; these crimes are committed in the privacy of the family. This makes it difficult to have other sources of evidence for prosecution apart from the victim's testimony.

However, Spanish Procedural Law establishes a serious obstacle to the incorporation of this testimony into evidence material. On the one hand, it establishes the general obligation for all witnesses to attend the appeal court and declare everything they know, but it also reflects the dispensing of this obligation to the closest relatives of the accused, and they are precisely the perpetrators of gender violence. It also reflects that no witness may be compelled to testify about a question whose answer may harm some of his/her relatives.

According to certain authors, the foundation of this dispensation is to protect the solidarity bonds between the witnesses and the person under investigation. These bonds are based in the protection of family relationships and the family intimacy besides.

But the consequence of this procedural privilege makes that many cases are filed, which go unpunished and, secondly, what is more serious, it causes the lack of protection for gender violence victims. We must find a solution; it originates in the report of the Judicial Police.

Keywords: gender violence, family privacy, evidence, dispensing, victim protection, judicial police.

INTRODUCTION

On December 28, 2004, the Spanish Parliament enacted the Organic Law 1/2004, about the Integral Protection against Gender Violence[2].

The Law[3] is trying to give a global, integral and multidisciplinary response to the violence against women, from the prevention (emphasizing educational and social fields), through

1 E-mail: ramiro.herranz@dgp.mir.es.
2 Official Magazine of State, number 313, dated 29th December, 2004.
3 Exposition of motives of the Constitutional Law 1/2004, dated 29th December.

assistance and care for victims, emphasizing civil laws related to family rights, within which the attacks mainly occur.

The integral law labels gender violence as the most brutal icon of our unbalanced society.

From an educational point of view, the main goal is to provide an integral education which allows a suitable perception of women, incorporating into the secondary school curricular content about equality and against gender violence. Likewise, a scholar board member is responsible for enhancing equality and struggle against violence against women.

In the field of advertising, this law is forcing media to give an equal and dignified image of woman. A procedure measure is added for helping the balance between men and women associations which are able to stop or rectify an opposite advertising.

Besides, there is a victims' support, providing information and a unique legal assistance without charge during all the judicial proceeding.

This law underlines the need for an available training for health service operators, police officers and judicial staff. It also established the need for applying the healthy protocols in case of attacks related to gender violence, which will be sent to competent court.

Furthermore, some measures aimed at achieving the early detection of these violent cases against women and at receiving an available psychologist care for victims.

Additionally, this law covers protection of minors, not only to protect their rights but also to protect them from indirect violence that attacks produce against their mothers.

When it comes to social measures, the Worker's Statute[4] is modified to justify early absence, geographical mobility, a reserved right to their job even with the possibility of employment contract cancellation which implies the acknowledgment of being legally unemployed.

The Law also collects financial aids[5] and recognizes the right to legal unemployment when the employment contract is suspended.

Labour insertion plan is provided for women victims with no means of subsistence, in that way becoming economically emancipated from their attackers, which many times is the key point to face their situation, and what's more in cases with victims with disabilities cared by their attackers.

This economic measure remains compatible with previous ones (about other violent crimes[6]).

Finally, this law also contains penal and procedure measures.

From a penal point of view, an aggravating circumstance is added, the fact that the victim is or was the perpetrator's wife or woman in a similar relation of affectivity, even without cohabitation, or a special vulnerable person who lives with the perpetrator.

In the same way, we can define as criminal offenses the threats and coercions in the cases when the victims are women previously mentioned.

With this penalty we do not only protect the guaranteed right to life or health of each person, but especially other rights such as moral integrity as well as the right to not be submitted to inhuman or degrading actions.

This Law aims to guarantee in an efficient manner an individual legal situation, as well as the family and social legal situation of the gender violence victims.

4 Legislative Royal Decree 1/1995, dated 24th March, based on which the Consolidated Text of the Legal Statute of Workers, was approved.
5 Legislative Royal Decree 1/1994, dated 20th June, based on which the Consolidated Text of the General Social Security Act, was approved.
6 Law 35/1995, dated 11th December, about Aids and Assistance for Violence Offenses and Offenses against Sexual Freedom Victims.

In order for that to be achieved, attempts are made so that the legal proceedings are much faster and the civil and penal code are aligned, with the objective to further facilitate the protection measures of women and children and to establish a series of cautionary measures with the urgent character.

This Law has selected the specialization of the legal authority, by creating the Tribunals for Violence against Women, in charge of proceedings and any failures in penal matters as well as related civil matters.

Presently, the protection measures are included in the Law of Criminal Procedure. These measures can be adopted by the Judge in charge of Violence against Women and it allows the opportunity for such measures to be used as protective measures, since the beginning of process and even after the sentence, all in order to provide protection even after the process has been finalized.

Finally, a new authority has been created within the Public Prosecutor's Office, the Prosecutor against Violence against Women. This authority will supervise and coordinate the activities of the Prosecutor in all of the proceedings related to gender violence, thus creating the special Section in the Superior Tribunals of Justice and the Provincial Courts.

The special prosecutor will intervene in the penal cases as well as civil cases of separation, divorce or annulment and in those in which the custody of minors is involved, with special attention to mothers and minors, victims of sexist violence.

THE EVIDENCE IN THE GENDER VIOLENCE CASES AND THE EXEMPTION OF THE OBLIGATION TO DECLARE IN THE PRESENCE OF RELATIVES

Despite all of the mentioned efforts, eleven years after the enactment of the Integral Law, the figures of diseased women, as a consequence of sexist violence, are still astonishing. On 16 December 2015, the annual figure of diseased victims in Spain was 53, with the total of 748 women since 2004[7].

The influence of sexist violence has motivated continuous legal reforms since the late 1980s, in order to punish this type of phenomenon and provide a greater protection of the victim.

Despite of that, a significant problem, which affects our legal system, accompanies this situation, that is, the violent crimes are most often committed in the privacy of family life.

As a consequence of such fact, we rarely have other sources of evidence, apart from the victim's statement. This is why the judicial authorities grant the value of this evidence alone, in order to exempt the presumption of innocence of the aggressor.

This evidence needs to justify the conviction of the sentencing authority through the adoption of principles of morality, contiguity, concentration and publicity.

The Supreme Court[8] has established that the valuation of the victim's statement corresponds to the Tribunal in charge, which needs to cautiously determine its truthfulness.

These cautionary measures are three. First of all, the absence of the subjective incredibility, determined by the characteristic or the personal circumstances of the victim, the level of victim's development or maturity, as well as any false drives which could result in tendencies to fantasize or invent.

7 Data from Government Delegation for Gender Violence (Ministry of Health, Social Services and Equality). Available at: http://www.inmujer.gob.es/estadisticas/violencia/victimasMortalesI/2012/w809.xls.
8 Sentence of the Supreme Court dated 21st March 2011.

Secondly, we must not disregard the credibility of the testimony itself, based on the logic of the statement supported by objective information.

In that sense, it is my opinion that what matters is the coherency of the facts presented, as well as, in the case of physical violence, the existence of the medical assistance which could confirm the presence of lesions. It is also important to keep in mind the immediacy of assistance, although, depending on the circumstances, it cannot be a crucial factor, since in many occasions, the victim is in such state that makes it impossible for her to attend any medical center, or she cannot leave her children unattended, or on the other hand, is forced by the aggressor himself not to leave the household and seek medical attention.

Furthermore, the High Tribunal demands the presence of incriminating evidence, obtained in time and exposed without any ambiguities or contradictions. This prerequisite assumes the absence of any modifications in later declarations given by the victim, no contradictions or denial, no generalities or vague explanations, demanding for the order of events occurred to have a clear logical connection.

As is determined by the Supreme Court[9], in order to correctly examine the evidence, it is important to bear in mind the fact that the event has occurred in a private environment, as well as the social reality of a time in which this law is being applied. This reality, without a doubt, demands a blunt answer to a problem which, whether or not we want to recognize it, traditionally has been masked within the private environment, contrary to the Penal Law.

Therefore, in the field of penal proceedings the declaration of the victim is essential for the recognition of facts occurred; however, Spanish Procedural Law has a significant obstacle when it comes to its implementation in the evidence collection.

On one hand, the Article 410 of the Law on Criminal Procedure establishes an obligation for all witnesses who reside on the Spanish territory to answer when summoned by the Court and to testify of all the facts known to them, while on the other hand the Article 416 of the same Law adopts the exemption of this obligations when closest relatives are involved, precisely due to the perpetrator of sexist violence.

Besides that, the Article 418 of the Law on Criminal Procedure reflects that no witness can be obligated to testify in regard to any question which could damage in any way some of the relatives referred to in the Article 416 of the Law on Criminal Procedure.

If, as we have stressed, the victim's testimony is fundamental, having in mind the special circumstance which are related to the commission of sexist violence acts, the inexistence of such a testimony, even though charges have been pressed previously, as a consequence of its use in later stages of proceedings such as exemption from Article 416 of the Law on Criminal Procedure, will determine, on one hand the absolution of the accused, and on the other, according to my opinion, which as a consequence is far more troublesome, the victim's complete lack of protection.

In the absence of the testimony, even with medical confirmation of the facts, medical expert or any medical documentation will only confirm the existence of physical injuries, or in some cases psychological damage, but, putting it bluntly, will only confirm the existence of the aggression, not its source.

That being the case, evidence must be provided against the perpetrator, in the lack of other direct witnesses who are not relatives, whom are rather difficult to obtain through witness' testimony, since the testimony itself with no other proof or evidence, cannot annul the presumption of innocence[10].

9 Sentences of the Supreme Court dated 3rd March and 26th October 2000.
10 Among others, Sentence of the Supreme Court dated 12th July 2007.

Another possible solution to the problem would be to read, upon request of any of the parties, the testimony, based on the Article 730 of the Law on Criminal Procedure[11], however, this possibility cannot be applied, and it is detailed so in Spanish Jurisprudence[12] as well as in the European Tribunal on Human Rights[13], since the mentioned article is only applicable in cases of the lack of a possibility to testify for other reasons than personal will of the witness, especially when the witness does not appear on trial, and not in the case of the use of right to be exempt from testifying, in particular, against the accused.

In relation to that, The General State's Prosecution has been faced with a significant number of charges withdrawn due to the fact that the gender violence victim during the trial refers to the exemption from the Article 416, which is why, as is pointed out by Martínez Mora[14], the judicial protection of the victim appears to be very difficult due to the concurrence of the mentioned article, which led to a large number of withdrawals in the year 2014, a total of 56,79 %[15], with a growth tendency since the year 2008.

THE FOUNDATION AND THE REACH OF THE EXEMPTION

What is the foundation of the exemption? Alcalá Flores[16] considers that it is found in the principle of not demanding a different conduct of that of being silent, due to the relation of solidarity which exists between the witness and the accused, a relation which is based on the constitutional protection of family relations[17] and the intimacy of any household[18]. We can notice the same view from the authors such as Aguilera De Paz[19], which sees the foundation of the exemption in the Natural Law, Moreno Catena[20], Magro Servet[21] or Escobar Jiménez[22].

In this case, the Law is also unanimous, understanding that the exemption could resolve a conflict which the witness could be facing such as to have to decide on whether to tell the truth or not to break the family bonds and the solidarity which relates him/her to the accused, *the witness often hides or denies to testify to the Court about the situation of abuse, out of love or out of other personal and family reasons*[23].

11 The Article 730 of the Law Criminal Procedure Act: *The testimony could be read to any of the parties involved in the case of any reasons other than personal will of the parties, which could prevent the reproduction of said testimony during trial, as well as testimony obtained in accordance with the Article 448 during the stage of the investigation of victims who are minors, or victims with any kind of disability and particular need for protection.*

12 Among others, the sentences of the Supreme Court dated 27th November 2000 and 17th December 1997.

13 Sentence of the European Court of Human Rights dated 24th November 1986, as. C-9120/80, Unterpertinger vs. Austria.

14 Martínez Mora, G., "La difícil protección judicial de la víctima de violencia de género. La dispensa del deber de prestar declaración del Artículo 416 de la Ley de Enjuiciamiento Criminal", *Bulletin of the Ministry of Justice*, 2015, p. 7.

15 Data from General Prosecutor's Office, 2014.

16 Alcalá Flores, R., "La dispensa del deber de declarar de la víctima de violencia de género: interpretación jurisprudencial", *III Observatory against gender violence meeting,* 2008.

17 Article 39 of the Spanish Constitution.

18 Article 18 of the Spanish Constitution.

19 Aguilera De Paz, E., *Comentarios a la Ley de Enjuiciamiento Criminal,* Madrid, 1924, p. 604.

20 Moreno Catena, V. M., *El secreto en la prueba de testigos del proceso penal***,** Marcial Pons, Madrid, 1980, p. 168.

21 Magro Servet, V., "La imposibilidad de conceder a las víctimas de la violencia de género la dispensa de declarar contra sus agresores (artículo 416 LECrim): ¿Es necesaria una reforma legal?", *La Ley,* 2005, p. 1701.

22 Escobar Jiménez, R., "La facultad de no declarar contra determinados familiares en el proceso penal (artículo 416.1º LECrim)", *La Ley*, 2009, p. 2.

23 Sentence of the Supreme Court dated 22nd February 2007.

Varela Castro[24] shares the same opinion and apart from that, adds that the above explained case should be implemented into the justice system alongside with the exemption of all penal responsibility which might come as a consequence of committing Concealment.

Finally, Marchena Gómez[25] refers to the more practical reasons, since the legislator understands that by insisting that the witness should testify and tell the truth, it still lacks the desired effects, having in mind that said witness should then oppose the family, it is necessary to implement more than an exemption from the obligation to testify, but to be exempt as well from the obligation to cooperate with the judiciary authorities. The need to stay silent is what protects the witness.

Keeping in mind the last opinion, Villamarín López[26] believes that the legal nature of the exemption is a subjective right, as well as a fundamental right, detailed in the Article 24 of the Spanish Constitution[27], which puts the relatives in a situation of privilege, compared to the other witnesses, granting them the right to decide whether or not they will testify in the presence of a family member, a right which originates from the right for personal and family intimacy, a line of thoughts supported by Castillejo Manzanares[28], Ortega Calderón[29] and Piñeiro Zabala[30] as well.

However, as the Supreme Court indicates[31], this authority does not permit the alteration of the truth, in the case of testifying, and being aware of one's rights not to have to testify, in which case the testimony will be incorporated, with all its legal consequences into the evidence material.

Sánchez Melgar[32] also mentions as a foundation of the exemption the reasons of pragmatic nature, since the pressures to any witness at telling the truth and the explanation of the consequences which may occur if such obligation is not fulfilled, do not have a desired effect when relatives are involved.

However, Sánchez Melgar also reflects upon something very meaningful, and that is that the witness should be informed about having the right not to testify against the relatives as well as the lack of an obligation to press charges, which has for a consequence the prohibition of evidence valuation.[33]

Besides that, the Supreme Court demands[34] that the witness should be warned that the application of the Article 416 of the Law on Criminal Proceedings is in force, which not only affects the judge but also the police, since its exclusion would be pointless having in mind that the objective of the Law is clearly defensive, and the judicial police always acts as a body delegated or representing the judge in terms of collecting evidence, and as is pointed out by our High Tribunal, *in order to resign one's rights, one should always be informed of having them. No one can resign on something they are unaware of.*

24 Sentence of the Supreme Court dated 26th March 2009.
25 Sentence of the Supreme Court dated 23rd March 2009.
26 Villamarín López, M. L., "El derecho de los testigos parientes a no declarar en el proceso penal", *Indret, Revista para el análisis del derecho*, 2012, p. 16.
27 In accordance with this doctrine, the action of not communicating to the witness the exemption of the testimony would harm the legal development of the proceeding.
28 Castillejo Manzanares, R., "La dispensa del deber de declarar del art. 416 de la Ley de Enjuiciamiento Criminal respecto de la mujer que sufre violencia de género", *Revista de Derecho Penal*, 2009, p. 135.
29 Ortega Calderón, J. L.,"La superación procesal del ejercicio por las víctimas de violencia de género de la dispensa legal de declarar", *La Ley*, 2007, p. 1070.
30 Piñeiro Zabala, I., "La víctima de violencia de género y la dispensa del artículo 416 de la LECrim", *Revista Jurídica de Castilla y León,* 2011, p. 98.
31 Sentence of the Supreme Court dated 23rd March 2009.
32 Sentence of the Supreme Court dated 10th May 2007.
33 In accordance with the articles 238 and 11.1 of the Constitutional Law of Judicial Authority.
34 Sentence of the Supreme Court dated 6th April 2001.

What is the reach of this right? First of all, we must point out that the judicial system is very passive when it comes to unmarried couples[35], when it is understood without saying that the application should be based on an analogy, since the legal system equalizes the two situations in every other case, such as for example the application in the circumstance of shared parenting, the domestic abuse, the concealment, or when it comes to the application of the absolution in regards to certain economic crimes[36].

Secondly, the legal system is also unanimous in regards to ending the determining relation of the existence of the solidarity principle which justifies the exemption, which is why the exemption is not to be applied in the case of a divorce or once the cohabitation of the union becomes *more uxorio*[37].

However, there are some resolutions in which the Supreme Court understands that if the foundation of the exemption is not solidarity, but rather family intimacy, it is necessary to extend the field of application of the exemption further to the existence of such a bond, since the mentioned intimacy is still affected, even after the termination of the inherent cohabitation[38], a criteria which is shared among authors such as Chozas Alonso[39], who refers to it as *ultra-activity of this authority,* while others, like Hurtado Yelo[40] have a completely opposite opinion.

THE EXEMPTION IN THE COMPARATIVE LAW. INTERPRETATION OF THE CONSTITUTIONAL COURT AND THE SUPREME COURT

What does Comparative Law state? In this case, Spanish legal system is quite similar to the Italian or French legislation.

In Italy[41], despite considering that the exemption is not applicable in the case when a witness is pressing charges as well as is a victim, it extends when a spouse testifies in regard to the events occurred during cohabitation.

Villamarín López[42] understands that the Italian doctrine bases the exemption on three reasons. First of all, that the one pressing charges has dealt with the internal conflict of wanting to protect the relative and having to testify, secondly, the contribution of the one pressing charges to the reconstruction of facts is of great importance, and finally, due to the fact that the violence the accused has committed breaks the unity and family solidarity.

In France[43], the exemption is also extended to beyond the family bond, and only refers to the obligation of taking the oath, in fact it is permitted to demand taking the oath if none of the parties is opposed to it[44].

35 Sentence of the Supreme Court dated 22nd February 2007.
36 Respectively, articles 23, 173 and 454 of the Penal Code, as well as the non-Judiciary plenary hearing held on 1st March 2005, in regards to the economic crimes described in the Article 268 of the Penal Code.
37 Among others, the Sentence of the Supreme Court dated 21st September and 5th October 2006 as well as 30th April 2007.
38 The Sentence of the Supreme Court dated 26th March 2009.
39 Chozas Alonso, J. M., *El interrogatorio de testigos en los procesos civiles y penales,* La Ley, Madrid, 2010, p. 341.
40 Hurtado Yelo, J. J., "¿Se debe suprimir el artículo 416 de la Ley de Enjuiciamiento Criminal en los delitos de violencia de género?", *La Ley Penal*, 2010, p. 40.
41 Article 199 of the Procedural Code.
42 Villamarín López, M. L., "El derecho de los testigos parientes...", *op. cit*., p. 8.
43 Article 448 of the Penal Code.
44 Piñeiro Zabala, I., "La víctima de violencia de género y la dispensa del artículo 416 de la LECrim", *Revista Jurídica de Castilla y León,* 2011, p. 109.

In the United Kingdom, however, it is understood that spouses are authorized to testify as witnesses, whether it is done based on the request of the defence or the one pressing charges and, specifically, when it comes to gender violence, in particular when there are victims younger than 16 years who live in the household, the mentioned authorization becomes an obligation. However, the spouses mutually accused are exempt of this obligation[45].

Quite contrary to this, in Germany, where the regulation of the exemption is absolute, in regards to the relatives of the accused, without any type of exception for victims or the ones pressing charges[46].

What is the opinion of our Constitutional Court? The Constitutional Court, on one hand, has decided that the cohabitation is not the reason for exemption based on the Article 416, but that the persons exempt of the obligation to testify can be both ones living in cohabitation with the accused or the ones who are not[47].

And on the other hand, when it comes to the interpretation of the exemption which is not specified to the victim[48], it is understood that such an obligation of instruction is just a formality when the victim offers solid evidence on which the charges are based on, which could turn into an implicit renunciation when the victim, advised by the attorney, decides to make particular accusations, where the sentence is concluded taking into consideration that the lack of exemption does not have to exclude the testimony on the trial in terms of evidence material.

Finally, in 2013, the Supreme Court seemed to have unified the different opinions on the matter, establishing, in accordance with the Agreement of non-Jurisdictional Plenum[49], that the exemption affects the persons who are or who have been united by some of the relations described in the Article 416, excluding two cases. In the first case, that the facts presented in the testimony have occurred after the termination of the marriage or after the termination of the cohabitation. In the second case, when the witness is the accused in the process.

For this reason, the problem of the exemption remains when the victim is united to the aggressor, whether it is by marriage or any other analogue relationship, in the moment of events occurring.

However, when it seemed that in 2013 the Supreme Court has made things clear, as is pointed out by Betrán Pardo[50], the sentence of the Supreme Court of July 14, 2015 *has reactivated the debate on whether it should be granted to a female victim of violence to have the indefinite possibility of having one or the other procedural status at the expense of her will.*

In the mentioned sentence, it is discussed on whether there is value in the testimony of a victim who, after reporting gender violence and pressing charges, after one year, renounces of any penal or civil actions, giving oral testimony, and stating that she is the former partner of the accused, without previously being offered the exemption.

The Tribunal, after mentioning the Agreement of 2013, points out that, one year after the private prosecution, even though after she renounces, she is excluded of the obligation to be informed of exemption, adding that the right to do so is annulled by the act of private prosecution, which puts her in the position of a normal witness and as such, there is no obligation of warning her, in which case the testimony is valid as an evidence.

45 Section 80 of the Police and Criminal Evidence Act 1984. Available at: http: //www.legislation.gov.uk/ukpga/1984/60/section/80
46 Martínez Mora, G., "La difícil protección judicial...", *op. cit*., p. 17.
47 Article of the Constitutional Court 187/2006, dated June 6th.
48 Sentence of the Constitutional Court 94/2010, dated November 15th.
49 Agreement on non-Jurisdictional Plenum of the Supreme Court, dated April 24th 2013.
50 Betrán Pardo, A. I., *A propósito de la última interpretación jurisprudencial del Tribunal Supremo sobre la dispensa del deber de declarar de las víctimas de violencia de género. Comentarios a la STS 449/2015, de 14 de julio*, Editorial Jurídica Sepín, 2015, p. 2.

The main problem which arises with this sentence is that it is unclear whether the mere fact of presenting oneself in the lawsuit, even if after follows the renouncement of the action, already supposes the inapplicability of the exemption.

With the interpretation being such, we must keep in mind that the majority of victims makes the decision to go into a lawsuit at the timeframe very close to pressing charges, when they are very much confused and with low self-esteem, feeling emotions which can change in a short period of time, due to which they can decide to withdraw the accusation, after realizing that the majority of judicial proceeding goes very fast. With the private prosecution of such low intensity is it enough not to demand the previous warning of exemption?

It must be emphasized that the sentence is in regards to a case in which the victim has made petitions under the private prosecution as many as five times, which does not happen in the majority of the cases which occur.

THE SOLUTION TO THE PROBLEM

This situation determines that it is necessary, from the point of view of various sectors, to demand the suppression or at least to delimit the exemption of the Article 416 in the case of the victims, and at the same time witnesses of gender violence, as is stated by the very Supreme Court[51]; the position of the victim in this process is of such importance that it cannot be left to arbitration, since that would assume the recognition of the lack of penetration of the Law in the area of the family, for prosecution of public crimes, a situation which is completely contrary to the objectives of the Integral Law of 2004.

This means that the legal system has, on the one hand, offered to the victim an integral protection, while on the other, it has put in front of her some of the major obstacles which stop that protection from being put into action.

In the same way the opinion of the State Observatory of Gender Violence[52] is presented, which reminds us that the foundation of the exemption is to respect the solidarity of the witness with regard to the accused, which commits a crime which does not put at risk his legal rights, which is not the case when it comes to gender violence.

Also, the State Prosecutors' Office indicates that we can either abolish the excuse for the crime victims, or prohibit that those regularly informed of it, who renounced it, take refuge in it[53].

Magro Servet[54], following the same line of thoughts, understands that the exemption from the Article 416 cannot be applied on the gender violence victims.

Finally, there is also a legal point of view which explains that the exemption should only be applied in the cases of witnesses who, being victims, are not also the part pressing charges[55], since the right from the Article 416 is renounceable, in regards to the witnesses, but not in regards to the spontaneous complainant when it comes to the facts which are harmful, and which require police protection.

This doctrine indicates that the right to exemption should be advised to a relative who testifies before the Magistrate, within the process of the investigation, but it is not obligatory to do so when a person seeks police assistance.

51 Sentence of the Supreme Court, dated January 25th 2008.
52 Annual Report of the State Observatory of Gender Violence, dated June 28th 2007.
53 Report of the General Prosecutor of the State 2008.
54 Magro Servet, V., "La imposibilidad de conceder...", *op. cit*., p. 1708.
55 Sentences of the Supreme Court dated July 12th 2007 and February 20th 2008.

As a solution to the problem, a special attention should be paid to the proposal of the Group of Experts in the area of Gender and Domestic Violence of the General Legal Counsel[56] who suggested the introduction of the new Article 730 of the Law of Criminal Proceedings, which creates a possibility, at the request of any of the parties, to read, during the trial, the testimonies from the witnesses as well as victim's testimony, in order to waiver of testifying based on the Article 416 of the Law of Criminal Proceedings.

In my opinion, to the above mentioned reading of the testimony during the Trial, one should add the incorporated evidence material of the testimonies of the relevant witnesses, such as police officers who have seen the victim's situation first hand. These kind of relevant testimonies, alongside the rest of the gathered material, such as non-compulsory assistance, forensic report and other evidence, like previous testimonies of the neighbours to the police, or police investigatory reports in regards to the victim and the victim's surroundings, without a doubt could serve as a valid argument before the judicial authority which can weaken the presumption of innocence of the aggressor.

For all the above mentioned reasons, I believe that it is of the upmost importance to provide all of the information possible during the testimony before the police officers, who are the first to intervene, which makes them direct witnesses of the ambience which surrounds the aggression and other related consequences, and they must be, without a doubt, taken into consideration by the judicial authority, at least as a circumstantial proof, in order for the Trial to obtain its goal of reaching the truth .

It is also important to underline the importance of the victim's testimony, gathered during the police statement, at the time so close to the violence occurred.

We should also stress the importance of the testimony given in the police statement having as many details as possible, since in many occasions that very testimony is the only one with effect in the phase of preliminary investigation, allowing the victim the ratification before the judicial authority.

Besides, as we have already pointed out, in the cases of the victim withdrawing her testimony in the act of oral hearing, the legal system allows the valuation of summary testimonies, or even, which is the main topic of our thesis, the testimony made in the police headquarters, as is clearly elaborated by the Supreme Court[57], due to its spontaneity and closeness to the incident.

On the other hand, regardless of whether the victim on her own initiative presses charges, or if she is accompanied by the police, before testifying, she should receive the medical assistance, in the case of injuries.

This kind of assistance should always be offered to the victim before taking her testimony. In the case of injuries occurring, the victim should be accompanied to the medical institution by the police officers and after being attended by a physician, that physician should, in accordance with the Protocol on medical assistance in the gender violence cases[58], make an official report which is to be included in the police report.

This part is of vital importance, as I have already pointed out in regards to the issues of evidence when it comes to this type of crimes, assuring at least a documented proof of the existence of injuries, which as was mentioned before, does not define the perpetration of them.

56 Report dated January 11th 2011.
57 Sentences of the Supreme Court dated April 29th 2009, May 14th and January 15th 2008, dated April 10th 2007 or February 3rd 2006.
58 The Joint Protocol on medical assistance in the cases of Gender Violence, approved by the Interterritorial Council of the National Health System, during a meeting held on December 20th 2012, available at: http://www.msssi.gob.es/ssi/violenciaGenero/violenciaGenero/protocoloActuacion/ambSanitario/home.htm.

In the case of a victim, despite of having visible injuries, refuses to be transported to the medical center, as is defined by the Protocol, it should be stated in the report, acting with consideration, that the injuries were noticeable and a victim should be kindly asked to allow for those injuries to be photographed, so that they can be added to the testimony.

In my opinion, these photographs are also of vital importance, due to the fact that with the lack of the medical report, they can be used as documented proof of the existence of injuries and in the case of a victim refusing to allow taking of those photographs, the report should, without a doubt, include a statement of the police officers, as witnesses of external indicators of aggression, as well as their statement of the overall condition and appearance of the victim, a report similar to the experts' report[59] which could be used in the future stages of the process as a proof of the existence of abuse, even in the cases of the victim refusing to testify.

To conclude, as long as the Integral Law sees the victim, by the words of Piñeiro Zabala[60], as one of the pillars of the legal proceedings, as the main source of the *notitia criminis*, while on the other hand she is included as an integral part, as is well pointed out by Rodríguez Lainz[61], of a process stuck in the XIX century, constantly modified in order to adjust itself to the current reality, it is necessary to proceed to the amendment of the Article 416 of the Law on Criminal Proceedings, in accordance with the meaning we have seen in other legislations of comparative law , in order to be able to offer to the victim an integral protection, foreseen by the Constitutional Law 1/2004, since with the current composition it is impossible to protect the one who refuses to be protected.

REFERENCES

1. Agreement on non-Jurisdictional Plenum of the Supreme Court, dated March 1st, 2005.
2. Agreement on non-Jurisdictional Plenum of the Supreme Court, dated April 24th, 2013.
3. Aguilera De Paz, E., *Comentarios a la Ley de Enjuiciamiento Criminal,* Reus, Madrid, 1924.
4. Alcalá Flores, R., "La dispensa del deber de declarar de la víctima de violencia de género: interpretación jurisprudencial", *III Congreso del Observatorio contra la Violencia Doméstica y de Género*, 2008.
5. Annual Report of the State Observatory of Gender Violence, dated June 28th 2007.
6. Auto of the Constitutional Court 187/2006, June 6th.
7. Betrán Pardo, A. I., A propósito de la última interpretación jurisprudencial del Tribunal Supremo sobre la dispensa del deber de declarar de las víctimas de violencia de género. Comentarios a la STS 449/2015, de 14 de julio, Editorial Jurídica Sepín, Madrid, 2015.
8. Castillejo Manzanares, R., "La dispensa del deber de declarar del art. 416 de la Ley de Enjuiciamiento Criminal respecto de la mujer que sufre violencia de género", *Revista de Derecho Penal*, 2009.
9. Chozas Alonso, J. M., *El interrogatorio de testigos en los procesos civiles y penales*, La Ley, Madrid, 2010.
10. Escobar Jiménez, R., "La facultad de no declarar contra determinados familiares en el proceso penal (artículo 416.1º LECrim)", *La Ley*, 2009.

59 As was already analyzed in the headings related to the issue of intelligence expertise, these reports should reflect not only the facts, but also knowledge of the matter of the officers specialized in gender violence who could contribute by adding relevant elements important for the overall retrospective of the incident, which will be presented to the legal authority.
60 Piñeiro Zabala, I., "La víctima de violencia de género..." *op. cit*., p. 110.
61 Rodríguez Lainz, J. L., *Juzgado de Violencia sobre la Mujer y Juzgado de Guardia*, Bosch, Barcelona, 2006, quoted by the previous author.

11. French Criminal Code, Article 448.
12. General Prosecutor of State. Report from 2008.
13. General Prosecutor of State. Report from 2014.
14. Government Delegation for Gender Violence (Ministry of Health, Social Services and Equality). Available at: http://www.inmujer.gob.es/estadisticas/violencia/victimasMortalesI/2012/w809.xls.
15. Group of Experts in the area of Gender and Domestic Violence of the General Legal Counsel. Report dated January 11th 2011.
16. Hurtado Yelo, J. J., "¿Se debe suprimir el artículo 416 de la Ley de Enjuiciamiento Criminal en los delitos de violencia de género?", *La Ley Penal*, 2010.
17. Italian Procedural Code, Article 199.
18. Joint Protocol on medical assistance in the cases of Gender Violence, approved by the Inter-territorial Council of the National Health System, during a meeting held on December 20th of 2012. Available at: http://www.inmujer.gob.es/estadisticas/violencia/victimasMortalesI/2012/w809.xls.
19. Law 35/1995, 11th of December, about Aids and Assistance for Violence Offenses and Offenses against Sexual Freedom Victims.
20. Legislative Royal Decree 1/1995, 24th of March, based on which the Consolidated Text of the Legal Statute of Workers was approved.
21. Legislative Royal Decree 1/1994, 20th of June, based on which the Consolidated Text of the General Social Security Act was approved.
22. Magro Servet, V., "La imposibilidad de conceder a las víctimas de la violencia de género la dispensa de declarar contra sus agresores (artículo 416 LECrim): ¿Es necesaria una reforma legal?", *La Ley,* 2005.
23. Martínez Mora, G., "La difícil protección judicial de la víctima de violencia de género. La dispensa del deber de prestar declaración del Artículo 416 de la Ley de Enjuiciamiento Criminal", *Boletín del Ministerio de Justicia*, 2015.
24. Moreno Catena, V. M., *El secreto en la prueba de testigos del proceso penal*, Marcial Pons, Madrid, 1980.
25. Organic Law 1/2004, about the Integral Protect against the Gender Violence, dated December 28th
26. Ortega Calderón, J. L., "La superación procesal del ejercicio por las víctimas de violencia de género de la dispensa legal de declarer", *La Ley*, 2007.
27. Piñeiro Zabala, I., "La víctima de violencia de género y la dispensa del artículo 416 de la LECrim", *Revista Jurídica de Castilla y León,* 2011.
28. Police and Criminal Evidence Act, Section 80, 1984. Available at: http: //www.legislation.gov.uk/ukpga/1984/60/section/80.
29. Rodríguez Lainz, J. L., *Juzgado de Violencia sobre la Mujer y Juzgado de Guardia*, Bosch, Barcelona, 2006.
30. Sentence of the Constitutional Court 94/2010, dated November 15th.
31. Sentence of the European Court of Human Rights, dated 24th November 1986, as. C-9120/80, Unterpertinger vs. Austria.
32. Sentence of the Supreme Court dated March 3th 2000.
33. Sentence of the Supreme Court dated October 26th 2000.
34. Sentence of the Supreme Court dated April 6th 2001.

35. Sentence of the Supreme Court dated September 21st 2006.
36. Sentence of the Supreme Court dated October 5th 2006.
37. Sentence of the Supreme Court dated February 22nd 2007.
38. Sentence of the Supreme Court dated April 10th 2007.
39. Sentence of the Supreme Court dated April 30th 2007.
40. Sentence of the Supreme Court dated May 10th 2007.
41. Sentence of the Supreme Court dated July 12th 2007
42. Sentence of the Supreme Court dated January 15th 2008
43. Sentence of the Supreme Court dated January 25th 2008.
44. Sentence of the Supreme Court dated February 20th 2008.
45. Sentence of the Supreme Court dated May 14th 2008.
46. Sentence of the Supreme Court dated March 23rd 2009.
47. Sentence of the Supreme Court dated March 26th 2009.
48. Sentence of the Supreme Court dated April 29th 2009.
49. Sentence of the Supreme Court dated March 21st 2011.
50. Spanish Constitution dated December 29th 1978.
51. Spanish Criminal Procedure Act dated September 14th 1882.
52. Villamarín López, M. L., "El derecho de los testigos parientes a no declarar en el proceso penal", *Indret, Revista para el análisis del derecho*, 2012.

UDC: 314.15(4)
314.113:323.14/.15
005.334:314.15

MODERN MIGRATIONS AND DIVERSITY OF CONFLICT PARADIGM[1]

Srđan Milašinović, PhD[2]
Academy of Criminalistic and Police Studies, Belgrade
Zoran Jevtović, PhD
University of Niš, Faculty of Philosophy

Abstract: By careful analysis of important trends, phenomena and processes that characterize modern migration in the European context, the authors focus on the emergency crisis management and address the national audiences, attempting to construct the dominant model of conflict paradigm using a comparative analysis of public discourses. Noting the transformation of migration policies and changes in the structure of the migration, a complex security framework and the importance of communication control and information management has been indicated, and, if not, in certain parts of the European Union moral panic and chaos may spread. Critically reviewing the current changes the authors extracted their economic, conditionally organized and targeted resettlement, which will produce long-term tectonic earthquakes in the countries of immigration. Some adaptation and acculturation transformations might be visible, rapid and painful changes of disjunctive complex process, typically leading to further conflict and contradiction. The analysis is focused on the phenomenon of ethnic stratification that would eventually expand the social distance between the majority and minorities, such as the disharmony within the social processes and between them. As the idea of multiculturalism diminishes, a deepening in internal, religious, ethnic and interclass difference will occur, which is essential for effective and efficient management during the emergency crisis or potential conflicts.

Keywords: migrants, crisis, migration policy, management, public relations, conflictology, security.

INTRODUCTION

Migrations in their diverse manifestation forms have always represented an important safety factor, but only with the processes of training of communication tools, the rising geo-political, demographic and socio-economic interdependence have become trans-regional networked, organized, dynamic and massive, threatening with migrations of entire populations, cultures and religions. They are still being globally a hot topic, as the rapid changing of ethnic, religious and cultural characteristics of the population of many countries may lead to new clashes with unforeseen consequences. The problem is most pronounced in Europe that

1 The paper was written under the Project No. 179008, implemented by the University of Belgrade – Faculty of Political Sciences, and the University of Niš – Faculty of Philosophy as well as Project No. 179045 (The Academy of Criminalistic and Police Studies), which is funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia.
2 E-mail: srdjan.milasinovic@kpa.edu.rs.

without a single migration policy, security and intelligence procedures allows member states improvisations, so that the overall security system becomes porous and vulnerable to possible excesses, including acts of terrorism, such as the one on November 13 in Paris.[3]

The outlines of migrant ripples could be seen at the beginning of century, when there were more than 150 million migrants worldwide, of which about 20 million accounted for refugees. In 2013 there was a tremendous acceleration of migration flows and the increase of this numbers to over 214 million, while data processing for 2015 show much higher final number. Current trends indicate that during 2016 the number of refugees in Europe will increase by three million people, indicating the potential change of the security context. Migrations, through turbulent processes of violent political changes and ideological fractures, created "Arab Spring", military intervention and the growing gap in wealth redistribution only imploded, so that unrest and instability of regime in Syria, Iraq, Somalia, Lebanon, Afghanistan and other countries additionally encouraged a process, which like a wave overflows to neighbouring countries and continents. Hence, the ethnic composition of the population of the European Union changes daily, so, for instance, Germany has almost 10 million new inhabitants, France close to eight million, Spain more than six million. It is important to notice that an uncontrolled influx of economic migrants, combined with the increasing number of refugees fleeing conflicts in Africa and the Middle East leads to the escalation of xenophobic reaction in countries that are being hit by a growing influence of right-wing parties. Conflictological paradigm shows how fast and unprepared changes of the structure of the population usually lead to the change of traditional social and cultural relations, identity, values and patterns. Also, the practice shows that all of those are not of the same importance for the stability and the internal dynamics of the community.

Decades of experience of many European countries and the United States show that it is possible to gain significant economic and social benefits, to stabilize economic growth and the development of pluralist democracy, but if the migration is uncontrolled, it may fall into the range of social, political and security conflicts. The new world order is increasingly based on the establishment of peace and peaceful relations among members of the international system, and the ways of its implementation represent the replacement of political power with the concept of collective security, which would ensure the establishment of peace based on the principles of cooperation and trust.[4] Hence, the subject of our research – the crisis of migrants is not an issue made by individual countries; it is a priority concern of each of the member states, but also all the members together, because it is a question of the stability of the overall social relations and territorial internal security. In a broader platform, we see that its solution is hard to imagine without the active involvement of NATO and United States, as partners in the creation of a common strategy for a long-term problem solution. Coordination and concerted management[5] of migration routes have become the foundation of a proactive approach, which would ensure full control of the entire process and reduce the risk to security of both the migrants themselves and the European Community.

3 In one of the worst terrorist attacks at European soil, in France, around 130 people attacked in a restaurant, the national stadium and concert hall were killed.
4 See in: Bajagić, M.: *Međunarodna bezbednost*, Beograd: Kriminalističko-policijska akademija, 2012, p. 167.
5 Kešetović and Milašinović see the risk management as a proactive part of crisis management, which is in turn part of a broader process of management uncertainties. "Going from certainty to uncertainty, the potential risks are growing. To the extent that it is not controlled, uncertainty governs us, leading to the field of crisis management, followed by the disaster management" See in: Krizni menadžment i slični koncepti – pokušaj razgraničenja, *Bezbednost*, 2008, p. 54.

MIGRATION OR SPATIAL MOBILITY

Contemporary sociology theoretically differentiates concepts of *migration* and *spatial mobility*, which is important for creating the conflictological paradigm. In practice, each migration refers to the movement of people, but at the same time every movement does not necessarily represent the migration. António Manuel de Oliveira Guterres, the head of the United Nations Refugee Agency, singled out the climate change, more explosive growth of the world population, urbanization, lack of food and water and the struggle for natural resources as causes of mass population displacement. "The world produces displacement faster than solutions", noted a senior UN official: "That means only one thing: a higher number of people caught in the trap of exile for many years, without being able to return home, to integrate into new environments or to move to another place. In general, global displacement is an international problem that requires international solutions, and thus, I primarily think of a political solution".[6]

By watching the European Union as a space, one can notice that the majority of flows of displacement leads to certain countries in the center, while the periphery and underdeveloped parts are not subject to interest of newcomers. Conflictologically, traces of *theory* could be perceived, developed by Kenneth Boulding[7], starting from the premise that the mental capital of individuals and groups determine the performances that are adopted from the early childhood socialization processes. In crisis situations, this means that migrants choose, for example, Germany, France or the Scandinavian countries, caused by the rooted media representations of these environments in their minds as rich, open and democratic communities that will gladly accept them. It is evident that today's migrants use their mobile phones, social networks or accompanying multimedia. As a new element we can see that they are well organized, often financially secured and routed to specific destinations. Without prejudice to the consensus on the sovereign right of states to control immigration, and that this right is not disputed either by the International Organization for Migration IOM or UNHCR, nor any other prominent and influential organization or research institute, we see that in the case of migration of entire communities, a dilemma of limitations of immigration policy occurs, with the growth of potential inter-ethnic conflicts.

In terms of terminology, here arises the duality that hides different meanings, often producing discourse of negative stereotypes and prejudices in the public. Displaced populations are usually divided into two groups: first, the *refugees* that receive the status by the UNHCR or the country to which they move. Usually these are people who come from refugee camps, running from political persecution, violence, armed conflict, natural disasters and similar events. However, there are also *migrants*, groups consisting of individuals crossing the border and seeking asylum in order to improve conditions of personal life, from education to better paid job or merging with previously displaced family members. For easier moving they often pose as refugees, as it is difficult to verify in the mass of people who come every day to some area. In the complex administrative process of determining the status of these people and checking the justification of their demands, governments have a moral obligation to, until not proven otherwise, accept these people and treat them as refugees. "Otherwise, if those people were immediately deported to the countries of their origin, countries would be directly responsible for their fate, especially if those people were really in danger of persecution on

6 *The increase in the number of displaced persons in the world*, UNHCR, United Nations High Commissioner for Refugees, 08/26/2015. Available at: http://www.unhcr.rs/dokumenti/saopstenja-za-medije/porast-broja-raseljenih-svetu.html.
7 Boulding, K.: *The Image: Knowledge in Life and Society*, Ann Arbor : University of Michigan Press, 1956, p. 142.

the ground of which they have sought the asylum".[8] This distinction is important, because the refugees are protected by international law and the states have an obligation to help them and to protect them, while the migrants are treated in accordance with migration policy that each country leads according to its legislative orientation.

In further analysis, we consider migration as a permanent change of residence, and we distinguish the term in a more narrow sense (*final migration*), meaning the resettlement of a persons from the previous place of usual residence to the place of immigration or a new place of permanent residence (permanent relocation). The migration necessary meets two criteria:

- during the process of moving, a crossing of a certain, significant line of the relevant administrative-territorial units;

- the case of a long-lasting change of the place of permanent residence.[9]

Current international migrations are characterized with perspective of social networks, made of dense interpersonal and group relationships that organize migrants and non-immigrant population in areas of origin and destination, over the relations of kinship, friendship or membership in a particular environment. These networks between countries of origin and destination act in order to reduce the financial and psychological risks of migration, by increasing the level of awareness and the likelihood of successful completion of the entire operation. However, as a novelty in recent migration (in)to the European Union it is observed that highly educated and skilled population create a wide range of different forms of relationships, exchanging information on routes, destinations and modes of their acceptance by the local population, thus making potential routes of movements that are rapidly transformed and adapted to the changed conditions. It is no longer only connection of friends and relatives, but also the intelligence, professionally organized mass movements of population that receive a number of specific guidelines of already established procedures that can help not only the decision of migration, but also in various stages of crisis treatment. Contemporary migration flows are limited by space-time dimension, with communicationally-trained managing of the process of relocation.[10] The emphasis is on a permanent communication of actors (mobile phones and GPS citing), financial logistics (foreign remittance accompanying them during the journey), and the support of previous migrants by pointing out the weak points of the corridor allow the successful functioning of the network.

ADVANTAGES AND DISADVANTAGES OF MIGRATION PROCESSES

By analyzing the contemporary migration, we have concluded that they are not a short-term problem, as the layman thinks, but a long-term process that will only grow. If the current birth-rates remain, in only two decades, the population of Europe would be considerably reduced. In the year 2035, it would be (in relation to the end of 2015) lessen by 54 million (from 737 to 683), whereby the decrease would mainly be related to the eastern part (45 million), and to a much lesser extent in western countries (9 million). Transitional state, according to

8 Đorđević, B.: Etika migracije, *Godišnjak Fakulteta političkih nauka*. Beograd: Fakultet političkih nauka, Vol. 2, No. 2, (2008), pp. 244–245.

9 See in: Penava, M.: Utjecaj krize na imigracijsku politiku EU. Zagreb: *EFZG Occasional Publications*, No.1 (2011), pp. 113–128.

10 "Social networks are basically modified distribution channels of content, but are at the same time the means of design and publication of information organized through nodes and links", say Milašinović and Jevtović. They are essential for providing social and emotional support, but also as "a source of information that allows establishing and maintaining relationships with other people" (2013; 135–136).

this projection, would have reduction from 320 million to 275 million, meaning that, in only half of a century, the lost would be counted to the fifth of the population

In the case of the countries of Eastern and Southeast Europe as a reason we can accept a transitional poverty, which led to the decreased of natality, and the opening of borders and immigration, primarily to the west of the continent. As a result we get the fact that from 1990 to 2011 in twenty countries in transition, the number of residents decreased by 21 million, while at the same time the number of residents of the so-called non-transitional states increases for 36 million people. In two decades between the two parts of Europe, a difference of 57 million inhabitants was created. The ratio of increase and decrease of population is illustrated in the following table:

Table 1: *Total population movements in the period 1990–2011.*[11]

1990–2011.	Пораст – смањење бр. становника	Природни прираштај	Миграциони салдо
Аустрија	+714.000 (9,3%)	+96.000 (1,2%)	+618.000 (8,1%)
Велика Британија	+6.011.000 (10,5%)	+2.782.000 (4,9%)	+3.229.000 (5,6%)
Грчка	+946.000 (9,3%)	+58.000 (0,6%)	+888.000 (8,7%)
Италија	+2.660.000 (4,7%)	-272.000 (-0,5%)	+2.932.000 (5,2%)
Немачка	+2.365.000 (3%)	-2.387.000 (-3%)	+4.752.000 (6%)
Норвешка	+712.000 (16,8%)	+330.000 (7,8%)	+382.000 (9%)
Француска	+6.514.000 (11,5%)	+4.829.000 (8,5%)	+1.685.000 (3%)
Шпанија	+7.892.000 (20,3%)	+1.267.000 (3,3%)	+6.625.000 (17,1%)
Швајцарска	+1.197.000 (17,8%)	346.000 (5,1%)	+851.000 (12,7%)
Шведска	+890.000 (10,4%)	+237.000 (2,8%)	+653.000 (7,6%)
Албанија	-473.000 (-14,5%)	757.000 (23%)	-1.227.000 (-37,5%)
Бугарска	-1.370.000 (-15,7%)	-779.000 (-8,9%)	-591.000 (-6,8%)
Мађарска	-402.000 (-3,9%)	-740.000 (-7,1%)	338.000 (3,3%)
Пољска	-48.000 (-0,1%)	+790.000 (2,1%)	-837.000 (-2,2%)
Румунија	-3.054.000 (-13,2%)	-648.000 (-2,8%)	-2.406.000 (-10,4%)
Русија	-5.013.000 (-3,4%)	-13.039.000 (-8,8%)	8.027.000 (5,4%)
СРБИЈА	**-585.000 (-7,5%)**	**-461.000 (-5,9%)**	**-125.000 (-1,6%)**
(Косово и Метохија)	-133.000 (-6,9%)	+664.000 (34,4%)	-796.000 (-41,3%)
Украјина	-6.102.000 (-11,8%)	-5.585.000 (-10,8%)	-517.000 (-1%)
Хрватска	-494.000 (-10,3%)	-122.000 (-2,5%)	-373.000 (-7,8%)

The data clearly show that the western part of the continent as a whole or for the most part shows positive trends, while the east is mainly in red, minus "zone". In these parts, the greatest percentage of depopulation stand out for Latvia (23%), Lithuania and Moldova (18%), as these countries' population decreased for the fifth in just two decades. Geopolitical projections combined with demographic indicators warn that many areas in Eastern Europe remain empty or even devastated in population. In addition, it will have an extremely unfavourable age structure, becoming an elderly population. Hence the powerful states in the long run solve their problem by accepting skilled and educated young workforce.

In order to understand the migration processes in the context of the overall European picture, it is necessary to know where the causes of the fear of the locals are hidden. In 2014, 122 million people or 24.4% of the European Union population were at risk of poverty or so-

11 "Tri mape za dve Evrope". *Politika*, 5. May 2015.

cial exclusion, stated by the National Statistical Offices – Eurostat. A risk-of-poverty rate was the highest in Romania, and the lowest in the Czech Republic. More than a third of the population in the three countries of the EU was at risk of poverty or social exclusion (Romania with 40.2%, Bulgaria with 40.1% and Greece with 36%). In contrast, the lowest rate-of-poverty rates were registered in the Czech Republic (14.8%), Sweden (16.9%), the Netherlands (17.1%), Finland (17.3%) and Denmark (17.8%). The largest decrease in that rate was recorded in Poland, while the highest growth was recorded in Greece.[12]

These data are important if we further analyze the possibilities and potential benefits of a wave of refugees. For example, Germany will provide the provincial and municipal authorities 670 euros monthly from the federal budget for every asylum seeker. The government agreed to reroute to the provinces at least 3.7 billion euros to cover the costs of accommodation, while in 2016 around four billion euros will be given. The refugee crisis has been a huge burden on the budget in Austria, and the Minister of Finance calculates that the cost of supplying the refugees will be around one billion euros. Each refugee, according to the calculations of the Ministry of Finance, costs the government an average of 10.724 euros. Despite the increase in costs for the reception of migrants, the major western countries say there is no reason to panic. German Institute for Economic Research has calculated that a migratory public spending will further increase the economic growth of Germany by 0.25%, which means even more government revenue. In addition to these benefits, the business elite points out that the admission of refugees will have a long-term financial gain to Germany, as, if they are fully integrated, they can decisively contribute to the maintenance of standard of living and to ensuring pensions and social benefits of the elder population. The government's policy is that refugees are not allowed to stay at the expense of the state, but to learn language and business skills in order to integrate into the local labour market supported by the largest German corporations, having a chance to maintain a low cost of labour, together with the production increase.

From the perspective of demography, we note that labour migration helps developing not only host countries but also the countries of origin of migrants. Martin Schulz, President of the EU Parliament, at the World Economic Forum in Davos, dedicated to the problem of migration, said that the biggest problem is that politicians in Europe only register migration problem as a phenomenon, "but do not manage it well". "We lack the legal system and norms for regulation of migration, both working as well as those of a refugee type. If we had those norms, such as America, many things would be clearer, easier and simpler. Thus we have no EU quotas for immigration, we have no rules, and this is where politicians failed. On the other hand, if the importance and necessity of labour migration was not explained by the voters, it is normal that the vacuum would be utilized by populists and say 'we do not need migration'. That's a lie. Look at the demographics of Europe. It is getting old. We need young population, consumers and population capable to work."[13]

Conflictologists have noticed long before that all inter- and intra-conflict transitions are preceded by several stages: "social distance and the conflict situation on the basis of which a conflict is created. If it does not stop properly (in terms of consensus, dismissal or termination) and with the appropriate means, there is a possibility for his focus and escalation."[14] It is certain that the mass movement of populations from Syria, Afghanistan, Iraq and other

12 One fourth of EU residents have a risk of poverty. *Tanjug*, October 17, 2015. Available at: Radiotelevizija Vojvodine, http://www.rtv.rs/sr_ci/ekonomija/globus/cetvrtina-stanovnika-eu-u-opasnosti-od-siromastva_649552.html.

13 WEF Davos: Beg od siromaštva i problem migracija. Beograd: *Mesečnik Biznis & Finansije,* 22/1/2015. Available at: http://bif.rs/2015/01/wef-davos-beg-od-siromastva-problem-migracija/.

14 Milašinović, R., Milašinović, S., Putnik, N.: *Teorije konflikata*. Beograd: Fakultet bezbednosti Univerziteta u Beogradu, 2012, p. 180.

countries of the Middle East lead to the changes of ethnic and religious structure of the states of inhabitation, which in perspective leads to a change in the security paradigm at a part of the migrants who participated in previous conflicts become possible terrorists. Uncontrolled migration reshapes the geopolitical space of Europe and radically transforms the ethnic, religious and cultural relationship, but the consequences will be seen over time.

MIGRATION AND MEDIA INTERPRETATION

Migrants, asylum seekers, irregular migrants, refugees, migrants, illegal migrants, immigrants, illegal immigrants – these are all terms that the media use to indicate hundreds of thousands of people fleeing the wars fought in the countries of Asia and Africa, pass the Balkan corridor seeking refuge in the European Union. The crisis management means that the potential threats are being identified, targeted and conceptually formed, as it is the only way to get the public consent for the prompt and proactive action. In other words, the terminological definition of social groups in crisis situations has ideological interest. The term migrant is impersonal. It hides some ambiguity, so it conceals the fact that we have a problem with a large influx of refugees.

Parallel use of the terms "migrants" and "refugees" in a crisis situation is not only a product of professional ignorance (journalists) or social ignorance of the situation (the public). Numerous international organizations or major media outlets transmit a political assessment of the influential members of the elite, marking the same time both terms, as it spills security problem.[15] In word of international institutions, term migrant is a broad term – includes asylum-seekers and refugees, and among the people (referred to in this case), there are both. In the propaganda tone the social disorganization and disintegration of entire countries and peoples are lost, thus contributing to the escalation of the crisis to other territories. Leading representatives of the social disorganization, A. Elliott and F. Merrill,[16] define the phenomenon as disorders in social communication. They indicate the levels of its manifestation, establishing that reporting formalism on public speaking is the first level of disorganization, to which, then, built confrontation leads to a complete loss of social consensus. American theorists have noted that in the crisis situations an unclear conceptual category can easily be politicized, so in our everyday life a part of the extreme-oriented media may use the term "economic migrants", emphasizing that waves of people come to Europe for business or economic benefits, which increases the xenophobia and the risk of new confrontation. Hence the designation of refugees as migrants is not only a question of vocabulary, but becomes "renaming of their problems and responsibilities that politicians of the corridor countries or destination countries, have to solve".[17]

CONCLUSION

The analysis of total migration flows towards the European Union at this time was not done, but it is clear that it should include a range of very different issues. For security assessment, in addition to the quantitative aspects (statistical study of the number of migrants

15 Babar Baloh, a spokesman for UNHCR, Radio Free Europe said that, "in Hungary in this year 90.000 people applied for asylum, of which 60.000 came from Syria, Iraq, Afghanistan and Pakistan." From this it is more than clear that this is not a migrant, but the refugee crisis.

16 Elliott, A., Merrill, F.: *Social disorganization*. New York: Harper and Brothers, Publishers, 1961.

17 Service for legal protection of the UNHCR Belgrade office. Why media Refugees converted to migrants, Cenzolovka, 13/8/2015. Available at: https://www.cenzolovka.rs/iz-prve-ruke/zasto-medijiizbeglice-pretvaraju-u-migrante/.

and the reasons for relocation, migration flows, the length of their movement and types of migration according to their size), a special attention should be given to the demographic and security aspects and the issue of selectivity of migrants according to different characteristics (gender, age, profession, education, etc.), the study of demographic, economic and social aspects of migration flows, as well as many other issues. If the migrants are males, younger age, militarily trained, with experience in conflict, it is clear that the security policy of the country of immigration must be urgently transformed in accordance with the migratory changes. Population inflow influences the population growth, and thus the assessment of the security risk.

We should not neglect the fact that more than two-thirds of the current migrants in Europe are Muslims, which have been slowly integrated into domicile cultural patterns, especially the Christian community. They almost do not accept European values and habits, and are often not able to fit in the larger culture, adhering to religious beliefs and traditions – from customs and diet, through clothing, behaviour and moral norms, to the general behaviour and the role of women and families.[18] These problems are passed from generation to generation as young people living in migrant ghettos attend expensive schools, socialize with each other, are often separated from the broader community, and remain unaccepted and disoriented, searching for identity in connecting to groups of Islamic extremists who lurk these persons with powerful media propaganda.[19] The consequences are manifested in different ways: by provoking riots in the streets and throwing bombs in subways, through open funding or showing sympathy for terrorist groups, to the growth of antagonism towards the natives. At the same time, in Europe we have a growth of suspicion towards Muslims in general, fear of religious radicalism, and the open forms of hatred and discrimination.[20]

Well managed migration can bring genuine benefits to all participants of the migration. However, for the ultimate success, a necessary dialogue and cooperation with non-EU countries and international organizations is a must. Multilateral policy of migration management (Europe, USA, NATO, Russia, and countries of crisis), in our opinion, represents the only way out of the current crisis situation. There is no simple or single answer to the challenges that arise from migration. Also, no Member State can solve the problem alone. "It is obvious that we need a new, pro-European approach to tackling the crisis."[21]

Sociological challenges and turbulence of social trends are visible in changing the character of migration, because with the new transnational character the classic traits of previous forms of migration are being complemented and transformed. Migrations of entire populations across the borders of third countries now receive transnational forms. To some extent, the structure of the population was changed, but also cultural and value patterns, impacting on national identity that is increasingly adapting to global environment. The idea of pot

18 For example, out of nearly 140 Turkish immigrant women who were interviewed in the German Federal Ministry for Family Affairs, every second said that her husband was chosen by her family, and every fourth that she did not know her husband before marriage. See in: Malešević, M.: Hrišćanski identitet sekularne Evrope. Beograd: *Glasnik Etnografskog instituta SANU*, book. 55, (1), (2007), p. 12.

19 Jevtović, Z. i Aracki, Z.: Požar islamskog fundamentalizma i ćutanje Zapada, *Viteška kultura*, Beograd, 2015, p. 232.

20 The latest research of the American "Pew" center, conducted in July 2015 on a sample of 21.235 people in 21 countries, showed that the fear of radical Islamists is growing around the world, and compared to 2011 the percentage of those who declared themselves to be scared of terrorists rose to 21%. Fear is most evident in France (increased from 29% to 67%), in Spain (from 32% to 61%), Germany (from 26% to 46%) and in the United States from 36% to 53%. The research also showed that fear is growing not only in western countries but also in those with a majority of Muslim population, mostly in Nigeria, Lebanon, Pakistan, Palestine and Turkey. Source: *Blic online*, Ove zemlje se najviše plaše islamista, 22/7/2015. Available at: http://www.blic.rs/Vesti/Svet/577337/STRAH-Ove-zemlje-se-najvise-plase-islamista.

21 *Spoljna migraciona politika EU: odlučniji pristup.* Delegacija Evropske unije u Republici Srbiji. 24/2/2014. Available at: http://europa.rs/spoljna-migraciona-politika-eu-odlucniji-pristup/.

in which ethnic differences, religious affiliation or traditional patterns are conjugating and equalizing resembles the American model, but it is currently almost invisible in European practice. Migrant communities use economic privileges, but are slowly integrated into spiritual patterns, especially in areas where they represent the majority of the population.[22]

By exploring the phenomenon of contemporary migrations, we noted the need for multilateral exchange of information between state authorities and the security services of the countries involved. Then a brief, but in the public discourse visible noise of porosity of national borders or mutual economic blockade will be absent. Instead of a "tabloids war" it is better to formulate and refer the official initiatives towards the countries of the region and European Union member states as a measure to restore the cooperative activities, aimed at well established management during the migration process, which would possibly lead to the reduction of conflicts to a minimum.

REFERENCES

1. "Tri mape za dve Evrope". *Politika*, 5. May 2015.
2. Bajagić, M.: *Međunarodna bezbednost*, Beograd: Kriminalističko-policijska akademija, Beograd, 2012.
3. Boulding, K.: *The Image: Knowledge in Life and Society*. Ann Arbor : University of Michigan Press, 1956.
4. Đorđević, B.: Etika migracije.*Godišnjak Fakulteta političkih nauka*. Beograd : Fakultet političkih nauka, Vol. 2, No. 2, 2008.
5. Elliott, A., Merrill, F.: *Social disorganization*, New York : Harper and Brothers, 1961.
6. Gidens, E.: *Sociologija,* Beograd: Ekonomski fakultet, 2003.
7. Jevtović, Z. i Aracki, Z.: Požar islamskog fundamentalizma i ćutanje Zapada, *Viteška kultura*, in: IV, No. 4, Beograd, 2015.
8. Kešetović, Ž. i Milašinović, S.: Krizni menadžment i slični koncepti – pokušaj razgraničenja, *Bezbednost*, y. 1-2, Beograd, 2008.
9. Malešević, M.: Hrišćanski identitet sekularne Evrope. Beograd: *Glasnik Etnografskog instituta SANU*, book. 55, (1), 2007.
10. Milašinović, R., Milašinović, S., Putnik, N.:*Teorije konflikata*, Beograd : Fakultet bezbednosti, 2012.
11. Milašinović, S. i Jevtović, Z.: *Metodologija istraživanja konflikata i krizno komuniciranje u savremenom društvu*, KPA, Beograd, 2013.
12. Penava, M.: Utjecaj krize na imigracijsku politiku EU. Zagreb: *EFZG Occasional Publications*, No. 1, 2011.
13. Predojević-Despić, J.: Ka razumevanju determinanti međunarodnih migracija danas – teorijska perspektiva. *Stanovništvo,* Beograd: Institut društvenh nauka, y. XLVIII, No. 1, 2010.
14. Radičević, N.: Kako nučiti izbeglice da žive na nemački način. *Politika*, 11/10/2015.

22 Radičević, N.: Kako naučiti izbeglice da žive na nemački način, *Politika*, 11/10/2015.

INTERNET SOURCES

15. 2015: Godina kada su migranti pokorili Evropu. *Tanjug,* 26/8/2015. Available at: http://www.tanjug.rs/full-view.aspxizb=195873. (Accessed 24.12.2015).
16. Četvrtina stanovnika EU u opasnosti od siromaštva. *Tanjug*, 17/10/ 2015. Available at: Radio-televizija Vojvodine, http://www.rtv.rs/sr_ci/ekonomija/globus/cetvrtina-stanovnika-eu-u-opasnosti-od-siromastva_649552.html. (Accessed on 25/12/2015).
17. Ove zemlje se najviše plaše islamista. *Blic*, 22/7/2015. Available at: http://www.blic.rs/Vesti/Svet/577337/STRAH-Ove-zemlje-se-najvise-plase-islamista. (Accessed on 24/12/2015).
18. Služba za pravnu zaštitu Beogradske kancelarije UNHCR: Zašto mediji izbeglice pretvaraju u migrante, *Cenzolovka,* 13/8/2015. Available at: https://www.cenzolovka.rs/iz-prve-ruke/zasto-mediji-izbeglice-pretvaraju-u-migrante/. (Accessed on 25/12/2015).
19. *Spoljna migraciona politika EU: odlučniji pristup.* Delegacija Evropske unije u Republici Srbiji. 24/2/2014. Available at: http://europa.rs/spoljna-migraciona-politika-eu-odlucniji-pristup/. (Accessed on 24/12/2015).
20. *Tanjug*, October 17, 2015. Available at: Radio-televizija Vojvodine, http://www.rtv.rs/sr_ci/ekonomija/globus/cetvrtina-stanovnika-eu-u-opasnosti-od-siromastva_649552.html.
21. *The increase in the number of displaced persons in the world*, UNHCR, United Nations High Commissioner for Refugees, 08/26/2015. Available at: http://www.unhcr.rs/dokumenti/saopstenja-za-medije/porast-broja-raseljenih-svetu.html.
22. WEF Davos: Beg od siromaštva i problem migracija. *Mesečnik Biznis & Finansije,* 22/1/2015. Available at: http://bif.rs/2015/01/wef-davos-beg-od-siromastva-problem-migracija/. (Accessed on 23/12/2015).

UDC: 343.85:[343.9.024:336.7(497.7)
346.23

ROLE OF THE ENTITIES IN THE SYSTEM FOR PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE REPUBLIC OF MACEDONIA

Svetlana Nikoloska, PhD[1]
Faculty of Security, Skopje
Gordana Jankuloska, PhD

Abstract: The system on prevention of money laundering and financing of terrorism in the Republic of Macedonia has its roots since 2001. It was established upon the adoption of the Law on Prevention of Money Laundering. This system is established on three pillars, as it follows: the first pillar comprises the entities, the second pillar is the Financial Intelligence Office and the third pillar is represented by the prosecution authorities. From the aspect of prevention the first pillar has the key role in detecting suspicious transactions and suspicious clients and prevention of the integration of criminal or dirty money in the legal financial system of the state and movement of the criminal money in the global financial system.

This paper will analyze the positioning of the entities in the system, the measures and activities undertaken in accordance with the law, and will further analyze the cooperation with the Financial Intelligence Office by analyzing the delivered data and information on the regular transactions exceeding the legal amount and suspicious transactions in the period of research 2008-2014. The subject of this paper is studying the role of the first pillar in the System on prevention of money laundering and terrorism financing in order to get insight into the indicators on how much these subjects have helped in discovering suspicious transactions, and thus, had certain contribution in preventing money laundering and terrorism financing as the most serious criminal danger of the day.

Keywords: entity, money laundering, terrorism financing, suspicious transactions, prevention

INTRODUCTION

Money laundering, as a security-related and a criminal problem which endangers primarily the legal economy and the safety and stability of the financial systems on national levels and wider, is a common research problem from multiple points of view. Money laundering has an evident influence on growing of the organized crime, from there arises the knowledge that combating money laundering is one of the most effective means of combating organized crime that especially threatens all societies[2]. From the point of view of money laundering

1 E-mail: svetlananikoloska@hotmail.com.
2 Јакулин В., Спречување на перењето пари во Европската унија и словенечкото кривично право, Македонска ревија за казнено право и криминологија бр. 1 – 2, Скопје, 1999, стр. 55.

prevention, in the area of detection of criminal money before and during their placement, it is necessary to study the methods and institutions through which actually the first step or the first stage of money laundering was made. Since 2001 the Republic of Macedonia has devoted attention to this problem by adopting the Law for prevention of money laundering and financing of terrorism[3] and setting the basis of the system for prevention of money laundering, especially with the establishment of the Directorate for prevention of money laundering, currently known as the Financial Intelligence Office. The abovementioned law represents implementation of several international documents: The United Nations Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention), The United Nations Convention against Transnational Organized Crime (UNTOC) known as Palermo Convention, the Stockholm Convention and especially the FATF recommendations. The system itself is designed and established to be able to detect criminal assets and other revenues via wider action or giving jurisdiction to a number of financial and non-financial institutions in their everyday activities to have legal obligation to detect suspicious transactions and suspicious clients, as well as to submit data to the Financial Intelligence Office for every transaction involving amounts over euro 15,000, aiming to control the transactions with higher amounts. By law all institutions that have this legal obligation are called "entities" and their work will be subject to analysis in the period from 2009 to 2014. The entities represent the first pillar in the System for prevention of money laundering and financing of terrorism, the second pillar is the Financial Intelligence Office and the third pillar are the law enforcement authorities under the coordination of the Public prosecutor[4]. The functioning of this system is important for the prevention of money laundering but also for detecting of this type of crime, securing evidence, full disclosure of the criminal situations and the money subject to legalization that helped in those criminal acts. The same applies to the redefinition of the criminal act "Money laundering and other revenues from criminal action" from 2009 where entities can be sanctioned for not taking any legal actions of detecting suspicious clients as well as sanctioning as an act of corruption, the employees with the status of official personnel that will discover information for the financial investigation initiated by the persecution bodies. The role of the entities is significant and takes place in two directions:

- The first direction is when the entities are the first ones to detect suspicious activity aimed at legalizing criminal money by using their professional knowledge, skills, according to a previously defined indicator. Their doubts, in a form of information are transmitted electronically by completing the CTP form, according to which the information and data related to the client and transaction should be transmitted and shall be submitted to the Financial Intelligence Office for further analysis and treatment. This is the direction when the entities have the initial information, that during the proceedings could develop "from information to clarification of the criminal case," that is responsibility of the law enforcement agencies or the third pillar. The entities can detect money laundering in the first stage of the placement, but also in the second phase when transferring reveals suspicious transaction (especially banks), but also in the phase of integration when the benefits of the money are enjoyed.

- The second direction is when law enforcement agencies, on operational level, run the criminal investigation and clarify the existence of the grounds for suspicion of committing crimes, where the perpetrators have gained illegal profit[5]. In such cases the prosecuting

3 Official Gazette of Republic of Macedonia No. *70/01, 04/08, 57/10, 35/11, 44/12*

4 Николоска С., *Перење пари, криминолошки, криминалистички и кривично – правни аспекти*, Ван Гог, Скопје, 2015, p. 129.

5 Nikoloska S. Inter-Institutional Cooperation in the Process of Investigating Economic-Financial Crime in the Republic of Macedonia, Revija za kriminalistiko in kriminologijo / Ljubljana 65 / 2014 / 4, pp. 361–372.

authorities initiate checks or financial investigations through the Financial Intelligence Office, and the Office receives the necessary information from the entities. This is actually a search for the money and the proceeds generated from criminal activity, detecting the flow of the money or its placement, transferring and integration which would mean that all stages of money laundering have passed.

Money laundering is a process which is previously planned and always, especially when it comes to the organized criminal groups, has previously defined schemes and methods whose detection is a success of the established system for prevention of money laundering and financing of terrorism.

Money laundering is not just a process associated with the functioning of the criminal organizations but also an indicator of their success. Furthermore the money laundering secures a constant cash flow that enables them to buy protection by corrupting government officials and members of law enforcement agencies. The more attractive money laundering is for the law enforcement agencies, the more energetic the criminal organizations become and introduce new ways in securing transformation of their illegal initiatives into usable assets. The expansion of the activities of transnational criminal groups is increasingly contributing to the rise of the need to protect the legitimate economies against the penetration of the illegal proceeds of crime[6]. Criminal organizations have the "dirty" money and perform various transactions to integrate that money into the legal economic and financial flows or to smuggle it across the border into a foreign country[7]. The consequence is that money laundering is one of the most important links between the criminal world and the legitimate society. Money laundering is one of the basic ways in which the criminal organizations enter the legal economy and often include seemingly respectable members of the society (bankers, lawyers etc.). If we allow money laundering to freely develop it will have a damaging influence on the financial institutions' integrity.[8]

The problem of money laundering has global economic and security dimensions. Therefore the United Nations has included it in the types of dangerous criminal phenomena to which the international community attaches great importance and adopted a Global Programme against Money Laundering which foresees assisting countries - States leveling of national legislation with international documents, and training law enforcement agencies and the creation of financial intelligence units and finding new methods and tools for successfully confronting sophisticated forms of modern criminal activities related to money laundering[9]. The phenomenon of money laundering is commonly described as a veiled, sophisticated and profitable criminal activity, and the perpetrators are intelligent people, always a step ahead of the representatives of the state bodies and institutions whose competence is investigation of economic - financial crime with elements of money laundering and other proceeds of the offenses.[10]

Money laundering is defined as "using money derived from illegal activities by hiding the identity of the individuals who received the money and their transformation into assets that appear to come from legitimate sources." This can be simplified by saying that money laundering is a process through which dirty money becomes clean. According to the US laws dirty money is never 'clean', no matter how many times it has gone the cycle of 'rinse and spin'[11].

6 Тасева С. , *Перење пари*, Дата Понс, Скопје 2003, p. 18.
7 Бошковиќ М.и Јовичиќ Д. , *Криминалистика - Методика*, БањаЛука, 2002, p.363.
8 Вилијамс Ф. , *Перење пари,* Безбедност бр. 4, Скопје, 1997, p. 369.
9 Ignjatović Dj., *Suzbijanje najteźoblika kriminaliteta u uslovima tranzicije i nesigurnosti*, Teški oblici kriminala, XVI Seminar prava, Budva, 2004, p. 10.
10 Ignjatović Dj , op. cit. p. 3.
11 Мединger Ц. , *Перење пари – водич за кривични иследници,* Дата – Понс, Скопје 2009, p. 8.

Money laundering is a process where the criminal assets are presented as if they were coming from a legitimate source. Research activities related to money laundering have double-side approach according to Layman and Potter:[12]

1. Investigation of the criminal activity, or simplified, if there is no criminal activity or "certain illegal activity" that would generate illegal assets then there cannot be a question of money laundering. A parallel financial investigation for discovering the financial infrastructure of the criminal organization. Tracing the money and disclosure of its flow inside of the organization in order to hide, mask or cover the assets.

The role of the stakeholders in detecting the criminal revenues is crucial and can be analyzed through the activity of the entities in delivering information to the Financial Intelligence Office, but they also have a significant role in detecting the cash flow, the identification of the clients and the final destination or "shelters" of the criminal money backed by international collaboration, because for the high criminal incomes the criminals always seek "safe shelters" for the obtained assets.

SYSTEM FOR PREVENTION OF MONEY LAUNDERING IN THE REPUBLIC OF MACEDONIA

The system for prevention of money laundering and financing of terrorism in the Republic of Macedonia has been established by acceptance of the recommendations of several international documents, but the FATF Recommendations open a new dimension in the prevention of money laundering. The undisputed role of the criminally – legal repression and the central role of the criminally – legal mechanisms as acknowledged, the confiscation of criminal assets etc. as inevitable for undermining the financial power of the organized crime groups. But at the same time, relying solely on criminally – legal mechanisms and a wide range of measures for reducing money laundering is needed. The initial idea of the FATF is the new strategic frame by putting the banks and other financial institutions on the front line in the fight against money laundering. That initial idea is justified by the fact that the prevention of money laundering is not just problem of crime prevention but also a problem of preserving the integrity of the financial institutions and the financial system as whole. It is estimated that temporary measures and confiscation will be introduced and according to the Third recommendation the state authorities should (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

It is provided that the countries should consider adopting legal measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or to require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation. Actually the basis of the functioning of the whole system for prevention of money laundering and financing of terrorism involves the principle of "information to confiscation of criminal revenues". It especially indicates the need for predicting effective, proportionate and dissuasive criminal, civil or administrative / civil penalties for individuals or legal entities that do not meet the requirements for prevention of money laundering or terrorist financing, and recommendation not to establish business relations with "shell" banks. After 40 recommendations of the FATF, 9 special recommendations for prevention of terrorism con-

12 Лајман Д. М. и Потер В. Гари, Организиран криминал, четврто издание, Магор, Скопје, 2009, p. 211

tain modifications of these recommendations in 2009 that reflect changes in regulatory priorities and are result of public consultation on this issue. The changes include increased focus on the access based on the risk in the area of prevention of money laundering and measures for the fight against financing of terrorism designed to enable the countries within the FATF standards to adopt a set of more flexible measures that correspond to the nature of the identified risk, as, for example, politically exposed persons and expanding the recommendations so they can deal with the challenges like proliferation of weapons of mass destruction. The main changes in the recommendations are set towards including the tax criminal offences as predicate criminal acts; expansion of the obligation for the financial institutions for enforced control, due diligence of the risk for domestic politically exposed persons, adopting more rigorous demands for the countries to establish mechanisms for basic information records so the companies can provide the financial institutions and the state authorities to conduct proper control over the users (Customer Due Diligence) and adopting a new procedure (step by step) to determine the ultimate users and control of the companies as part of the user control.

The system for prevention of money laundering in the Republic of Macedonia is developing; it was founded in 2001 and in 2008 there were significant results in the area of detecting suspicious transactions and clients as well as in the area of financial investigation and allowing confiscation of criminal revenues and property in and out of the country. The system is set to identify suspicious transactions by implementing indicators, and the first in line to identify such transactions are the entities, which react when criminal assets enter or are about to enter the legal financial system. The Financial Intelligence Office or the state authority follows the suspicious transactions and, eventually, the prosecution authorities need to detect and prosecute the perpetrators who obtain high criminal incomes with which they either attempt or manage to invade the legal financial system.

According to Tupanchevski[13] there are several reasons why it is necessary to establish a system to prevent money laundering and the uptake of laundered money into the legitimate financial system: "First, seeing it from point of view in the interest of the national governments, the absence of prevention of money laundering results in increasing the criminal rate in a way that enables the criminals to have benefit from their actions which makes the crime even more attractive and enables the criminal organizations to finance further criminal activity. Second, the uncontrolled use of the financial system for money laundering can jeopardize the individual financial institutions and as a result of that the whole financial sector. The reasons that motivate the financial sector for more organized approach in the prevention of money laundering can appear as the result of the awareness of the long-term success in the functioning and the financial sector and depends on the ability to attract and keep legal and legitimate funds. Those funds can be attracted and kept via legal origin and the nature of the goods and services, the quality and safety of the service, the reputation of the institution. The dirty money can harm their reputation and scare honest investors".

The system for prevention of money laundering consists of three pillars:

- The first pillar consists of entities that have a legal obligation to take measures and actions to prevent money laundering and terrorist financing.

- The second pillar is the Financial Intelligence Unit which is the administrative authority for financial intelligence which acts as an intermediary between entities, on the one hand, and the investigating authorities on the other.

- The third pillar consists of the prosecution - the Public Prosecutor's Office (Department for Organized Crime and Corruption), the Ministry of the Interior (Department for organized crime and all organizational units for suppression of organized crime) and the Ministry of

13 Тупанчески Н., Економско казнено право, Стоби Трејд ДООЕЛ, Скопје, 2015, p. 140

Finance (Financial Police and Customs Administration), but it cooperates with the Public Revenue Office, although it is not a body which is directly involved in the investigation of crime, but indirectly participates in many cases to identify reported or unreported income, money and property of suspected legal entities and individuals. These authorities are responsible for detecting, highlighting and providing evidence of the crime with elements of laundering money and evidence of the crimes from which criminal money and revenues originate. According to Levi[14], property acquired through crime rarely reaches the courts in the form of ripe fruit from fruit trees. To make a right judgment the competent authorities for criminal investigation have to provide relevant evidence[15]. Particularly in laundering money despite criminal investigations, it is necessary to run financial investigation at the same time as well. In the absence of financial investigation it is less likely that criminal proceeds will be found and confiscated. In order to provide relevant evidence the above mentioned institutions cooperate with the Public Revenue Office, although it is not a body which is directly involved in the investigation of crime, but indirectly participates in many cases to identify any irregular or taxable income, money and property from suspects (individuals and legal entities). Financial investigation against suspects includes assessing whether their life style is associated to "honest life" or "comfortable life" provided by the criminal activity[16].

Graph 1: *Positioning of the system for prevention of money laundering and financing of terrorism in the Republic of Macedonia*

LEGAL ENTITIES AS THE FIRST PILLAR OF THE SYSTEM TO PREVENT MONEY LAUNDERING AND FINANCING OF TERRORISM

Within the Law on prevention of money laundering and financing of terrorism the following entities are defined: "Entities are persons that have the obligation to undertake measures and acts to prevent money laundering and financing terrorism provided by law." The meaning of the entity, for the functioning of efficient system for prevention of money laundering and financing of terrorism is explained from two points of view. On one side, the professionalism

14 Levi, M., Osofsky, L., (1995). *Investigating, seizing and confiscating the proceeds of crime*, London: Home Office Police Department, pp. 6 - 7.
15 Боба Рејчел, *Криминалистичко истражување*, Нампрес, 2010, p. 62.
16 Bošković G. i Marinković D. ,*Metodi na finansijske istrage u suzbijanju organizovanog kriminala,* NBP, Journal of criminalistics and law - Žurnal za kriminalistiku i pravo, br. 2, Beograd, 2010, p. 89.

of the employees that work in the entities is undisputed, as well as their professionalism and knowledge of the subject they are working with, added by the knowledge in the area of fight against money laundering and financing terrorism, is a source of experience in terms of identifying products, clients and activities, dangerous in terms of money laundering and financing terrorism, as a source of identifying ways and methods of executing this criminal activities. On the other side, which is very important to be mentioned, starting from the fact that the entity employees know their clients very well, their intentions and the justification of the actions they perform i.e. knowing the client profile, they can easily recognize activity in terms of the wholeness of that business relationship.[17]

The entities that are obliged to take measures and activities for prevention of money laundering and financing of terrorism envisaged by law:[18]

1. Financial institutions and subsidiaries, branches and business units of foreign financial institutions that carry out an activity in the Republic of Macedonia in accordance with the law;

2. Legal entities and individuals that provide the following services:

a. trade in immovables,

b. audit and accounting services,

c. notaries, lawyers and other legal services related to: sale and purchase of movable items, immovables, partners' shares or stocks, trade and management of cash and securities, opening and management of bank accounts, safe deposit boxes and other financial products, establishment or participation in the management or the operation of legal entities, representation of clients in financial transactions etc.,

d. tax advising,

e. providing consulting services, and

f. providing investment advisor services.

1. Organizers of games of chance in a game shop (casino);
2. Internet casinos;
3. Providers of services to legal entities;
4. The Central Securities Depository; and
5. Legal entities that accept movable and immovable items as pledge.

In the interest of preventing money laundering and financing of terrorism the entities are obligated to undertake concrete measures and activities. These measures and activities are taken from the recommendations of the international legal acts in order to harmonize the Macedonian legislation and the unstoppable action in suppressing money laundering and information exchange with appropriate foreign state agencies. The law obliges the entities to conduct the following:

- client due diligence,
- monitoring particular transactions,
- collection, keeping and submission of data regarding the transactions and the clients that carry out the transactions, and
- introduction and application of programs.

17 *Прирачник за спроведување на мерки и дејства за спречување на перење пари и финансирање на тероризам од страна на субјектите,* Министерство за финансии – Управа за спречување на перење пари и финансирање на тероризам, Скопје, 2010, p. 22

18 Article 5, Law for prevention of money laundering and financing of terrorism („Official Gazette of the Republic of Macedonia No. *04/2008, 57/2010, 35/2011и 44/2012*

The entities are obliged to carry out a client due diligence procedure in the following cases:[19]

- upon establishment of a business relationship;
- if a single or several linked transactions in the amount of Euro 15.000 or more in Denar counter value are made;
- in the case of suspicion of money laundering or financing of terrorism, regardless of any kind of exception or amount of the funds; and
- in the case of suspicion of the veracity or adequacy of the previously obtained data about the identity of the client.

The procedure itself includes identification of the clients and verification of their identity by using documents, data and information from reliable and independent sources; identification of the principal of the power of attorney and verification of their identity by using documents, data and information from reliable and independent sources; identification of the beneficial owner and taking appropriate measures for verification of their identity in order for the entity to be assured who the beneficial owner is, by using documents, data and information from reliable and independent sources; provision of information about the aim and purpose of the business relationship; and continuous monitoring of the business relationship and the transactions that are made within the established business relationship with the client for the purpose of ensuring that these transactions are consistent with the risk profile and the business of the client, and if necessary, determination of the sources of funds.

The entities are obliged to apply every measure under the client due diligence procedure, and their scope depends on the risk assessment of the client, the business relationship, the product, or the transaction. The entities have to make a risk assessment on the basis of an internal procedure for risk analysis which is an integral part of the program, as well as on the basis of the indicators prepared by the Financial Intelligence Office in cooperation with the entities and the supervisory bodies. The entities are obliged to make the documents for risk assessment available to the Financial Intelligence Office and the supervisory bodies in order for them to confirm that the established risk of money laundering and financing of terrorism is adequate and that the scope of the measures taken is in compliance with the risk of the client, the business relationship, the product, or the transaction.[20] In particular, the entities have policies and procedures regarding "non face to face" business relationships and transactions.

The entities[21] are obliged to monitor the transactions carried out under the business relationship with the client and regularly update the documents and the data about the existing clients with whom they have established a business relationship in order to confirm that such transactions are made in accordance with the aim and the purpose of the business relationship, the client risk profile, their financial situation, and, if necessary, the sources of financing.

The entities are obliged to pay special attention to the complex, unusually high transactions or transactions carried out in an unusual manner, that have no obvious financial justification or visible legal purpose. Special attention of the entities is required with regard to the business relationships and the transactions with citizens' associations and foundations from countries that have not fully or partially implemented the measures for the prevention of money laundering and financing of terrorism, as determined by law. According to the law the entities have a wide range of available measures and activities but the procedure for acting from the mo-

19 Article 9, Law for prevention of money laundering and financing of terrorism („Official Gazette of the Republic of Macedonia No. *04/2008, 57/2010, 35/2011u 44/2012*

20 Nikoloska S. and Simonovski I., Role of banks as entity in the system for prevention of money laundering in the Macedonia, Elsevier, Procedia - Social and Behavioral Sciences 44 (2012) pp. 453 – 459.

21 Article 12b, *Law* for *prevention* of *money laundering* and *financing* of *terrorism* („Official Gazette of the Republic of *Macedonia No. 04/2008, 57/2010, 35/2011u 44/2012*

ment of receiving the information, preparing the information and the process of reporting it, is defined more precisely. Especially in the part related to the client identification the legislator dedicates special attention on identification or determination of the identity of individuals, officials, authorized persons, legal entities or authorized persons as well as identification of the subjectivity of the legal entities. The duration and timing of each of the activities is precisely determined in the interest of fast and efficient acting and paying attention to the process of business of the legal entities concerned in the identification process. The entities receive directions from the Financial Intelligence Office, including indicators for each action of possible money laundering and electronic forms delivering information connected to regular cash transactions over 15 000 Euros and suspicious transactions that can be spotted or connected with suspicious clients. The law provides for the storage of confidential data by the entities which may be used only for the detection and prevention of money laundering and financing of terrorism. The delivery of information to the Financial Intelligence Office, the supervisory authorities or to the law enforcement agencies is not considered as disclosing confidential information. The entities are obliged to submit the collected data, information and documents to the Financial Intelligence Office in the following cases: [22]

- when they suspect or have grounds to suspect that money laundering and/or financing of terrorism has been or is committed or an attempt to launder money and/or to finance terrorism has been or is being made, regardless of the amount of the transaction;
- when the property is proceeds of crime;
- in the cases of a cash transaction in the amount of Euro 15,000 in Denar counter value or more and in the cases of linked cash transactions in the amount of Euro 15,000 in Denar counter value or more.

The entity is obliged to submit data, information and documents to the Financial Intelligence Office in a form of a report within a period of 24 hours at the latest.

All data and information by the entities are delivered to the Financial Intelligence Office electronically, by filling a special electronic form, a report known as STR. STR is a electronic form that defines all the data that needs to be secured in the process of identification of the client and the transactions.

If the entity employs more than 50 persons, the entity should form a special department within the framework of its operation[23] that will be in charge of conducting the program and respecting the definitions of the Law for prevention of money laundering and other incomes form criminal act and financing terrorism and to notify the Financial Intelligence Office in written form.

The significance of the entities to the functioning of an efficient system for prevention of money laundering and financing of terrorism is great because the professionalism, expertise of staff in the entities, upgraded via training in the field of combating money laundering and financing of terrorism, for the purpose of identification of products, customers and activities and as a source for identification of ways and methods to carry out criminal activities. In particular it should be pointed out that the employees of the entities are most familiar with their customers, their intentions and legitimacy of the activities they perform, knowing that the profile of the client can easily identify activity that deviates from the usual activities of the client, activity which is illogical in terms of the whole of that business relationship.

22 Article 29, *Law* for *prevention* of *money laundering* and *financing* of *terrorism* („Official Gazette of the Republic of *Macedonia No. 04/2008, 57/2010, 35/2011u 44/2012*
23 Article 40a, *Law* for *prevention* of *money laundering* and *financing* of *terrorism* („Official Gazette of the Republic of *Macedonia No. 04/2008, 57/2010, 35/2011u 44/2012*

The client's importance is vital when it comes to discovering a crime after performing a criminal act with elements of money laundering and other incomes of criminal background with the entity's data we can analyze the flow of the criminal money and all the transfers in investigating criminal situations where the perpetrators obtained unlawful gains that have been legalized. The search for the money and the property leads to the perpetrators i.e. towards disclosure of the facts and connection of other persons, but also the entity employees' involvement in certain cases, thus becoming liable for abuse of their authority and disrespecting legal definition.

DATA ANALYSIS SUBMITED BY THE ENTITIES TO THE FINANCIAL INTELEGENCE OFFICE IN THE PERIOD 2009-2014

An analysis is made, based on data provided by the annual reports of the Financial Intelligence Office for the period 2009 - 2014, collected according to a harmonized methodology for collecting and presenting of data, submitted by the entities to the Financial Intelligence Office, data on the analyzes and on obtaining the grounds of suspicion for criminal offenses of money laundering and financing of terrorism where data are submitted to law enforcement agencies with special reports.

In addition to the prosecution in the field of tax evasion the reports are also submitted to the Financial Intelligence Office and other state authorities and institutions. The role of stakeholders in identifying possible activities (transactions) related to money laundering or financing of terrorism is crucial in the fight against these phenomena, the success of institutions in the system, to prove and confirm crime depends on their success to detect suspicious activity. The submission of suspicious transaction report (STR) is the starting point in the process of establishing the existence of suspected money laundering or terrorist financing.

The methodology for collecting and presenting data is constantly being upgraded as a result of the standards and measures established by the international bodies dealing with the phenomenon of money laundering and financing of terrorism.

The methodology of collecting and presenting data is constantly improved as a result of the standards and measures established by international bodies dealing with the issue of combating money laundering and financing of terrorism[24].

Table 1: *Data for submitted STR by legal entities to state bodies and institutions which are directly and indirectly responsible for fighting money laundering and financing of terrorism*

Entities	Submited STR by legal entities to the Financial Intelligence Office						TOTAL:
	2009	2010	2011	2012	2013	2014	
Banks	163	122	114	145	136	111	791
Savings Banks	2	14	7	/	/		23

24 Николоска С., *ibid. p*. 154.

Brokerage houses	1						1
Notaries	10	11	26	77	8	29	161
Loyers	20	2	2	1	4	1	30
Service Providers - money transfer	2	2	2	1	5	3	15
Exchange office	/	5					5
Insurance companies	/	0					
Insurance brokerage companies	/	0					
Insurance agencies insurance	/	0					
brokerage houses	/	1	1				2
Management companies of investment funds	/	0	2			1	3
Companies managing supplementary pension funds	/	1		1			2
Post offices	/	0					
Legal entities performing financial transactions, telegraph money transfer or delivery of valuable items	/	0				1	1
Leasing companies	/	0		2	12	1	1
Real estate agencies	/	1					1
Audit Company	/	0				1	1
Accountacy Company	/	2				1	3
Casinos	/	4	1	1	3	2	11
Civil associations and funds	/	0		1	1		2
Securities and Exchange Commission	/	/	1				1
Macedonian Stock Exchange	/	/	1				1
Pension fund			1				1
Legal entities whose business is the purchase of vehicles						2	1
Finacial associations						1	1
Legal companies that mediate micro payments						1	1
TOTAL:	198	165	156	229	169	153	1070

According to the data, the most active subject in the period of research were the banks, as expected, because they realize the majority of the financial transactions and any legal entity has a bank account where all of the financial transactions are realized. The banks are stakeholders that perform analyses and thorough analyses of the clients but also follow the financial transactions of individuals and legal entities on national level as well as financial

transactions made to banks outside the country and transactions from outside to banks in our country. Noticeably, in the research period most STR were submitted in 2012, 229, and least in 2015, 153. From the data sheet we can say that the list of stakeholders gets bigger by new stakeholders that submitted STR, the first year noticed the least while expectantly the last one had the most. These data are just a starting point for the Financial Intelligence Office to analyze, compare and run additional checks with the purpose of submitting a report to the prosecution authorities or other authorities for investigating criminal activities such as the inspectorates. Those data are shown in the second sheet for the same period of time.

According to the data from the second sheet, the Financial Intelligence Office, in most of the cases where there is ground for suspicion according to their analysis, submits reports to the Ministry of Internal Affairs, which is understandable given the fact that it is the oldest institution for crime suppression. Although in 2001 several new bodies for suppression of money laundering were formed, including Financial police, Financial Intelligence and although the reports are also submitted to them, it is noticeable that even within the new concept that has been introduced, where the public prosecutor is the coordinator of the criminal investigation, the Office still submits the reports to the bodies where operative workers have been delegated for the judicial police that have the role of investigators and act in coordination with the public prosecution.

Table 2: *Reports submitted to the Financial Intelligence Office on ground of suspicion of money laundering and financing of terrorism and other criminal acts*

Bodies to which the reports/notifications have been submitted to	Submitted reports on money laundering and financing of terrorism						Submitted reports for other crimes					
	2009	2010	2011	2012	2013	2014	2009	2010	2011	2012	2013	2014
Ministry of the Interior	24	24	20	30	19	25	40	67	47	56	105	128
Financial Police	11	4	3	6	1	4	31	21	24	19	27	22
Public Prosecutor	2	2	2	0	2	2	2	2	4	1		2
Public Revenue Office	0	0	0	0	0	0	21	34	22	20	13	19
Customs Administration	0	0	0	0	0	0	9	1	5	7	1	2
Security Exchange Office	0	0	0	0	0	0		1	5	15		
Basic Court	0	0	0	0	0	0		1		2	1	
Ministry of Interior and Public Prosecutor	0	0	0	0	3	3						
Ministry of Interior and Public Revenue Office	0	0	0	0	0	0					1	
Public Revenue Office and Financial Police	0	0	0	0	0	0					1	
Intelligence Agency	0	0	0	0	0	0					5	

Financial Intelligence Units of other countries	0	0	0	0	0	0	7	13		1	3	
TOTAL:	37	30	25	36	25		110	140	107	121	157	173

CONCLUSION

According to the research we can say that the System for prevention of money laundering in the Republic of Macedonia in the past few years has justified its existence as regards prevention of money laundering and financing terrorism, which can be seen from the analyzed data and from the submitted reports that the Financial Intelligence Office as a second pillar has delivered to the prosecution bodies based upon the initial data gathered from the entities. By studying the legislative and sub – legislative acts we can conclude that the Republic of Macedonia has implemented the recommendations of the international community and that it supports the attitude of the international community for joint and coordinated action in suppressing money laundering and financing of terrorism.

REFERENCES

1. Бошковић М.и Јовичић Д., *Криминалистика - Методика*, Бања Лука, 2002.
2. Вилијамс Ф. ,*Перење пари,* Безбедност бр. 4, Скопје, 1997.
3. Ignjatović Dj. , *Suzbijanje najteźoblika kriminaliteta u uslovima tranzicije i nesigurnosti*, Teśki oblici kriminala, XVI Seminar prava, Budva, 2004.
4. Лајман Д. М. и Потер В. Гари, Организиран криминал, четврто издание, Магор, Скопје, 2009.
5. Law for prevention of money laundering and financing of terrorism (*Official Gazette of the Republic of* Macedonia No. *04/2008, 57/2010, 35/2011и 44/2012*
6. Јакулин В. , Спречување на перењето пари во Европската унија и словенечкото кривично право, Македонска ревија за казнено право и криминологија бр. 1 – 2, Скопје, 1999.
7. Levi, M., Osofsky, L., (1995). *Investigating, seizing and confiscating the proceeds of crime*, London: Home Office Police Department.
8. Медингѐр Ц. , *Перење пари – водич за кривични иследници,* Дата – Понс, Скопје 2009.
9. Nikoloska S. and Simonovski I., Role of banks as entity in the system for prevention of money laundering in the Macedonia, Elsevier, Procedia - Social and Behavioral Sciences 44 (2012) 453 – 459.
10. Nikoloska S. Inter-Institutional Cooperation in the Process of Investigating Economic-Financial Crime in the Republic of Macedonia, Revija za kriminalistiko in kriminologijo / Ljubljana 65 / 2014 / 4, 361–372.
11. Николоска С., *Перење пари, криминолошки, криминалистички и кривично – правни аспекти*, Ван Гог, Скопје, 2015.
12. *Прирачник за спроведување на мерки и дејства за спречување на перење пари и финансирање на тероризам од страна на субјектите,* Министерство за финансии – Управа за спречување на перење пари и финансирање на тероризам, Скопје, 2010.
13. Рејчел Б. , *Криминалистичко истражување*, Нампрес, 2010.
14. Тасева С. , *Перење пари*, Дата Понс, Скопје 2003, стр. 18.
15. Тупанчески Н., Економско казнено право, Стоби Трејд ДООЕЛ, Скопје, 2015, стр. 140.

UDC: 377.1:351.74/.75
316.42

SOCIAL CHANGES AND EDUCATION OF POLICE OFFICERS[1]

Zoran T. Đurđević, PhD[2]
Academy of Criminalistic and Police Studies, Belgrade
Slaviša Lj. Vuković, PhD
Academy of Criminalistic and Police Studies, Belgrade
Nenad Radović, PhD
Academy of Criminalistic and Police Studies, Belgrade

Abstract: If we want a modern, democratic, responsible and efficient police service, evaluation and improvement of the system of education of police officers is a necessity. The efficiency and length of the transition as a process of changes depends on the expertise and the educational system of its people who participate in the process. The subject of the analysis is a system of education of police officers, concepts and standards that must be met by every officer in relation to the type of work and a certain position in the hierarchy of the police organization. This underlines a certain degree of harmonization of work and educational profiles of police officers with the challenges that come with the changes in society. In order to answer this question it is necessary to point out the external and internal factors that affect them most, primarily: trends and structure of crime; profiles of perpetrators and victims of crimes and trends in the development of society. Special emphasis is on the analysis of the impact of development of information technology and globalization, on the work of the police and also on trends in crime. The conclusion emphasizes a need to create a body for the protection of police integrity, whose one segment of operations would be to improve the quality of education of police officers.

Keywords: police, social change, work profile, educational profile, education.

INTRODUCTION

Police integrity is a reflection of the degree of professionalization. In addition to ethics the most important element of professional integrity is knowledge[3]. Knowledge is not an inert organizational resource, because by applying knowledge you can create new knowledge. When we talk about knowledge, we usually talk about education - the process of acquiring knowledge, the system of values and standards of one profession. Quality indicator of this process is the degree of functionality of the acquired knowledge necessary for the efficient work performed within the profession whose prefix is in the core of educational institutions that educate staff for a certain profession. With regard to its mission to protect the fundamental rights and freedoms of citizens, police profession has special significance for society. That is why it is

1 The paper is the result of the project named "Development of institutional capacities, standards and procedures for combatting organized crime and terrorism in the conditions of international integration" (No. 179045), funded by the Ministry of Education, Science and Technological Development of Republic of Serbia, and implemented by The Academy of Criminalistic and Police Studies and "Crime in Serbia and Instruments of State Response", which is financed and carried out by the Academy of Criminalistic and Police Studies, Belgrade – the cycle of scientific projects 2015-2019.
2 E-mail: zoran.djurdjevic@kpa.edu.rs.
3 Djurdjevic *et. al.*, 2013, p. 160.

necessary to analyse the system of police education and trends of society development, so that the professional work force can be created, i.e. the professionals who can meet the requirements of society during the transition period in an efficient manner.

The selection of candidates and functional education are essential elements in building and protecting police integrity. Police education must be harmonized with immediate developmental needs of profession. This is why it is necessary to have constant evaluation of quality of education and this is why it needs to be harmonized with the new security challenges and factors that directly affect them. The mission those who directly participate in exercising the educational functions, besides the ability to transfer knowledge and being competent is also to do scientific research, to give forecast for the development of factors that affect the profession and prepare the profession accordingly for a period of change, transition. When we talk about education in transition, we often talk about the transition of education without a clearly emphasized connection with the transition of society. Educational system must serve the society and its needs, and it cannot just be the segment that works for itself.

Transition means changes, a transition from one system into a new one that is supposed to represent the solution to the problems. The term "crisis", besides its negative side, also represents a chance for change. Certain elements in society change more slowly while others change faster. As the members of the profession, we can influence some changes more and some less. Some changes depend on our decisions, and some other changes we simply have to accept and adapt to them. Efficiency and length of transition, in addition to readiness, mostly depends on the available human resources, namely the expertise and education of those who make these changes happen. The subject of analysis is the system of police officers' education, the concepts and standards that must be met by every police officer regarding the type of work and a place in the hierarchy of the police organization, as well as the degree of alignment of work and educational profiles of police officers with the challenges that come with the changes in society including the methods for their assessment.

Educational policies and opportunities for change are the paradigms placed within the context of generic trends of the development of society. For us, the argument that education should keep the pace with the changes in society is not correct. Instead of that, we presume that the changes in education that have arisen on the basis of forecast of science development and society development should be encouraged for other positive social innovations, namely the creation of professionals who will provide practical solutions for the elimination of possible negative social phenomena. Ideally, the goal we should strive for is not to seek solutions when problems have already arisen, but to make assumption that the problems may occur and propose solutions that will prevent the occurrence of problems. The basic assumption for the success of any profession is the ability to forecast, more accurately understand and adapt to social trends, to implement positive solutions and create mechanisms for protection against negative phenomena[4]. Taking into consideration this assumption, human resources which will strengthen the institutional capacity for implementation of all necessary social changes are created.

POLICE EDUCATION SYSTEM IN THE REPUBLIC OF SERBIA

According to the Development Strategy of the Ministry of Interior RS (2011-2016), one of the biggest challenges is the establishing of a modern system for human resources management. One of the important tasks is to develop the capacity for staff planning and candidate selection, career monitoring and managing the course of service, basic and specialized

4 The Law on Police, "Official Gazette of RS", no. 6/2016

training. Special emphasis was put on the development of a system of specialized training, management training, and continuous professional education. Based on the analysis of educational needs, it was concluded that the introduction of new ways of learning could improve the quality of education of police officers. In 2011, in cooperation with the Organisation for Security and Cooperation in Europe a Strategy named "The introduction of e-learning as a support for the development of the training system in the Ministry of Internal Affairs" was adopted. It has been harmonized with the Development Strategy of the Ministry of Interior 2011-2016, the Education Development Strategy until 2020 and the Education Strategy for Adults in the Republic of Serbia. In the development of this strategic document the following documents were used: Strategy on Development of E-Government in the Republic of Serbia for period 2009-2013, Strategy on Development of Electronic Communications in the Republic of Serbia for period 2010-2020 and Information Society Development Strategy in the Republic of Serbia.

In order to define the strategic course more precisely the Republic of Serbia adopted the Development Strategy of Human Resources in the Ministry of the Interior 2014-2016. The biggest step, which was used to legally regulate the area of human resource management, is the adoption of the new Law on Police.[5] The function of human resource management will be performed by a separate organizational unit, the Division of Human Resources (Article 130). In accordance with the law, professional training is done through basic police training, specialist training and police training base level (Article 131, paragraph 3). When it comes to professional education, law is imprecise given the declaratory provision which indicates that professional education is to be carried out in accordance with the regulations in the field of higher education (Article 134).

Police education, which is a part of the educational system of the Republic of Serbia, consists of: basic police training/education; higher police education and professional in-job training/development. Basic Police Training Centre in Sremska Kamenica as an organizational unit of the Ministry of Internal Affairs of the Republic of Serbia (hereinafter: MIA RS) is responsible for the basic police training, while the Academy of Criminalistic and Police Studies is an accredited institution of higher education for three scientific fields: 1) Criminalistics, 2) Forensic engineering, and 3) IT and computing. The accredited programs include undergraduate and master academic studies for all three scientific fields, undergraduate vocational studies of criminalistics and graduate specialist academic studies of criminalistics, while the doctoral studies in all three accredited scientific fields are in the process of getting the accreditation. The Academy of Criminalistic and Police Studies performs basic, applied and development research in the field of criminalistics, forensic engineering and information science and computing, as well as research projects that support the development of educational activities and performance of police duties. The goal is to create a coherent system, which will ensure the development of police profession and protection of police integrity.

Higher police education, besides being a part of the educational, scientific space of the Republic of Serbia, is trying to keep pace with trends and to contribute to improving the quality of European police educational system. The Academy of Criminalistic and Police Studies is a member of the Association of European Police Colleges. The Association currently consists of 45 members from 37 European countries. Besides the Law on Higher Education, general provisions for professional education, training and development are defined in Articles 152-154 of 2005 Police Act. Thus, within the Republic of Serbia's MIA, there is the Directorate for Police Education, Professional Development and Science.

5 The Law on Police, "Official Gazette of RS, no. 6/2016

CHALLENGES OF POLICE PROFESSION

Basic requirements that society places before the police are a high level of security, the protection of fundamental rights and freedoms and effective law enforcement. However, the challenges that the police organization faces are specific for each time period. In order to prepare for future challenges the police must work on:

1. Identification of determinants that will influence the scope and structure of crime, the ways of committing criminal acts and the profiles of potential perpetrators and victims of crimes and other security occurrences;
2. Identification of determinants that may affect the police profession, organization and efficiency in performing tasks within the competence of the police;
3. Determining objectively the working profile of a police officer who should confront future challenges;
4. Improving educational profile, type and level of specialization;
5. Implementing the strategies and development plans of the police;
6. Establishing a system for knowledge sharing and knowledge management; and
7. Providing an objective system for personnel tracking and management that would be based on knowledge and performance.

Awareness of adapting the police to social changes is not new, but it is relevant. Through the analysis of patterns of immigration and increasing of the accountability of the police, Bayley and Nixon[6] speak of a changing environment for the police. Sklansky[7], Weisburd and Neyroud[8] as well as Travis and Stone (2011), talk about new elements of police professionalism as a reaction to changes in the working conditions of the police. In order for a police organization to be efficient, it is necessary to critically examine all external and internal factors that can affect the success in achieving this goal. The characteristics of crime that need to be taken into account when defining the general elements of learning and work profiles are first of all:

1. Forecasting entire crime (the number of offenses and trends);
2. Forecasting types of crimes (including the manner and means of performing them);
3. Forecasting profiles of the most common offenders;
4. Forecasting the most common objects of criminal offenses;
5. Forecasting the spatial and temporal particularities of crime.

These factors, in combination with other relevant factors are the criteria for the analysis of: the required number of police officers (the number of offenses and their trends); the required type of specialization (the structure of criminal acts); criminologist's job profile (profile of the perpetrators of the offense); work priority (routing measures of protection towards the most frequent objects of attack); the models of work organization (temporal and spatial distribution of offenses).[9]

Police managers should be competent and educated for strategic planning, which should keep pace with the three most significant social trends:

6 Bayley, D.H. and Nixon, C., "The changing environment police 1985-2008", 2010, *New Perspectives in Policing Bulletin*, Washington, D.C.: US Department of Justice, National Institute of Justice. NCJ 230, 576th.
7 Sklansky, D.A., "The persistent pull of police professionalism", 2011, *New Perspectives in Policing Bulletin*, Washington D.C.: U.S. Department of Justice, National Institute of Justice. NCJ 232,676th
8 Weisburd, D. and Neyroud, P., "Police science: toward a new paradigm", 2011, *New Perspectives in Policing Bulletin*, Washington D.C.: U.S. Department of Justice, National Institute of Justice. NCJ 228922.
9 Djurdjević, Z. and Radović, N., *Criminalistics operatives*, Belgrade: Academy of Criminalistic and Police Studies, 2012, p. 17.

1. The development of information technology;
2. Globalization, and
3. Protection of human rights.

INFORMATION TECHNOLOGY (IT)

The development of information technology is a useful means for solving various problems and tasks. It has led to the situation in which public administration faces changes at different levels, ranging from citizenship (citizens becoming participants in governance), through the nature of public service jobs (in terms of skills, work processes and job design), organizational changes (from a hierarchical to a more horizontal structure, to network or even virtual organizations) to the entire government (from classic bureaucracy to New Public Management and to network and digital governance).[10] The achievements of information technology influence the police in two ways: as a tool or as an object of actions of offenders and as means of improving the efficiency of police.

Alkaabi and associates[11] classify cybercrime as crime where the computer is the target of a criminal activity and crime where the computer is the tool to commit a crime. Continuous development and availability of information technology has contributed to the increased use of it, and also the growing number of attacks on systems protected by the perpetrators. Unauthorized deletion, alteration, concealment or in other ways making computer data or programs unusable, bank frauds, frauds with credit cards, frauds in business operations, making pornographic material available to persons in different parts of the world, the promotion of racial hatred and religious extremism are just some of the incriminating acts that can be committed more easily with the help of information technology.

The first step in confronting this type of crime at the international level was the Council of Europe Convention on Cybercrime adopted in Budapest on November 28, 2001. Before that, the countries where information technologies were developing faster, had adopted a number of different legal acts at the national level in order to prevent the commission of cybercrime offenses (e.g. the USA in 1986, Australia in 1988, UK in 1990, and Holland in 1993). In the Republic of Serbia the first offenses against the security of computer data were introduced into the criminal legislation in 2003 by the amendments to the Criminal Law, in the way that they accepted the solutions of the Draft document on Criminal Code of the Federal Republic of Yugoslavia from February 2000.[12] Taking into account the specificity of these offenses, the need for a separate working profile of those in charge of proving procedures (collecting specific types of evidence, digital evidence), the Law on organization and jurisdiction of state authorities to combat cybercrime was adopted, which helped particularly specialized organizational process of proving to be formed (2005, Articles 4 through11).

Great social danger and material damage require intensive approach to the development of human resources for the prevention of these crimes. Cybercrime is evolving rapidly, which requires the state authorities involved in their prevention and proving to have comprehensive computer knowledge to understand trends and patterns of development of information

10 Şandor, S.D., "ICT and Public Administration Reforms", 2012, *Transylvanian Review of Administrative Sciences,* vol. 36E, pp. 155-164.
11 Alkaabi, A., G., Mohay, M., McCullagh, A., J. and Chantler, A., N., "Dealing with the problem of cybercrime", *Conference Proceedings of 2nd International ICST, Conference on Digital Forensics & Cyber Crime*, 4–6 October 2010, Abu Dhabi, [Online] at http://eprints.qut.edu.au/38894/1/c38894.pdf, accessed February 17th, 2012.
12 Stojanovic, Z., *Review of the Criminal Code*, Belgrade: Official Gazette, 2006, p. 663.

technologies and their possible misuse. To achieve this goal it is necessary to harmonize and synchronize the activity of a large number of organizations, not just of those that are involved in the process of proving, but also of those whose networks can be used for committing a criminal offense or possibly cause some damage. A major contribution in the fight against cybercrime is given by the European Cybercrime Centre in a way that they provide assistance to organizations outside the criminal justice system.

Another very important aspect that information technologies have is the development capacity of the police in the process of proving crimes and organizing and coordinating the work of police officers. The use of software enables collection, storage and search of large amounts of data that contribute to the efficiency of the police, above all in detecting and proving criminal offenses. There are specialized types of software for the analysis of certain offenses or groups of offenses, such as Automated Tactical Analysis of Crime, CrimeStat, Holmes, I2, Viclas, Dragnet, etc. In addition, the use of software contributes to more efficient organization of police work (for example: GeoBalance, StaffWizard, The School Crime Operations Package, etc.). In Serbia the police also use an electronic diary for registration of crimes and offenses. In addition, crime mapping in the function of problem-oriented work is of special significance for the organization of the police.[13]

Information technology is important and can be significantly used in education. Some police trainings can be automated and conducted individually in the period suitable to the officer and the organization, thereby reducing costs and work absence. This is particularly important given that a lack of resources, lack of time and difficult access, as well as the low level of information could impede the learning process during the service.[14] Internet and Forensic Expert Forum – IFOREX takes an important place within the Europol for the exchange of best forensic practices and experiences. The Europol invests a lot in Computer Forensic Network which functions as a horizontal system that supports intelligence and operational activities in the fight against cybercrime. In order to protect the work of Europol, there is a supervision authority in charge of full respect of the principles of data protection while the communication uses two information systems – Europol Information System and Europol Platform for Experts. Europol undertakes a number of activities in the field of education and supports the European Cybercrime Training and Education Group. Information technology increases the efficiency of police officers and encourages the exchange of information, promotes horizontal versus vertical communication. This raises the question of changes in the traditional ways of managing police organizations and the need for building a new system of accountability, the ways to verify the effectiveness and achieving the goals of the profession.

GLOBALIZATION

By using global information systems the cooperation and communication between people has been made easier. Something that comes with this trend is the increase of transnational organized crime. Weapons of mass destruction are easier to produce in some countries where they are smuggled from and used in other countries. Drug smuggling, human trafficking, trafficking in children for adoption, making pornographic material available, bank frauds and other similar crimes with the help of the Internet are being committed in more than one country.

13 Milic, N., "Mapping crime in the function of problem-oriented policing", 2012, *Journal of Criminalistics and Law*, no. 1, pp. 123-140.
14 Ciolan, L., Stingu, M. and Marin, E., "The human factor: training and professional development as a policy tool", 2014, *Transylvanian Review of Administrative Sciences*, vol. 43E, pp. 48-67.

Tax evasion and frauds done by founding phantom companies have resulted in enormous material damage. Herman van Rompuy points out that due to tax evasion and fraud Europe loses 1 000 billion Euros annually and that the key to a well-functioning economy and social justice is in effective tax mechanisms (AFP, 06/05/2014). In 2008, the EU failed to adopt a directive on the exchange of banking data because of the opposition from Luxembourg and Austria, which demanded that similar conditions should also be imposed to certain countries which are not the EU members: Switzerland, Monaco, Andorra, San Marino and Liechtenstein. The mentioned problem was overcome by the adoption of the Declaration on Automatic Exchange of Information in Tax Matters at the meeting of the Organization for Economic Cooperation and Development (OECD) at the ministerial level in Paris in 2014. The declaration was signed by 47 countries, among the OECD member countries and the G20, and a number of other countries, including Singapore. Transnational cooperation of organized criminal groups and the degree of social danger can be indicated by the revenues that these groups make from drug trafficking and the amount of money laundered through financial institutions. In analysing these data one needs to be careful because these estimates cannot completely cover dark field of crime. The most quoted data in this field are the data of the International Monetary Fund. Meta-analysis of the results from various studies indicates that the revenues of the overall crime in 2009 were probably about 3.6% of gross domestic product (GDP) at the global level which is equivalent to 2.1 trillion dollars. Income from drug trafficking and other offenses committed on the territory of several countries (global level) in the first decade of this century are estimated to be around 650 billion on average per year or 1.5% of world GDP. According to the estimates, the revenues in 2009 were 870 billion dollars (UNODC, 2011, p. 7).

These data indicate that the global nature of crime, especially organized crime, requires the definition of transnational strategy, whose starting point should be the active participation of all, both individual countries and international institutions. National borders are often an obstacle to effective response and sometimes they are protection from criminal responsibility for the perpetrators. The assumption of international cooperation is to define a platform for the improvement of joint activities in the prevention, investigation and prosecution, which would consist of harmonization of legal regulations, standards of conduct and the exchange of good practice. Countries and police organizations are aware that an effective system for combating international crime requires joint activities. Intensive, legally defined police cooperation of interested countries is a necessity. To achieve a satisfactory level of efficiency, it is necessary to harmonize the legal framework of cooperation, including the work on harmonization of basic legal acts to combat crime (above all the Criminal Code and the Code of Criminal Procedure), the standards and procedures of police action. Taking into account the status and plans of the Republic of Serbia, attention will be focused on harmonization of the above mentioned elements with the EU standards. These trends can be accepted as a part of the concept of global education, whose purpose is to enable individuals to acquire knowledge and develop skills and attitudes necessary for responsible life in a globalized world society.[15] In spite of international conventions, treaties and examples of good police cooperation when an obstacle appears, such as differences in legal systems, the extradition or confiscation of illegally obtained property becomes impossible.

15 Milutinovic, J., "Social reconstruction and global education", 2013, *Social science journal 'Themes'*, no. 2, p. 536.

HUMAN RIGHTS

Throughout history human rights have significantly evolved and transformed in many ways.[16] Efficient opposing to contemporary forms of crime often raises the question of the relation between the increase in police powers and the protection of human rights. Uncritical acceptance of the legal strategy expansion of police powers leads to a larger number of legal options for restricting human rights and freedoms. The point is to find the necessary balance between the extension of the authority and functions of the police and the respect of human rights standards.

In the United States in the early 20th century, August Vollmer pointed out that police officers should be properly educated and trained and then he employed the college students as police officers at Berkley police department. Presidential Commission on Law Enforcement and Administration of Justice in the country in the late 1960s, and the National Advisory Commission on Criminal Justice Standards and Goals in the early 1970s pointed out that every police agency should require the completion of four-year education at an accredited college no later than 1982 as the minimum education level.[17] Nevertheless, only 1% of local police departments in the country require a four-year college level, and this difference was the result of a small number of empirical evidence that education had the desired effect on the behaviour of the members of police force.[18]

The commitment of police officers to the protection of human and civil rights and freedoms depends significantly on the attitudes of police officers towards the way in which they need to control crime and in this regard, in which way they should co-operate with the citizens and select other methods to control crime. These attitudes are largely formed during the process of education and training. There is no doubt that priority should be given to preventive and proactive methods and means of crime control, or at least to the process of putting prevention into balance with repressive activity.[19] Numerous studies have been conducted in the United States since 1960s and they have attempted to empirically examine the influence of higher education on the attitudes of police officers. It could be said that the conclusions of these studies showed that the police officers who had college education held less authoritarian, rigid and punitive beliefs than those who did not have college education.[20] Thus, college education definitely has positive influence in this direction and realistically contributes to the adoption of attitudes in favour of establishing partnerships with citizens and institutions in the local community, which is essential for the effective prevention of crime.

In the past, scientists tried to explore the influence of higher education on the behaviour of police officers, particularly the deprivation of liberty and the use of force, but a lot of these works had poor methodology (inadequate samples and the lack of control of theoretically relevant variables) and they were aimed at determining this influence on one of these behaviours of police officers.[21] In an attempt to overcome some of these limitations, the survey was conducted in two medium-sized cities (Indianapolis, Indiana and St. Petersburg, Florida) in the United States, as part of the Neighbourhood Policing Project in order to determine the effects of education of police officers on three key points in decision-making – the arrest (detention),

16 Simović, D., Avramović, D. and Jugović, S., "Evolution and transformations of human rights", 2013, *Social Sciences Journal 'Themes'*, no. 4, p. 1528.
17 Scott, J., Evans, D. and Verma, A., "Does higher education affect perceptions among police personnel? A response from India", 2009, *Journal of Contemporary Criminal Justice*, vol. 25, no. 2, pp. 214-236.
18 Rydberg, J. and Terrill, W., "The effect of higher education on police behaviour", 2010, *Police Quarterly*, vol. 13, no. 1, pp. 92-120.
19 Vuković, S., *Crime Prevention*, second amended and supplemented edition, Belgrade: Academy of Criminalistic and Police Studies, 2014, pp. 238-241.
20 Rydberg and Terrill, 2010, *op. cit.*
21 *Op. cit.*

search and use of coercion.[22] The results of the analysis showed that higher education had no effect on the probability of arrest or search during the meeting of the police and a suspect, but that college education significantly reduced the likelihood of use of coercion.

Another survey on the influence of education and work experience on the use of force was conducted within the same project in Indianapolis and St. Petersburg and the results showed that the policemen who had any kind of college education used verbal force significantly less when meeting citizens than the police officers who had secondary school education, while those police officers who had completed a four-year college used less physical force.[23] On the other hand, police officers with more experience in dealing with citizens used less both verbal and physical violence. Therefore, both college education and experience are in relation to the use of coercion. Although higher levels of education and experience have influence on force being used less, it was not determined that the presence of both elements provided some added value. The results indicate that police departments should consider adopting some form of requirement for college education, and maybe a four-year college education, as well as patrol officers whose appointment will depend on experience. Appointment of officers on the basis of experience may be difficult because of the natural tendency that senior police officers must be withdrawn from patrol and especially from some shifts. In order to overcome this, the coordination of senior and junior officers should be taken into account that can help in 'learning the ropes' from senior police officers, and additional payments may be introduced for senior police officers working with the younger ones in that direction.[24]

Education and training of police officers have influence on creating the police culture, which represents a set of moral norms and principles that determine what the police are and the way they conducts their work, and it significantly affects the manner of performing police duties by police officers, and ultimately their relation to the citizens' rights and freedoms.[25] Earlier studies were directed towards a monolithic culture within the police service, and now there is a general agreement that the police service includes numerous cultures with their negative aspects, among which the literature focuses on racism, the domination of men, cynicism and isolation.[26] The impact of these negative aspects of police cultures should be reduced through education, since they can occur as early as in the process of education in institutions of higher education, as well as during training. Many believe that there is still reluctance by the police to really address the issue of discrimination in their ranks and their institutions for training and that discrimination prevails today in the police service, but in a less obvious form.[27]

Education of police officers is an important process, hence the expression of many forms of unethical behaviour and breaches of discipline during the process of their education may represent an alarm signal in order to take adequate measures to prevent the possibility of manifestation of not only unethical, but also of criminal behaviour later in service. The participation of police officers in training for the qualification and professional development at universities highlighted a problem of their academic offenses, but universities have devoted relatively little attention to the problem.[28] Police students involved in academic offenses are faced with the possibility of severe sanctions imposed by fellow students in other programs,

22 *Op. cit.*
23 Pauline, A., E. III and Terrill, W., "Police education, experience and the use of force", 2007, *Criminal Justice and Behaviour*, vol. 34, no. 2, pp. 179-196.
24 *Op. cit.*
25 Macvean, A. and Cox, C., "Police Education in a University Setting: Emerging Cultures and Attitudes", 2012, *Policing: A Journal of Policy and Practice*, vol. 6, pp. 16-25.
26 *Op. cit.*
27 *Op. cit.*
28 Stout, B., "Professional ethics and academic integrity and police education", 2011, *Policing: A Journal of Policy and Practice,* vol. 5, no. 4, pp. 300–309.

because they may face direct sanctions by the employer and may cause damage to their reputation that could negatively affect their future career. In addition, an increasing number of police forces are engaged in partnerships with universities for basic police training, and the largest number of such arrangements include the exchange of information, which means that employers in the police are required to respond in some way to academic violations carried out by police students and one of these problems is plagiarism in university education.[29]

A key factor in the protection of human rights and freedoms is also the way of managing the police organization, and this factor is also significant in shaping police culture and its relation to its negative aspects. Leadership plays a key role in achieving the desired results in both formal and informal groups and inadequate leadership in policing can lead to significant consequences for the service and its people, violations of professionalism, integrity, responsibility and rights.[30] While trying to determine how the best leadership skills can be developed and what the obstacles along the way are, the students of FBI National Academy were interviewed (managers with a medium duration of their career) and it was found that the participants pointed out that the best leadership skills were developed through a combination of education, experience and mentoring.[31] Subjects covered by the survey indicated that developing effective leadership depended on the ability to overcome obstacles in the profession and obstacles at the level of an individual officer. Limited resources, macro and micro aspects of police culture and failures of leadership by the current leaders were seen as factors that reduce the growth of effective leadership practices. A small number of respondents believed that leaders were born being leaders, while a majority believes that successful leaders were created or had innate skills that could be strengthened through education, training and experience. Some respondents felt that these processes should begin as early as possible in their career of police officers as a part of the training before the service. Although not all the students would become leaders, some respondents considered it useful for every police officer to know the basics of theory and leadership skills because such training could help them become more successful in mobilizing citizens, in coordination between fellow colleagues and making more efficient work of their organizational units easier. Lack of timely education and training influenced the executives to develop deeply ingrained bad habits, ill will, miss useful opportunities and 'burn bridges' between them and co-workers, community members and the broader professional community.[32]

Another survey also pointing out the importance of leadership has been conducted on a sample of police officers in India, the country where there are strong demands to improve the services that the police provide to citizens through education.[33] The goal of this study was to determine whether better trained police officers perceived their responsibilities differently (their role, work values, stress and management problems). The results showed that education had a marginal impact and that higher education did not lead to the desired perception among police officers. It seemed that higher education had made the police officers become more rigid and less idealistic in their views. The results showed that it was more likely that they did not agree with the way the law was applied, or with problem-solving and what was particularly disturbing is the fact that they disagreed on the importance of protecting the rights of citizens. However, those with higher education who were recently employed strongly agreed that civil rights had to be protected. However, it seems that this research shed light

29 *Op. cit.*
30 Schafer, A.J., "Developing effective leadership in policing: perils, pitfalls, and paths forward", 2009, *Policing: An International Journal of Police Strategies & Management*, vol. 32, no. 2, pp. 238-260.
31 *Op. cit.*
32 *Op. cit.*
33 Scott, J., Evans, D. and Verma, A., "Does higher education affect perceptions among police personnel? A response from India", 2009, *Journal of Contemporary Criminal Justice*, vol. 25, no. 2, pp. 214-236.

on the factors that have contributed to the emergence of such attitudes. Police officers with higher education demanded greater accountability and support from management, especially in terms of external adverse impacts. Experience from the research in India showed that education alone would not make much difference in the perceptions and attitudes of police officers towards the desired direction and that the management should influence the external pressures that affect the organization of the police, such as the media and insufficient budget. In addition, it is important to pay attention to disciplining those police officers who violate the norms and to honouring those who demonstrate work skills. If such an environment is provided, the introduction of trained police officers will facilitate the development of positive ethic and more responsible work values within the organization.[34] However, it is encouraging that the police officers with higher education thought more of fulfilling the function of the community policing concept and they noticed less stress for non-routine aspects of police work.

DISADVANTAGES AND POSSIBLE DIRECTIONS FOR IMPROVING THE EDUCATION OF POLICE OFFICERS

The indicator for determining the functionality of the educational system is a high degree of correlation between employment and educational profile. Employment profile makes integrated framework of necessary knowledge required for solving specific tasks within the professional responsibility for a specific job. The educational profile is a system of scientific knowledge (subjects) and skills that criminalists, specialists adopt during education.[35] The above-mentioned facts clearly indicate that the current employment profile of police officer requires correction, and therefore the system of education that would constitute a "new type" of a police officer. The police are required to understand and apply the same law to all, without discrimination; understand the nature of social problems and the psychology of people with different attitudes towards the law; to manage and resolve professionally and efficiently the conflicts in the core of which there are cultural, racial, and socio-economic differences. A police officer must think and act proactively, not just reactively, and he/she must work on developing a partnership with the community.

A police manager must have energy that encourages the process to meet future challenges. The assumption for success is that the head of the police is a good organizer, a visionary, open, analytical, critical, self-critical and courageous enough to take risks and make tough decisions.

The abovementioned general elements of police integrity are the basis for defining of work and learning profiles and the criteria for the selection of candidates. In addition to the general requirements for admission to employment in state bodies (the Law on Civil Servants, 2005, Article 10), the Police Act establishes specific requirements: nationality (being a citizen of Serbia for five years before applying), psychological and physical ability to perform tasks and lack of security-related obstacles as well as competence (Article 137). These are not the elements of work profile, but the conditions that must be met by each candidate who wishes to enter into employment. The entrance examination must identify both general and specific elements. General elements derive from specific ethical components and specific elements derive from different types of work profiles (for example, a police officer of criminal police,

34 *Op. cit.*
35 Djurdjević, Z., "Methods of analysis of the functionality of the criminalistic police organization", in Milošević, G. (ed.), *The structure and functioning of the police organization (tradition, current state and perspective) -1,* Belgrade: Academy of Criminalistics and Police Studies, 2013, p. 220.

police of general competence or traffic police). This means that the entry test cannot be the same for all of them.

General elements show the attitude towards the profession, namely the manner of implementation of activities within the competence of the police, including the attitude towards clients, colleagues, professional obligations and responsibilities. Candidates should demonstrate communication skills, including tactics and diplomacy; show the focus on community; demonstrate a sense of personal responsibility, integrity and tolerance, problem solving skills; show confidence and composure in stressful situations; possess high levels of literacy; have respect for diversity; inclination to teamwork but also the ability for individual work; demonstrate honesty and trustworthiness; have proper respect for confidentiality; have the ability to act decisively; have tolerance and restraint.

Douglas[36] suggests that one of the first questions during an admission interview should be why someone wants to work in the police. Sennewald[37] states that the essential characteristics of the job profile are the standards of conduct of police officers and others who provide security.

The starting point for defining the specific elements of the work profile is the kind of police work. Specific tasks require a special set of personality traits of candidates if we want effective and functional police. The current system of higher police education is in accordance with modern scientific trends and social changes, especially after the accreditation of study programs Informatics and Computing and the Forensic Engineering at the Academy of Criminalistic and Police Studies. In this way the personnel is also recognized and they will play an important role in the process of demonstrating, proving and promoting the work of the police in the future. Firstly, there is digital evidence as the consequence of using computers as a tool or object of the criminal offense. Secondly, the introduction of modern information technology has been recognized as an important way to promote the work of the police (for example, the introduction of modern software for data processing and analysis). The development of forensics increases the efficiency of providing documentary evidence that legal proceedings can be made more efficient and shorter.

The field which offers the possibility of improving the organizational capacity of the system is functional specialization. Levels of specialization should make a constituent part of the system for monitoring and management of human resources. In accordance with the abovementioned, a system of specialization should be:

1. in accordance with the type of work of the Ministry;
2. in accordance with the level of tasks complexity.

Specialization must be a standard. For example, a police officer who wants to work in the criminal police must have the first level of specialization that refers to the most common tasks of criminal police. The question is how many levels of specialization are needed. When it comes to police organizations there are usually three levels, and this can be seen on the example of Great Britain, where their criminal police training program is titled "Professionalizing Criminal Investigation Program" (ACPO, 2005).

In our opinion, the level of specialization of criminal police should be set in a following way:

The first level: basic knowledge which may be needed for work on preventing, detecting, uncovering and proving the most common offenses is the requirement one has to fulfil if he/she wants to work in the Department of criminal police at police outposts.

36 Douglas, J., *John Douglas's Guide to landing a career in law enforcement,* New York: The McGraw-Hill companies, Inc., 2005, p. 10.
37 Sennewald, A.C., *Effective Security Management,* Amsterdam: Butterworth-Heinemann, 2011, p. 183.

The second level: the knowledge necessary for work on prevention, detection, uncovering and proving specific serious crimes (such as murder, rape, robbery) is the requirement one has to fulfil if he/she wants to work in a specialized Criminal Police Directorate.

The third level: knowledge in the field of crime prevention and criminal investigations is the requirement police officer has to fulfil in order to become chief of department or head of investigations.

The fourth level: knowledge in the field of managing the organizational units of criminal police is the requirement a police officer has to fulfil in order to become head or chief of the criminal police.

Without these specializations, a police officer could not be assigned to a certain job or to a particular organizational unit. Besides, in order to achieve a certain condition, the possibility of specialization, a candidate must have the corresponding work-related results (for example, as a condition to enrol in master studies the average mark rating must be 8.00). In this way we would come to the threshold of achieving the very important task of licensing officers to perform specific police tasks.

Attention should be paid to a special segment: knowledge management. The fact that Europol has the Knowledge Management Centre just shows the importance of knowledge management for police work. There are different methods for identifying the necessary knowledge and Gottschalk[38] lists three:

1. **The problem of decision analysis**. This method aims to identify the knowledge stating the problems that workers face, solutions they must provide, decisions they will have to bring and what knowledge they need for all of this.

2. **Critical success factors**. This method aims to identify and specify the factors that lead to success. Success can be at the level of headquarters, police divisions, and departments or sections, at the individual level or the level of the specific case.

3. **Ends means analysis**. This method aims to identify and specify demands and objectives that are expected through the analysis of examples of positive practice.

Knowledge management is the subject of various studies and there are a number of systems to manage it in many different organizations including the police. Housel and Bell[39] speak of a knowledge management system in accordance with 'The knowledge management maturity' model.

CONCLUSION

The institutional capacity of the police, which is "the most visible hand" of the state, shows most objectively their degree of democracy. By accepting these assumptions, the need for constant improvement of the police officers' educational system is clear. However, several facts should be taken into consideration. The police as a traditional, bureaucratic organization have to meet the demand for quick reform, which is not in their nature. Secondly, the identification of future challenges does not automatically imply the efficiency of the police. Identification of all characteristics of the transition is the first part of the process, and after that it should be defined what the police have to do in order to cope with the forthcoming issue and thereafter take such steps. More specifically, the reform depends on the most important resource of any organization, knowledge and willingness of its members to change.

38 Gottschalk, P., *Knowledge Management Systems in Law Enforcement: Technologies and Techniques*, London: Idea Group Publishing, 2007, p. 33.
39 Housel, T. and Bell, A. H., *Measuring and managing knowledge*, New York: McGraw-Hill Irwin, 2001, p. 136.

The result should be a dynamic profession that is capable of answering efficiently to every problem. Every day is a new challenge that requires the use of knowledge in new and different situations. The efficiency of solving the new situation requires constant education throughout a career as a professional opportunity for advancing. Adopting knowledge does not end upon completion of higher education; it is a process that should be seen as part of the daily duties if we want an effective and functional police organisation. In order to ensure the steady development and modernization it is necessary to constantly evaluate the educational system and all segments of the profession.

Universities have a key role in meeting the demands of the profession when they are in search for quality staff. The quality of university programs and knowledge management system largely determine whether any organization, including police will have a high degree of efficiency in the future, and it will be based on the work of motivated police officers. In order to achieve this, besides high-quality education system it is also necessary to define a system for evaluating performance, and mechanisms to protect the integrity of the police. In this sense, it is necessary to establish a special body for the protection and development of police integrity. Additionally, an important element is the creation of a registry of staff with accurate technical competence of each employee.

REFERENCES

1. Alkaabi, A., G., Mohay, M., McCullagh, A., J. and Chantler, A., N., "Dealing with the problem of cybercrime", *Conference Proceedings of 2nd International ICST, Conference on Digital Forensics & Cyber Crime*, 4–6 October 2010, Abu Dhabi, [Online] at http://eprints.qut.edu.au/38894/1/c38894.pdf, accessed February 17th, 2012
2. Association of Chief Police Officers, *Practice advice on core investigative doctrine*, 2005
3. Bayley, D.H. and Nixon, C., "The changing environment police 1985-2008", 2010, *New Perspectives in Policing Bulletin*, Washington, D.C.: US Department of Justice, National Institute of Justice. NCJ 230, 576th
4. Ciolan, L., Stingu, M. and Marin, E., "The human factor: training and professional development as a policy tool", 2014, *Transylvanian Review of Administrative Sciences*, vol. 43E, pp. 48-67
5. Douglas, J., *John Douglas's Guide to landing a career in law enforcement,* New York: The McGraw-Hill companies, Inc., 2005
6. Djurdjević, Z. and Radović, N., *Criminalistics operatives*, Belgrade: Academy of Criminalistic and Police Studies, 2012
7. Djurdjević, Z., Radović, N. and Vuković, S., "Police integrity and standards of work profile of police crime investigators", in Milošević, G. (ed.), *Archibald Reiss Days*, volume I, Belgrade: Academy of Criminalistic and Police Studies, 2013, pp. 159-168
8. Djurdjević, Z., "Methods of analysis of the functionality of the criminalistic police organization", in Milošević, G. (ed.), *The structure and functioning of the police organization (tradition, current state and perspective) -1,* Belgrade: Academy of Criminalistics and Police Studies, 2013, pp. 205-224
9. Gottschalk, P., *Knowledge Management Systems in Law Enforcement: Technologies and Techniques*, London: Idea Group Publishing, 2007
10. Housel, T. and Bell, A. H., *Measuring and managing knowledge*, New York: McGraw-Hill Irwin, 2001
11. Council of Europe, *"Convention on Cybercrime"*, adopted on 28 November 2001 in Budapest, ETS no. 185

12. Macvean, A. and Cox, C., "Police Education in a University Setting: Emerging Cultures and Attitudes", 2012, *Policing: A Journal of Policy and Practice*, vol. 6, pp. 16-25
13. Milutinovic, J., "Social reconstruction and global education", 2013, *Social science journal 'Themes'*, no. 2, pp. 517-533
14. Milic, N., "Mapping crime in the function of problem-oriented policing", 2012, *Journal of Criminalistics and Law*, no. 1, pp. 123-140
15. Ministry of the Interior, "*Development Strategy of the Ministry of Interior 2011-2016"*, 2010
16. Ministry of the Interior, Strategy: "*The introduction of e-learning as a support to the development of the training system in the Ministry of Interior",* 2011
17. The Organisation for Economic Co-operation and Development, "*Declaration on Automatic Exchange of Information in Tax Matters*", 2014
18. *Law on organization and jurisdiction of government authorities to combat cybercrime*, Official Gazette of RS, no. 61/2005 and 104/2009
19. *Civil Servants Act*, Official Gazette of RS, no.79/2005; 81/2005; 83/2005; 64/2007; 67/2007; 116/2008; 104/2009
20. Police Act, Official Gazette of RS, no. 101/2005; 63/2009; 92/2011
21. Pauline, A., E. III and Terrill, W., "Police education, experience and the use of force", 2007, *Criminal Justice and Behaviour*, vol. 34, no. 2, pp. 179-196
22. Rydberg, J. and Terrill, W., "The effect of higher education on police behaviour", 2010, *Police Quarterly*, vol. 13, no. 1, pp. 92-120
23. Şandor, S.D., "ICT and Public Administration Reforms", 2012, *Transylvanian Review of Administrative Sciences,* vol. 36E, pp. 155-164
24. Schafer, A.J., "Developing effective leadership in policing: perils, pitfalls, and paths forward", 2009, *Policing: An International Journal of Police Strategies & Management*, vol. 32, no. 2, pp. 238-260
25. Scott, J., Evans, D. and Verma, A., "Does higher education affect perceptions among police personnel? A response from India", 2009, *Journal of Contemporary Criminal Justice*, vol. 25, no. 2, pp. 214-236
26. Sennewald, A.C., *Effective Security Management,* Amsterdam: Butterworth-Heinemann, 2011
27. Simović, D., Avramović, D. and Jugović, S., "Evolution and transformations of human rights", 2013, *Social Sciences Journal 'Themes'*, no. 4, pp. 1527-1553
28. Sklansky, D.A., "The persistent pull of police professionalism", 2011, *New Perspectives in Policing Bulletin*, Washington D.C.: U.S. Department of Justice, National Institute of Justice. NCJ 232,676th
29. Stojanovic, Z., *Review of the Criminal Code*, Belgrade: Official Gazette, 2006
30. Stout, B., "Professional ethics and academic integrity and police education", 2011, *Policing: A Journal of Policy and Practice,* vol. 5, no. 4, pp. 300 – 309
31. The Government of the Republic of Serbia. "*Strategy on Education Development by 2020"*, Official Gazette of RS, no. 107/2012
32. The Government of the Republic of Serbia. "*Strategy on Development of E-Government in the Republic of Serbia for period 2009-2013"*, Official Gazette RS, no. 83/09, 5/10
33. The Government of the Republic of Serbia. "*Strategy on Development of Electronic Communications in the Republic of Serbia for period 2010-2020*", Official Gazette RS no. 68/10

34. The Government of the Republic of Serbia. "*Information Society Development Strategy in the Republic of Serbia*", Official Gazette RS, no. 51/10
35. The Government of the Republic of Serbia. "*Strategy on Adult Education Development in the Republic of Serbia*", Official Gazette RS, no. 1/2007
36. United Nations Office on Drugs and Crime, *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*, research report, Vienna: United Nations Office on Drugs and Crime, 2011
37. Vuković, S., *Crime Prevention*, second amended and supplemented edition, Belgrade: Academy of Criminalistic and Police Studies, 2014
38. Weisburd, D. and Neyroud, P., "Police science: toward a new paradigm", 2011, *New Perspectives in Policing Bulletin*, Washington D.C.: U.S. Department of Justice, National Institute of Justice. NCJ 228922

UDC: 323.118:796.332.093(497.11)
316.624.3(497.11)

PREDICTION MODEL OF THE YOUTH'S PREFERENCES REGARDING RACISM AT FOOTBALL MATCHES[1]

Sasa Milojevic, PhD[2]
Academy of Criminalistic and Police Studies, Belgrade
Bojan Jankovic, PhD
Academy of Criminalistic and Police Studies, Belgrade
Goran Vuckovic, PhD
Academy of Criminalistic and Police Studies, Belgrade

Abstract: The paper presents a qualitative and quantitative analysis of the phenomenon of racism at football matches in Serbia. The statistic analyses relate to the youth aged 14 to 19. The paper proves that (1) a large part of the population of the young perceives the problem of racism at football matches, but without recognizing racist outburst, and (2) that male gender, membership in fan groups, and alcohol consumption are the common characteristics which, independently or in interaction, characterize a portion of Serbian population prone to racist behaviour. Moreover, the predictive model presented in this paper indicates that (1) there is a significant portion of population of the youth (less than 10%) prone to racist behaviour, as well as (2) the necessity of creating programmes for prevention of racism to be implemented in schools based on education of recognition and avoidance of racism.

Keywords: racism, perception, prediction, youth, football

INTRODUCTION

Hooliganism of some fans at football matches is the decades-long problem that many European countries are confronted with. Despite the efforts of European countries to combat this type of violence, it is still present to a greater or lesser extent in almost all countries and is manifested through various forms. The most common are the following three: the use of pyrotechnic devices, prearranged violence, and violence associated with alcohol abuse, or violence committed by persons intoxicated by alcohol.[3] In the past three years, besides the listed, there has been a noticeable increase of another characteristic form of violent behaviour of fans or the occurrence of racist outbursts. This is shown in the latest annual report of the Standing Committee of the Council of Europe for implementation of the European convention on spectator violence and misbehaviour at sports events and in particular at football matches.[4] The report shows that Romania, Russia and Great Britain are facing an increased number of racist incidents at football matches. France has submitted detailed data for the report related

1This paper is the result of the research on project: "Management of police organization in preventing and mitigating threats to security in the Republic of Serbia", which is financed and carried out by the Academy of Criminalistic and Police Studies, Belgrade – the cycle of scientific projects2015-2019.
2 **Corresponding author:**sasa.milojevic@kpa.edu.rs
3 Milojević, S., & Janković, B. (2012). *Police measures and actions in confronting football hooliganism in some European countries.* Paper presented at the Archibald Reiss Days, Belgrade, pp. 613.
4 Quidt, J. d. (2012). Annual Report of the Stadnding committee, part II - questionnire on recent trends. Strasbourg: Council of Europe, Standing Committee (T-RV) – European Convention on Spectator Violence.

to racist incidents that have occurred in only one season, indicating that in the said country there is a serious problem with racism.[5]

In the Netherlands there has been the widespread thesis that there is not a big problem with racism there; however, the research conducted by Müller shows that racist incidents are not so rare.[6] Namely, the research was conducted in Amsterdam, using in-depth interviews with the most extreme white fans of the *Ajax* football club, and with the players of different origins. The research has shown that many players were insulted and humiliated on the basis of race, both by fans, and by teammates and opponents.

Since Great Britain, France and the Netherlands are states with mixed population and different races, it was perhaps to be expected that racism, as both sociological and a safety issue may occur in them. However, the problem of racism is present in the European countries where the population is almost exclusively white. Thus, in Russia, the problem of racism is expressed in everyday life, especially among the young population, and it is transferred to sports events or football matches.[7] There is a similar problem in Italy as well, especially with both the fascist and racist behaviour of football fans.[8] Racist outbursts in Ukraine are linked to fans of *Dynamo* Kiev, *Karpaty* Lviv and *Metalist* Kharkiv football clubs.[9] A number of racist incidents at football matches have also been recorded in Germany. Three forms of racist behaviour have been identified: (1) racist and extreme right-wing behaviour of fans, at or close to sports facilities, (2) racist insults among players, and (3) a systematic and politically motivated right-wing extremist propaganda and agitation in the context of football.[10]

RACIST OUTBURSTS IN SERBIA

In the last 25 years in Serbia, there has been a problem with hooliganism at football matches. Members of fan groups in Serbia are very young people, as reported in the police reports, in which a typical perpetrator of crimes and offenses associated with violence at football matches in Belgrade is an adolescent of the average 16.23 years of age.[11] The fact that a large number of young people are involved in violence at football matches was confirmed in the survey in which a number of police officers of the Intervention Unit of the Ministry of Internal Affairs of the Republic of Serbia were interviewed, the ones who secure sports events. Police officials declared that in 94% of cases the persons involved in the violence were aged 14 to 25, in 6% of cases they were aged 25 to 35.[12]

Although reports present no data on racism as the present problem in sports arenas, certain events in football stadiums indicate that the problem exists. On a larger scale, the issue of racism was raised for the first time after the football match played by Serbia's Under 21 team versus England's Under 21 team. Namely, on 16 October 2012, after the end of the game, there was a physical confrontation between players of both national teams, but also racist chants from the crowd on the stands addressed to English players with dark complexion when the

5 Ibid, pp. 6.
6 Müller, F. (2009). *Communicating Anti, Racism.* (doctorate Dissertation), University of Amsterdam, Amsterdam.
7 Watson, M. R. (2013). The Dark Heart of Eastern Europe: Applying the British Model to Football-Related Violence and Racism. *Emory International Law Review, 27*(2), pp. 1066.
8 Scalia, V. (2009). Just a Few Rogues?: Football Ultras, Clubs and Politics in Contemporary Italy. *International Review for the Sociology of Sport, 44*(1), pp. 49.
9 Klymenko, P. (2013). *The Politics of Football: Radical Nationalism and Discrimination in the European Football. Case Study: Ukraine.* (Master master thesis), Vienna, pp. 65.
10 Peucker, M. (2009). Racism, xenophobia and structural discrimination in sports: Country report Germany. Bamberg: European forum for migration studies (EFMS), pp. 16.
11 Otašević, B. (2010). Urban Environment and Violence in Sport. *Bezbednost, 52*(3), pp. 271.
12 Janković, B. (2010). Prevention of Violence at Sports Events. *Herald of Law, 1*(3), pp. 138.

home fans imitated the cries of monkeys. The UEFA opened the disciplinary proceedings and imposed penalties against players who participated in the conflict and the organizer of the match, the Football Association of Serbia. It was the first punishment for Serbia associated with racist behaviour at a football match.

Accordingly, this paper aims to answer the following questions: (1) whether the young population in Serbia perceives the problem of racism at football matches, and (2) whether there are common characteristics that, independently or in interaction, characterize young people prone to racist behaviour. By answering these questions, the problem of racism would be identified at an early stage of formation and its intensity would be determined for the timely action in various prevention programmes.

METHODS

In order to obtain data on participation of the youth in violence at football matches and their relation to hooliganism of fans, and - in that context - on the perception of young people about the problem of racism in football, a questionnaire was designed, comprising 42 questions, 18 of which relating to the issue of racism. The constructed measuring instrument was, to a greater extent, of the closed type, with a possibility to choose several of multiple choice answers, while for one question the only possibility was to give an open (free) response, and in 11 questions given to respondents, there was a possibility to give an open (free) response within the available closed responses. The completion of the questionnaire was anonymous.

The collected data were analysed using statistical analysis methods as follows: procedures that show descriptive parameters (frequency and percentage), $\chi 2$ test of independence which determined statistically significant differences between the groups being compared or determined a statistically significant relationship between individual responses, as well as the direct binary logistic regression to test the validity of the prediction model.

SAMPLE

Data on racism and the young at football matches were collected on a sample that included high school students aged 14 to 19 from the territory of the Republic of Serbia. Respondents were from 12 cities which had first division football clubs in the 2012/2013 season, namely from two schools closest to the football stadium in each city. Students were surveyed in schools; they were from two classes of all four grades. Based on these criteria, 3662 students were surveyed. If we take into account that, according to data from the Statistical Office of the Republic of Serbia, there were 280,422 students of that age at the beginning of the school year 2012/2013, the sample comprised 1.3% of the analysed population.[13] Bearing in mind that it was a stratified sample, its size fully represented the target population of school students aged 14 to 19.

The sample included 55.3% of male respondents. A quarter of respondents (actually 25.3%) participated in some kind of conflict because of sports. The sample comprised 14.7% of members of organized fan groups. A large number of respondents consumed alcohol (69.0%), a significant number abused drugs (9.6%); 27.3% of respondents had an unfavourable attitude towards the police, while 27.5% of them had a favourable attitude. Because of sport-related violence, 5.5% of the respondents were apprehended for violence related to sports events, 3.7% of them were filed civil charges, and 3.1% criminal charges by the police.

13 Statistical Office of the Republic of Serbia (2013). Upper Secondary Education in the Republic of Serbia, Beginning of 2012/2013 School year, pp. 28.

RESULTS AND DISCUSSION

The data collected during the survey are consistent with the findings presented in the last annual report of the Standing Committee of the Council of Europe for the implementation of the European convention on spectator violence and misbehaviour at sports events. Namely, a relatively small percentage of respondents (1.7%) insulted opponents at football matches because of religion, skin colour or other differences. However, the perception of young people about the existence of racism at football matches in Serbia is largely different.

THE YOUTH'S PERCEPTION OF RACISM AT FOOTBALL MATCHES

A certain number of respondents (10.2%) believe that at football matches in Serbia there is no problem with racism, but that is an invention by foreign media. 19.3% of respondents believes that there is no racism at football matches. A significant number of respondents were indecisive or declared not to know whether there was a problem of racism at football matches. The greatest number of respondents – 35.4% believes that there is racism at matches, but to a small extent, while 26.7% of respondents believe that there is racism at football matches to a large extent. By analyzing these data, it is evident that a large number of respondents (62.1% cumulative), identifies racism as a problem that occurs at football matches in Serbia. Similar results were shown in the online survey conducted in England, which showed that 61% of spectators on football matches experienced racist behaviour or were present during such incidents in the period from 2000 to 2009,[14] which is similar to data obtained in this study. The research conducted in Spain showed something similar,[15] as its results indicated that in this country there is a problem of racism at football matches, although the official documents show the opposite. In this study, racist outbursts in football stadiums of the first and second Spanish football league during the seasons 2004/05 and 2005/06 were analysed. During the two seasons there were a total of 47 racist incidents. In addition to a significant number of registered incidents, a large number of people took part in the alleged incidents. Specifically, the survey results stated that eight incidents involved fewer than five people, there were 60 people in one, 150 in another, and there were two incidents involving between 500 and 1,000 people; in two of them there were between 2000 and 3000 people, in five cases there were several thousand people involved, while in five incidents the number of participants has not been determined.

The problem of racism in sport in Serbia came to public attention after the events in the football match of Under 21 teams of Serbia and England, played in October 2012. In contrast to the perceived problem of racism at football matches in general, young people perceived the event in Kruševac quite differently. Almost half of respondents (49.7%) were not familiar with the event that raised a lot of interest of the domestic and European public. 13.0% of respondents think that there was no racist behaviour of local fans, while there are 13.5% of respondents who believe there was no racist behaviour by local fans, but only the response to unsportsmanlike behaviour of individual players in England's national team. Thus, a larger portion of respondents (cumulatively) believes there were no racist outbursts. On the other hand, 10.4% of respondents believe there were racist insults by a very small number of local

14 Cleland, J., & Cashmore, E. (2013). Football fans' views of racism in British football. *International Review for the Sociology of Sport*, 1-17. doi: 10.1177/1012690213506585, pp. 7.
15 Llopis-Goig, R. (2009). Racism and xenophobia in Spanish football: Facts, reactions and policies. *Physical Culture and Sport Studies and Research, 47*, 35-43.

fans aimed at dark complexion players of the England's national team, while 8.5% of respondents think that there were racist insults by a larger number of local fans. Bearing in mind that after conducting disciplinary proceedings, the UEFA confirmed that there was a racist outburst and penalized the Under 21 Serbian national team and its members, it is obvious that the perception of young people concerning the problem of racism is somehow distorted. On the one hand, they perceived the problem of racism at football matches in general, and on the other hand, in this particular case, they did not recognize the problem of racism.

CHARACTERISTICS OF YOUNG DISPLAYING RACIST ATTITUDES

Results of χ^2 tests showed statistically significant differences between characteristics of the young who display racist attitudes and those who do not. They started from the position that racist attitudes are displayed by those students who: (1) insulted opponents at a football match because of religion, colour or other differences; (2) believe that local fans did not display any racist behaviour at the football match in Kruševac between Under 21 national teams of Serbia and England and (3) believe that there is no racist behaviour on football matches in Serbia.

Accordingly, the statistical analysis showed that racist insults are often hurled by male (87.1%), members of fan groups (45.2%), who were involved in conflicts because of sports (74.2%), who regularly consume alcohol (85.5%) and abuse drugs (37.1%). These respondents have more significantly expressed unfavourable attitude towards the police (39.1%). They were apprehended by the police more often (33.9%), they were more often filed civil (25.8%) and criminal charges (19.4%) (Table 1).

Table 1: *χ^2 test characteristics of respondents – insulting opponents because of religion, skin colour or another difference.*

Statistically significant difference	N	χ^2	Sig.	ϕ
Gender	3656	24.41	0.00	-0.11
Fan group membership	3662	44.13	0.00	-0.15
Attitude towards the police	3604	45.57	0.00	0.11
Participation in conflicts because of sport	3662	77.24	0.00	-0.15
Alcohol consumption	3662	7.27	0.00	-0.05
Drug abuse	3662	51.66	0.00	-0.12
Apprehension because of violence in connection with sport	3602	96.20	0.00	-0.17
Civil charge filed because of violence in connection with sport	3612	83.85	0.00	-0.16
Criminal charge filed because of violence in connection with sport	3593	56.53	0.00	-0.13

Male (71.3%) members of fan groups (22.4%) who were involved in conflicts because of sports (32.7%) (cumulatively) believe that there is no racism at football matches. They more often have an unfavourable attitude towards the police (31.8%). They frequently abuse drugs (12.2%), they are more often apprehended by the police for violence at sports events (8.6%), they were filed more civil (6.4%) and criminal charges (5.1%) because of violence at matches (Table 2).

Table 2: *χ^2 test characteristics of respondents – perception of problems with racism at matches.*

Statistically significant difference	N	χ^2	Sig.	ϕ
Gender	3496	160.51	0.00	0.21
Fan group membership	3502	78.01	0.00	0.15
Attitude towards the police	3475	21.89	0.00	0.06
Participation in conflicts because of sport	3502	55.30	0.00	0.13
Drug abuse	3502	20.70	0.00	0.08
Apprehension because of violence in connection with sport	3479	25.61	0.00	0.09
Civil charge filed because of violence in connection with sport	3488	27.58	0.00	0.09
Criminal charge filed because of violence in connection with sport	3470	18.82	0.00	0.07

Male (40.3%) members of a fan group (23.6%) believe that there were no racist outbursts in Kruševac. They tend to have an unfavourable attitude towards the police (34.6%). Those respondents more often consume alcohol (30.3%) and abuse drugs (40.3%). They often had conflicts because of sport (43.1%), the police have often apprehended them because of conflict in matches (55.6%), they have more often been filed civil (53.8%) and criminal charges (57.8%) (Table 3).

Table 3: *χ^2 test characteristics of respondents – whether there were racist outbursts at the Under 21 match of national teams of Serbia and England.*

Statistically significant difference	N	χ^2	Sig.	ϕ
Gender	3479	523.65	0.00	0.39
Fan group membership	3485	199.61	0.00	0.24
Attitude towards the police	3461	45.00	0.00	0.08
Participation in conflicts because of sport	3485	245.12	0.00	0.27
Alcohol consumption	3485	22.81	0.00	0.08
Drug abuse	3485	45.24	0.00	0.11
Apprehension because of violence in connection with sport	3470	128.930	0.00	0.19
Civil charge filed because of violence in connection with sport	3470	77.98	0.00	0.15
Criminal charge filed because of violence in connection with sport	3451	72.88	0.00	0.15

Previous analyses indicated that the characteristics of respondents who believe there were no racist outbursts in Kruševac are very similar to characteristics of respondents who believe that Serbia has no problem with racism, or the characteristics of respondents who have shown racist behaviour.

PREDICTIVE MODEL OF PREFERENCES OF YOUNG TOWARDS RACISM

Conducted analyses have imposed several important conclusions. Namely, out of the total number of respondents who answered that they had insulted opponents on racist grounds at a football match, 66.0% believe that in the game Under 21 teams of Serbia and England in

Kruševac there were no racist incidents of domestic fans, and 80.6% believe that Serbia has no problem with racism. χ^2 test between these three characteristics of the respondents indicates a significant association that can be estimated as mean in a statistical sense[16] (Cohen, 1988) (χ^2 (1, n=1629) = 242.988, p = 0.000 (with correction according to Yeats), whereby the coefficient is fi = 0.387).

On the basis of this result, and relying on facts that (1) the event in Kruševac was rated as the racist outburst by the international body, (2) together with deciduous statements of a part of respondents that they had participated in racist behaviour at football matches – it can be concluded that the population which does not perceive the problem of racism in Serbia represents a part of the youth who could potentially participate in a racist incident. This is primarily due to the fact that a part of the population does not adequately perceive racism or anti-social and delinquent behaviour motivated by racism. This is the reason why it is important to identify characteristics of the youth population who could potentially participate in racist incidents. Identification of these characteristics was carried out in four steps.

First, the direct binary logistic regression was used to assess the impact of multiple characteristics of young people in Serbia on the probability that respondents would answer that there is no problem with racism in Serbia. The model comprised nine characteristics derived in previous analyses (χ^2 test) that may be of importance as predictors of the model (gender, attitude towards the police, alcohol consumption, drug abuse, membership in fan groups, conflicts because of sport, apprehension because of violence at sports events, civil or criminal charges filed). The whole model (with all predictors) was statistically significant, χ^2 (9, n=1852) = 137,112, p = 0.000, indicating that the model distinguishes respondents who answered and those who did not answer whether there was a problem with racism in Serbia. The model as a whole explains between 7.10% (r^2 Cox-Snell) and 10.0% (r^2Nagelkerke) variance in respondents' attitudes towards racism in Serbia and accurately classifies 69.8% of cases. As shown in Table 4, four characteristics (predictors) provided a unique statistically significant contribution to the model (gender, alcohol consumption, drug abuse, and membership in fan groups). The strongest predictor of the view that there is no problem with racism in Serbia was gender with the ratio of probability of 2.27. This shows that male respondents are twice more likely to believe that there is no problem with racism in Serbia, with all other factors in the model being equal. The quotient of probability for alcohol consumption is 0.78, which is lower than 1, indicating that respondents who do not consume alcohol are 0.78 times less likely to respond that there is no problem with racism in Serbia, with all other factors in the model being equal.

Table 4: *Model of prediction of the attitude that there is no problem with racism in Serbia.*

Characteristics (predictor)	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
							Lower	Upper
Gender	0.82	0.11	52.02	1	0.00	2.27	1.82	2.82
Alcohol consumption	-0.24	0.12	4.38	1	0.04	0.78	0.62	0.96
Drug abuse	0.51	0.18	8.44	1	0.00	1.67	1.18	2.35
Membership in fan groups	0.53	0.15	12.81	1	0.00	1.67	1.27	2.27

In the second step, the direct binary logistic regression was used to assess the influence of the same characteristics of the youth in Serbia on probability that respondents would answer

16 Cohen, J. (1988). *Statistical power analysis for the behavioral sciences (2nd edn.)*. Hillsdale, New Jersey: Lawrence Erlbaum Associates.

that there were no racist outbursts by local fans during Under 21 football match of national teams of Serbia and England in Kruševac. The model was the same as in the previous analysis. The whole model (with all predictors) was statistically significant, $\chi 2$ (9, n = 939) = 38.912, p = 0.000, explaining between 4.10% and 5.5% of the variance, and accurately classifying 60.2% of cases. As shown in Table 5, three characteristics (predictors) provided a unique statistically significant contribution to the model (gender, alcohol consumption, and membership in fan groups). The strongest predictor of the view that there were no racist outbursts by local fans during Under 21 football match of national teams of Serbia and England in Kruševac was alcohol consumption with the ratio of probability of 1.71.

Table 5: *Model of prediction of the attitude that there were no racist outbursts during the match between Under 21 teams of Serbia and England.*

Characteristics (predictor)	B	S.E.	Wald	df	Sig.	Ex-p(B)	95% C.I. for EXP(B)	
							Lower	Upper
Gender	0.39	0.16	5.94	1	0.02	1.48	1.08	2.02
Alcohol consumption	0.54	0.16	11.93	1	0.00	1.71	1.26	2.32
Membership in fan groups	0.53	0.18	8.99	1	0.00	1.7	1.2	2.41

In the next step, the identical method was used to assess the impact of the same characteristics of young people in Serbia on probability that respondents insulted opponents at football matches because of religion, skin colour or another difference. The model was the same as in the previous two analyses. The whole model (with all predictors) was statistically significant, χ^2 (9, n=1974) = 61.007, p = 0.000 explaining between 3.0% (r^2 Cox-Snell) and 18.3% (r^2Nagelkerke) variance, classifying accurately 78.2% of cases. As shown in Table 6, four characteristics (predictors) provided a unique statistically significant contribution to the model (gender, alcohol consumption, membership in fan groups, and participation in conflict because of sport). The strongest predictor of respondents' participation in insulting opponents on racist grounds was participation in conflicts because of sports with the ratio of probability of 3.97.

Table 6: *Model of prediction of respondents' participation in racist insulting the opponents.*

Characteristics (predictor)	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for EXP(B)	
							Lower	Upper
Gender	0.88	0.52	2.91	1	0.04	2.42	0.88	3.68
Alcohol consumption	0.11	0.48	0.06	1	0.01	1.12	0.44	2.87
Membership in fan groups	0.19	0.4	0.23	1	0.03	1.21	0.55	2.66
Conflicts because of sport	1.38	0.48	8.38	1	0.00	3.97	1.56	5.1

Preliminary analysis of the direct binary logistic regression showed that male gender, alcohol consumption, and membership in fan groups are common predictors for all three dependent variables – that the respondent would have the attitude that there is no problem of racism in Serbia, that there were no racist outbursts by local fans during Under 21 football match of the national teams of Serbia and England in Kruševac and that the respondent participated in insulting opponents at football matches because of religion, colour or other differences.

Accordingly, the fourth and final step of identifying characteristics of the youth population that could potentially participate in racist incidents included the analysis using the direct binary logistic regression for the model in which predictors are the mentioned three characteristics of the youth in Serbia (Table 7).

Table 7: *Models of prediction of dependent variables with three predictors.*

Dependent variable	Characteristics (predictor)	B	S.E.	Wald	df	Sig.	Ex-p(B)	95% C.I. for EXP(B)	
								Lower	Upper
There are no problems with racism in Serbia	Gender	0.88	0.08	116.25	1	0.00	2.41	2.06	2.83
	Alcohol	-0.11	0.08	1.61	1	0.02	0.9	0.77	1.06
	Fan group	0.45	0.1	20.2	1	0.00	1.57	1.29	1.92
There were no racist outbursts during the match of Under 21 national teams	Gender	0.55	0.12	22.11	1	0.00	1.74	1.38	2.18
	Alcohol	0.33	0.11	8.83	1	0.00	1.39	1.12	1.73
	Fan group	0.44	0.13	12.11	1	0.00	1.55	1.21	1.99
Participation in racist outbursts	Gender	1.37	0.39	12.26	1	0.00	3.94	1.83	8.48
	Alcohol	0.86	0.37	5.55	1	0.02	2.36	1.16	4.82
	Fan group	1.23	0.27	20.95	1	0.00	3.41	2.02	5.76

It is obvious that the model which comprises three characteristics of youth – gender, alcohol consumption, and membership in fan groups predicts with a high probability (75.4%) that the respondent's attitude will be that Serbia has no problem with racism, that during the aforementioned Under 21 football match there were no racist outbursts, and that he will make racist insults aimed at opponents during a football match. The strongest predictor was gender, on the basis of which it can be concluded that the young male population belong to the minor potential holders of racist outbursts. This is followed by membership in the fan group, and finally alcohol consumption.

Previous analyses allow us to conclude with a high degree of reliability that young male alcohol consumers who are members fan groups represent the population that can potentially participate in racist outbursts. These findings are consistent with the previous studies by which men are much more likely to participate in racist behaviour,[17] and that racist incidents often have a background in situational factors – the effect of alcohol, together with the influence of "mass psychology" deriving from the membership in the club support group, at which the philosophy of the fan group that gathers the supporters sometimes has a racist point of view (Arishita, 2010).[18]

This study points to a very significant connection between all three characteristics – male gender, membership in a fan group and alcohol consumption – with a very high probability of a racist outburst deriving from it. In the studied sample, which is fully representative for the high school population in Serbia, 9.42% of respondents have characteristics that put them into the group of potential participants in racist outbursts, which is a significant percentage of young people and consequently requires taking serious measures on a wider social level.

17 Sidanius, J., & Veniegas, R. C. (2000). Gender and race discrimination: The interactive nature of disadvantage. In S. Oskamp (Ed.), *Reducing Prejudice and Discrimination* (pp. 47-69). Mahwah, New Jersey: Lawrence Erlbaum Associates Publishers.
18 Arishita, K. M. (2010). *Racism in soccer: Eliminating soccer racism and using sport as a vehicle for national change.* Texas A&M University.

CONCLUSION

Regardless of favourable reports of the Standing Committee of the Council of Europe for implementation of the European convention on spectator violence and misbehaviour at sports events, the incident in Kruševac in 2012 showed that there are racist outbursts at football matches in Serbia and that racism exists. The conducted survey showed that the percentage of respondents who participated in racist behaviour at football matches is relatively small, but also that the percentage of those who believe there were no racist outbursts in Kruševac, or that there is not a problem of racism in Serbia is relatively large.

Using statistical analysis, it is proved there is a significant relationship between respondents who have the attitude that in Serbia there is no problem with racism, those who believe there were no racist incidents in Kruševac and those involved in insulting opponents at football matches, that is, those who belong to population that participates or may potentially participate in racist behaviour. Initial statistical analyses indicated that these respondents have a number of common characteristics: they are male, they have an unfavourable attitude towards the police, consume alcohol and abuse drugs, they are members of fan groups, they had conflicts because of sport due to which they were apprehended by the police, they were filed civil and criminal charges.

These characteristics were used to create a predictive model which first proved that only three characteristics (gender, alcohol consumption, and membership in fan groups) really describe the respondents as the population prone to racism. The final statistical analysis has definitely proved that such respondents were precisely described with a high probability on the basis of these three characteristics.

Starting assumptions (1) that the young population in Serbia perceives the problem of racism at football matches, but in this particular case it does not recognize the racist outburst and (2) that the male gender, membership in fan groups and alcohol consumption are common characteristics that independently or in interaction characterize young people prone to racist behaviour have been proved. Moreover, the predictive model presented in this paper indicates that (1) there is a significant population of the youth in Serbia (less than 10%), which may be prone to racist behaviour and (2) it is necessary to create programmes for prevention of racism, that would be implemented by schools, primarily based on education how to recognize and avoid racist outbursts, which would, in the first place, involve young male consumers of alcohol and members of fan groups.

REFERENCES

1. Arishita, K. M. (2010). *Racism in soccer: Eliminating soccer racism and using sport as a vehicle for national change.* Texas A&M University.
2. Cleland, J., & Cashmore, E. (2013). Football fans' views of racism in British football. *International Review for the Sociology of Sport*, 1-17. doi: 10.1177/1012690213506585
3. Cohen, J. (1988). *Statistical power analysis for the behavioral sciences (2nd edn.)*. Hillsdale, New Jersey: Lawrence Erlbaum Associates.
4. Janković, B. (2010). Prevention of Violence at Sports Events. *Herald of Law, 1*(3), 129–154.
5. Klymenko, P. (2013). *The Politics of Football: Radical Nationalism and Discrimination in the European Football. Case Study: Ukraine.* (Master master thesis), Vienna.
6. Llopis-Goig, R. (2009). Racism and xenophobia in Spanish football: Facts, reactions and policies. *Physical Culture and Sport Studies and Research, 47*, 35-43.

7. Milojević, S., & Janković, B. (2012). *Police measures and actions in confronting football hooliganism in some European countries.* Paper presented at the Archibald Reiss Days, Belgrade, 613–629.
8. Müller, F. (2009). *Communicating Anti, Racism.* (doctorate Dissertation), University of Amsterdam, Amsterdam.
9. Otašević, B. (2010). Urban Environment and Violence in Sport. *Bezbednost, 52*(3), 267–281.
10. Peucker, M. (2009). Racism, xenophobia and structural discrimination in sports: Country report Germany. Bamberg: European forum for migration studies (EFMS).
11. Quidt, J. d. (2012). Annual Report of the Stadnding committee, part II - questionnire on recent trends. Strasbourg: Council of Europe, Standing Committee (T-RV) – European Convention on Spectator Violence.
12. Scalia, V. (2009). Just a Few Rogues?: Football Ultras, Clubs and Politics in Contemporary Italy. *International Review for the Sociology of Sport, 44*(1), 41-53.
13. Statistical Office of the Republic of Serbia (2013). Upper Secondary Education in the Republic of Serbia, Beginning of 2012/2013 School year.
14. Sidanius, J., & Veniegas, R. C. (2000). Gender and race discrimination: The interactive nature of disadvantage. In S. Oskamp (Ed.), *Reducing Prejudice and Discrimination* (pp. 47-69). Mahwah, New Jersey: Lawrence Erlbaum Associates Publishers.
15. Watson, M. R. (2013). The Dark Heart of Eastern Europe: Applying the British Model to Football-Related Violence and Racism. *Emory International Law Review, 27*(2), 1055-1104.

UDC: 343.983:343.53
657.632

FINANCIAL INVESTIGATIONS OF CRIMINAL ACTIVITIES IN FINANCIAL REPORTS OF LEGAL PERSONS

Goran Bošković, PhD[1]
Academy of Criminalistic and Police Studies, Belgrade
Darko Marinković, PhD
Academy of Criminalistic and Police Studies, Belgrade

Abstract: The intensity of criminal activities dynamics which reflect within the scope of work of legal persons in the different economy fields is on the rise and represents a considerable challenge for criminal-law response of the state. Namely, the processes of proprietary transformation, bankruptcy and restructuring, but also of allocating grants and business operations of legal persons represent a specific opportunity for "generation" of criminal profit in economic relations. Also, the criminal structures make efforts to use legal economic flows in order to hide their own criminal activities, the origin and existence of illegally earned property abusing various forms of economic activities. These criminal activities leave "paper" trails, which can be followed by the analysis of financial reports in financial investigations. Namely, a logical response to this type of criminal activities is to use accounting and auditing skills and principles in financial investigations of legal persons' business operations, which reveal the relevant facts contained in the documentation that suggest the concrete way a criminal activity is being done. The knowledge of these facts would accelerate the investigation procedure, since their accurate interpretation would lead to crucial evidence important for the criminal procedure.

Keywords: financial investigation, criminal activities, financial reports

INTRODUCTION

Long-lasting problems in the reform of both system and structure as well as the passivity of government bodies in solving the problems related to legal persons in different economic field have left space for various abuses within the field of economic crime. On the other hand, business operations of legal persons as a cover for criminal structures enable mixing of illegal with legal funds, which then enables their infiltration into legal economic flows. Furthermore, the abuses within legal entities in the process of bankruptcy, restructuring or privatization in this area represent yet another challenge for state institutions. From this aspect the financial investigation and the analysis of financial reports represent *powerful* tools in the prevention and suppression of crimes in the field of business operations of legal persons.

From the economic point of view, the goal of criminal structures is to maximize profit and reduce risky situations, on the model of the way legal business corporations do, except that criminal organizations, in addition to being included in the political corruption, use enforce-

1 Email: goran.boskovic@kpa.edu.rs.

ment to ensure exclusive influence on a given market.[2] Modern illegal markets operate on the principle, if there is a need for illicit goods or services, criminal structures create mechanisms to meet those needs by market principles in order to obtain criminal profits.[3] The larger the financial potential of criminal structures, the larger is also their capability to infiltrate legal economic flows and establish intensive corruptive relations with the representatives of political and government power.[4] Criminal structures most often attempt to use legal economic flows in order to hide their own criminal activities, the origin and existence of illegally gained property abusing various forms of economic activities.

The individuals or business entities (doing either legal or illegal business) must keep books and records so that they could determine whether they earn or lose money, in other words to monitor the sources and availability of funds. The books and records are kept by many legal persons doing business in economy and financial sectors, as well as the individuals. Financial institutions use books and records, primarily financial reports, in order to determine if an individual or a company would be granted a loan. Investors make decisions based on books and records as to whether their investments would be lucrative enough, in other words, if funds should be invested in some business. State organs (tax administration) estimate and collect taxes based on the data from financial reports (tax declaration), which both the individuals and companies submit.

From the abstract point of view, in order to achieve a goal each organization, even a criminal one, requires financial assets – they are provided through certain operations (legal or illegal), then filed into records, invested and transferred, whereas as a result of such financial activities certain *paper* trails occur in the various forms of documentation. [5] Such trails can be discovered by the use of investigation techniques which essentially *stem from* financial administration and accounting. One of the key pieces of evidence in the majority of property crime investigations are the facts contained in business books and records. The majority of individuals and companies keep some sort of books and records, regardless of whether they are involved in legal or illegal activities. Therefore, they represent important material traces which enable the investigators to follow the *money* trail.

The subject of research in this paper is criminal activity in the financial statements of legal entities. The main objective of this research is to emphasize the characteristics of criminal activity in this area; a specific objective is to present the possibilities of using the analysis of financial statements during the financial investigations. Namely, using accounting and auditing skills and principles in financial investigations and criminal investigations of crimes in the field of business operations of legal persons enables the collection of *financial* information which are of operative and evidentiary significance and which are very important for prevention and provision of evidence of criminal activities and more efficient conduct of criminal procedures.

2 Schelling, T. (1971). *What is the Business of Organized Crime?*. Journal of Public Law, Emory University Law School, vol. 20, No. 1, Atlanta, 71-84.
3 Kulić M., Bošković G. (2010). *Nelegalno tržište: specifičnosti organizacije i funkcionisanje*, Ekonomika poljoprivrede, Institut za ekonomiku poljoprivrede, broj 4, Beograd, 655-670.
4 The research conducted in Belgium suggests that 75% of criminal organizations known to the police that are active in that country use legal business structures for their activities. In 49.1% cases these are legal economic subjects founded by criminal organizations which engage in both legal and illegal activities. Ponsaers, P. (2002). *What is so organized about financial–economic crime? The Belgian case*. Crime, Law& Social Change, 37, 191-201.
5 Bošković G., Marinković D. (2010). *Metodi finansijske istrage u suzbijanju organizovanog kriminala*, NBP – Žurnal za kriminalistiku i pravo, Kriminalističko-policijska akademija, broj 2, Beograd, 63-78

ANALYSIS OF ACCOUNTING DOCUMENTATION IN FINANCIAL INVESTIGATION

From the point of view of investigation of abuses in financial reports, the so called *creative accounting* is of special significance for their understanding, which illustrates another side of accounting. In other words, creative accounting means the use or abuse of accounting techniques and principles in order to show financial results which deliberately depart from fair and true statement.[6] Essentially, it implies the transformation of accounting figures from the real ones into the desirable ones by overstepping the regulatory accounting rules. Therefore, by the measures used within creative accounting the management can most often influence the following: the amount of stated profit, in other words the income statement; the amount of net presented property, in other words the balance sheet and the amount of presented net cash from operative activity.[7] On the other hand, *forensic accounting* implies the use of accounting and auditing skills and principles in potential or real civil and criminal matters, in order to detect frauds, losses of profit, income, property or damage, as well as internal control evaluations, but also other activities which require accounting expertise for the requirements of the legal system.[8] The task of forensic accounting is that through the application of the law allowed procedures and resources investigate, prove and initiate proceeding of sanctioning of manipulating in financial statements.[9]

When auditing books and records, the procedure of financial investigation is exactly opposite (reverse) to the accounting procedure. Namely, during the examination of documentation it is necessary to analyze, compare and establish authenticity of accounting documentation from financial reports to source documents (records). Criminal appropriation of property can be done in various manners, and some of them are as follows: payment of inexistent purchases, multiple settlements of accounts of the same supplier, partial deliveries, and bogus purchases and similar. These criminal activities are being hidden by *fictitious* documentation. In such cases it is unavoidable during the analysis to compare the accounting and actual state of property of legal persons.

Criminal activities in order to present higher profit than the gained one include premature income presentation, presentation of inexistent income (fictitious accounts, invoicing to inexistent buyers, and so on) or overvaluing the gains. These activities are most often carried out through not making an entry of expenses based on obligations, discounts not agreed upon, extinguishing reserves at the expense of the income, and so on. Also, criminal activities may include presenting lower profit than actually gained in order to postpone payment of tax on profits as follows: postponing the acknowledgment of income, excessive writing off of property, not presenting the income gains, excessive reserve amounts, undervaluing income, presenting higher expenses than the actual ones and similar. These facts should unavoidably be checked in the analysis of accounting documentation of legal persons.

Financial reports can be falsified in the following manners: fictitious income (making an entries of the inexistent income, selling to inexistent buyers, false selling accompanied by false documentation – invoice, dispatch note, receiving note and similar); creating inexistent claims;

6 O'Regan, P. (2006). *Financial Information Analysis*. 2nd ed., John Wiley & Sons, London.
7 Škarić-Jovanović, K. (2007). *Kreativno računovodstvo – motivi, instrumenti i posledice*, Zbornik radova: *Mjestoi uloga računovodstva, revizije i finansija u novom korporativnom okruženju*, XI Kongres Saveza računovona i revizora Republike Srpske, Teslić, 51-70.
8 Kranacher, M., Riley, R., Wells, J. (2010). *Forensic Accounting and Fraud Examination*. John Wiley & Sons, New Jersey.
9 Dimitrijević, D. (2012). *Metode i instrumenti forenzičkog računovodstva za otkrivanje prevara u finansijskim izveštajima*, Računovodstvo, Savez računovođa i revizora Srbije, vol. 56, broj 3-4, Beograd, 17-24.

hiding obligations and expenses (not booking obligations, decreasing expenditures, false capitalization of expenditures, and similar); false time periods (premature acknowledgment of income, excessive deliveries of goods, not confronting incomes and expenses, etc.); incorrect disclosing and other manners.[10] The analysis of the said facts should be an unavoidable part of financial investigations.

In the course of analysis of accounting documentation the attention should be paid of the cases of invoicing the goods which were not delivered or invoicing the goods which were delivered but would be returned to the seller at the beginning of the next accounting period. Namely, this is most often done with a view of premature acknowledgment of income, which influences the business result, usually at the end of the accounting period. Excessive deliveries of goods are performed just before making the final statement of accounts in order to show larger income and thus increase the result, in other words increase the buyers' demand. These are the cases of overvaluing, or undervaluing of the results in order to manipulate the result at the end of the year acknowledging the income in one year and expenses in another.

Criminal activities may be carried out in the domain of false presentation of obligations and expenses occurring in one accounting period, which creates a false insight into the business operations and misleads the users of financial reports. They are most often done through: not booking of debts (postponed account recording, hiding the accounts or their destruction), decreasing the expenses (manipulation of reserve costs by wrong calculation or deliberate omission), false capitalization of costs (including the costs which cannot be included into the purchase value which represents a basis to acknowledge property in the balance sheet) and similar.

The analysis of transactions includes determining on which accounts the changes are recorded related to transactions and the influence of transactions on each account (increase or decrease of balance on the account). After that the entries in the records are compared with the input documents in order to determine the existence of possible illogicalities. Then the authenticity of input documents is checked (determining the existence of falsified documentation).

The main goals of the analysis of books and records are to determine their accuracy and find trails of illegal activities contained in them.[11] This is why it is crucial to check the input documents. By checking the input documents we can find the data on: presented/recorded value of property/assets and income being too high in order to get a loan from the bank (this is bank fraud); presented/recorded value of property/assets in bankruptcy procedure being too low (false bankruptcy); presented value of income and expenses being too high (money laundering); the origin of property and assets which are the result of illegal business activities (money laundering); recorded value of income being too low and recorded value of expenses being too high (tax evasion); redirecting the assets (embezzlement); the accounts containing the data on personal items (cash, cars, machines, etc.) which the property (assets) are formed of, financial obligations (debts), ownership capital, income and expenses of business operations; quantity of goods which the company has in stock in order to sell or raw materials for processing into final products intended for selling; claims from debtors (individuals or legal persons) occurring as a result of financial loans, or services which included selling of goods with deferred payment; selling costs (purchasing costs or production of goods which the company manufactures in order to sell to its customers) and net income which refers to total revenue of a company decreased for selling costs and business operation costs.

The analysis of accounting documentation should focus on observing exceptions and peculiarities – the transactions which happened on days or in months in which according to

10 Wells, T. J. (2004). *Corporate Fraud Handbook*. John Wiley & Sons, New Jersey.
11 Crumbley, L., Heitger, L., Smith,S. (2007). *Forensic and Investigative Accounting*. CCH, Chicago.

the business practice of legal persons in the sector they should not be happening or in the amounts which are too high, too low or very different. The mentioned criminal activities most often lead to material false statements in financial reports due to presentation of unrealistic income, property, costs and obligations.

The analysis of accounting documentation includes also determining mutual relations of items in a balance sheet and examination of mutually comparable data (financial information on gained income in comparison with previous years, capital turnover, transactions and business operation income, comparison of financial information with the achieved business results, and similar). All discrepancies occurring when comparing the information during the analysis must be documented, as well as all mathematical checking (by recalculation of items in business books), which will enable to determine the real and *fictitiously* presented state of affairs in business books. Proving criminal activities is based on material evidence contained in the accounting documents and business books, which may be falsified, destroyed or double-entry books are kept in order to hide the crimes committed.

The focus of analysis should be directed also at the electronic data bases and software used in accounting of legal persons. Namely, when entering the data into a data base, the data may be altered or the current data may be deleted, removing the key input documents in order to falsify the amounts, falsely represent the company profit, stealing of spare parts, raw materials and stocks, payment to suppliers twice for the same invoice, creating fictitious purchase transactions, transferring money to bogus accounts, having employees on a payroll after the termination of employment and similar. Also, the programmer may create such a program which would enable to record and monitor regular business operations, which are presented in financial reports, and he can also create a *secret* part which would contain the sales of goods *in the black market* for internal monitoring. The programmer can then make a program which would enable to change the data by returning into the orders in progress and not using the cancellation order, which makes an insight into the previous state impossible, since it cannot be seen that there were any changes made. This is why it is important in financial investigations to have the assistance of IT specialists, because a significant part of evidentiary facts may be in electronic form.[12]

The detection of criminal activities by financial analysis of accounting documentation is particularly complex, since none segment of accounting procedure cannot be observed separately. Namely, at the end of auditing and detection of all abuses, it is necessary to reconstruct the financial report because in that way it can be determined what the exact amount of illegally gained property is.

ANALYSIS OF BALANCE SHEET ITEMS IN FINANCIAL INVESTIGATION

The analysis of balance sheet items includes a wide range of activities which, through individual checking of all classes and groups make it possible to identify illogicalities (*questionable facts*) in financial reports of legal persons. For more efficient analysis, in addition to financial reports and business books, it is necessary to obtain the entire documentation based on which the entries into the book were made. Within this context, the analysis of company register is very significant, since it includes the business operation book, gross balance sheet, final balance sheet, bills, tax reports on VAT, tax on profits and other tax reports, which would confirm the information from the bank register and compare the data, which offer a complete

12 Pearson, T., Singleton, T. (2008). *Fraud and Forensic Accounting in the Digital Environment*. Issues in Accounting Education, American Accounting Association, Vol. 23, No. 4, Sarasota, 545-559.

picture of company business operations.[13] The analysis of balance sheet items consists of individual analyses of – annual financial report; income, expenses and financial results; annual financial report; assets and liabilities; incomes and expenses; capital assets and intangible asset investment; claims and income; liabilities and expenses; stocks; monetary flows; capital; time periods and calculation of salaries and so on.

Systematic analysis of balance sheet items creates preconditions for the reconstruction of financial report, which will show the objective state of balance sheet items, but also the real state of affairs in the company which is the subject of financial investigation.[14] The direction of analytic processing of information from financial reports goes from the items presented, towards business books and ends with accompanying documentation. The purpose of the analysis of balance sheet items is to notice any illogic facts in business changes, which are most often connected with either inexistent or falsified documentation. Namely, business events may reflect on at least two balance sheet items, so that if there are not any illogic facts on one item the second one most often suggests them. The access to the computer in these cases is of great significance, since in that way it is possible to get to know the accounting program, the manner of entering and processing the data, specific program functions and other characteristics important to detect criminal activities.

The analysis of annual financial report implies the knowledge of methodology of its creation and checking of correlations among the items. The starting point of the analysis is to compare gross balance and final sheet with financial report, since the information contained in these documents should be identical, and each discrepancy should be checked. The financial report of another company in the same line of work may be taken for comparative purposes, which enables their comparison and more efficient analysis. All facts suggesting the sudden changes in business operations should be analyzed based on which some guidance should be obtained for further work without individual listing of the entire documentation and we could focus on a specific type of analysis of balance sheet items.

The analysis of assets and liabilities focuses on various forms of assets and sources of assets and their mutual relations which may be – real, fictitious, proportionate or disproportionate. The purpose of this analysis is to draw a conclusion on the scope, structure and dynamics of business operations which would point to real or fictitious state of assets and liabilities. Within this context, the most common abuses connected to the assets are overvaluing or undervaluing of company's property, which, for instance, may be done by unrealistic presentation of the rate of depreciation or unjustified decommissioning of assets.

The analysis of liabilities and expenses deals with comparing the statements in the balance sheet, income statement and statistic annex with the state in business books, which brings into connection the liabilities and expenses, and which enables to identify undervalued or overvalued expenses and liabilities which suggest the existence of criminal activities.

The analysis of income and expenses is directed at determining and evaluating the reality of business profit and final financial result, before taxation, the analysis of items in the income statement and the items in the balance sheet. Also, during this analysis it is possible to do crosswise comparison of specific transactions in order to detect mistakes, the transactions intentionally left out or other facts not shown in the balance sheets. In addition to the documentation related to income and expenses, it is necessary to obtain the specifications of income and expenses, based on which it is possible to determine the reality of presented costs in comparison with the income.

The analysis of capital assets and intangible asset investments includes checking of the origin of capital assets, amount of expenses for purchasing of capital assets, the manner of capital

13 Milojević, D. (2010). *Finansijska revizija i kontrola.* Beogradska poslovna škola, Beograd.
14 Andrić, M., Krsmanović, B., Jakšić, D. (2012). *Revizija – teorija i praksa.* Ekonomski fakultet, Subotica.

assets analysis, real amounts for capital assets which were presented in the balance sheet, capital assets accounts, corrections in the values of purchase and disposal of capital assets, if the capital assets are actually in the company, the list of capital assets and so on. For the purpose of as efficient analysis of intangible asset investments as possible, it is especially important to determine the reliability of the system of recording the investments and precise delimitation of costs between two accounting periods.

The analysis of claims and income focuses on comparison of balance sheet, income statement and statistical annex with the state of affairs in business books. Then, it is necessary to compare the state of selling and income from the previous and current years and the same facts should be compared with the business or statistic or other data independent from the business books of the company which is the subject of analysis. Special attention should be paid of the facts referring to the corrections of values of uncollectable claims, the payment of claims by the buyers, writing off of disputed and questionable claims, the return of goods, the payment discounts granted and similar.

The analysis of stocks most often consists of comparison of book value and physical inventory in the warehouse of finished products, warehouse, whole sale or retail. Then, there follows the comparison of inventory list and book value, the examination of accounting records and checking of corrections according to the results of the inventory. For the requirements of this sort of analysis, it is necessary to obtain the standards for the production of each product (costs, shrinkage, wastage and breakage), which enables more efficient analysis and the use of sampling method. False statements in the stock item lead to false statements of working assets, working capital, total assets, costs, gross profit and net profit.

The analysis of monetary flows is aimed at determining if the company has funds for financing, i.e. at estimating short-term position of money in the company and financing needs. Namely, the analysis of inflow and outflow of money can determine the facts which suggest there are criminal activities which most often reflect in the existence of fictitious invoices for which there are not payments (presentation of income without real existence of money) and presenting the monetary flows without trade in goods and services and recording of income, expenditures or liabilities, which point to money laundering.[15]

The analysis of capital, long-term loans and long-term reserves focuses on understanding of transactions, checking of amounts and calculations, since very often transactions with related business entities are present in abuses, which enable to hide certain activities which are shown as transactions with external subjects. Also, the value of shares can be *overinflated* (the attempt to sell them in the market above their real value) or the shares are undervalued (in cases when there is *corruptive feedback* between the company management and potential buyers). The analysis of long-term liabilities determines – if the approved loans have been recorded; if they are planned correctly and if the loan and installment payments entered into the books match the loan contract. The analysis of long-term reserves is directed at identification of cases of wrongful presentation of these costs and their influence on items in the income statement and the amount of financial result.

The analysis of time limits refers to determining legal, contractual or other bases for booking of time limits, in order to determine if the liabilities are undervalued, overvalued or left out (it is more often a case in practice that the items in the assets are overvalued). The real purpose of income and expenses delimitation is more objective presentation of business results, since the income and expenses are presented within the period they refer to, and not in some other period, which is most often the case when there are abuses of any kind.

15 Bošković, G. (2005). *Pranje novca*. Beosing, Beograd.

The analysis of calculation of salaries is aimed at determining primarily the real number of employees and the real amount of net salaries. The good basis for the analysis enables the obtaining of documentation with actual list of employees and the presented salaries and comparison with fictitious documents.

The logical step following the analysis of balance sheet items is the reconstruction of financial report, which will enable the objective presentation of real items in the financial report, and thus financial state of the legal person in the sector. It is important because financial reporting is subject to manipulation and illegal activities, which results in *blurred* or falsified reports.[16] The purpose of the reconstruction is the complete consideration of consequences of criminal activities in financial reports. Namely, each business change influences at least two items in the financial report, without the reconstruction of financial report we can consider only one side of consequence manifestation.

MODUS OPERANDI OF CRIMINAL ACTIVITIES IN FINANCIAL REPORTS OF LEGAL PERSONS

By using the methods of financial investigation in the analysis of financial reports and business operations of legal persons, it is possible to detect facts contained in the documentation relevant for criminal investigation, which suggest the concrete *modus operandi* of criminal activity.[17] Knowing these facts accelerates the procedure of criminal investigation, since their correct interpretation leads to significant evidence relevant for criminal procedure. The probability of existence of criminal activity is most often the function of three factors: motive (attraction), possibility (opportunity) and the lack of integrity.[18] The capability to manipulate the facts in financial investigations in order to hide criminal activity should also be added to them.

The identification of transactions during the analysis in financial reports of legal persons which are not entered into books timely, recorded in the period the event refers to, recorded in wrong amounts or are not recorded in the entire amount is the manner which indicates the covering of facts and criminal activities. If during the financial investigation the following facts are observed, such as: inexistence or unavailability of documentation; purchase of goods without appropriate documentation; entry based on photocopies or falsified documentation; falsifying of inventory lists; fictitious invoicing; uncertified and electronic documents without the existence of the originals; favouring certain creditors through various illegal activities; unsigned financial reports; transactions with related legal persons; increased prices in invoices; false requisitions, fictitious sales and deliveries; incorrect entry and not recording of business events; forgery of signatures on documents; discrepancies in business books; existence of internal documentation which is not entered into business books; discrepancies in the order of entries, frequent counter entries; illegal cash payments, or payments of fictitious bills; disabling or limiting access to certain records to interested parties (auditors) and existence of unusual business transactions in relation to the amount and time of occurrence, then determining the stated facts gets us the mosaic of criminal activities which results in concrete crimes within the scope of economic crimes.

16 Kaparavlović, N. (2011). *Uticaj kreativnog računovodstva na kvalitet finansijskog izveštavanja*. Ekonomski horizonti, vol. 13, br. 1, Kragujevac, 155-168.
17 Bierstaker, J., Brody, R., Pacini, C. (2006). *Accountants' perceptions regarding fraud detection and prevention methods*, Managerial Auditing Journal, Emerald Group Publishing Limited, Vol. 21 Iss: 5, Bingley, 520-535.
18 Pickett, K.H.S. (2007). *Osnovni priručnik za internu reviziju*. Savez računovođa i revizora Srbije, Beograd.

The next manner of criminal activities refers to double-entry book keeping, or records or their destruction. There is not any legal business reason for double-entry book keeping and records since all persons who have insight into the books and records should have access to all data. Destroying the books and records eliminates evidence. In each concrete case when such facts are determined it is without any doubt that they refer to illegal activities, which should be brought into connection with other facts related to business operations of a legal person who is the subject of financial investigation.

Then, if during the financial investigation it is determined that there are specific facts contained in the cash receipts journal, the sales journal and input documents which suggest that there exists: obtaining loans from companies with their headquarters in the countries known as off-shore financial centers; large and frequent monetary transactions in a company whose business operations are not cash-intensive; falsifying sales receipts and bank deposits whose source cannot be traced by following the money. Also the data contained in the cash payments journal, purchases journal and input documents which suggest that there exists: falsification of purchase receipts; large amount loans to the employees or individuals under very favourable conditions; payments to *inexistent* companies or individuals, payment of personal expenses by company assets and payment of credits to financial institutions that are seated in off-shore financial centers. The mentioned facts undoubtedly suggest the concrete models of illegal business operations and require detailed criminal investigation to clarify all circumstances surrounding the criminal activities.

If during the criminal investigation it is determined using financial investigation methods that there exist the following facts: hiding of property/assets; use of services of individuals who have power of attorney and frequent use of cashier cheques, in such cases the reasons for such activities should be sought most often in the participation in criminal activities and hiding of sources of wealth, then in hiding income from tax authorities or destruction of material traces - by reducing the possibility to follow monetary transactions by bank cheques.

In addition to the said facts, the abuses and criminal activities can be suggested by the following exceptions and particularities in the documentation such as: discrepancy between the balance and the main book; use of accounting program which enables double-entry book keeping and corrections without cancellation order; shortage in stock; unapproved changes in documentation; inexistent employees (fictitious workers); excess or shortage of cash; complaints and claims by the customers; corrections on the accounts of both buyers and suppliers; increase of amounts due for payments; increased rejects and scrap; double payment for the same transaction; activation of previously long inactive accounts and similar.[19]

The facts contained in books and records in criminal processing of economic crime cases in business operations of legal persons are the crucial source of evidentiary material. Their analysis can reveal many traces which enable to follow the money and detect illegal activities in business operations. This is why in each individual case it is important to check the business operations of the persons who are subject of criminal processing, since the application of financial investigation methods can lead to significant evidentiary information, which cannot be gathered by other criminal-investigation methods, and which are essential for criminal procedure.

19 Golden, T., Skalak, S., Clayton, M. (2006). *A Guide to Forensic Accounting Investigation*. John Wiley & Sons, New Jersey.

CONCLUSION

The process of social and economic transition in Serbia has been going on for a very long time. An unavoidable factor in this process is the appearance of criminal activities in companies. Particularly vulnerable are the various fields of economy in which there exist continuous problems in systematical and structural reform of this sector, which open space for various abuses in the domain of economic crime. When considering this type of criminal activities personal evidence is often missing, then there is a large number of people whose criminal activities have not been revealed or there are difficulties in proving them, or crimes are committed by the individuals of certain status and social reputation, which additionally makes it difficult to discover and prove these criminal activities. In order to get positive results in this area, it is necessary to use financial investigation methods in this field, which have not been sufficiently used so far leaving considerable space for criminal activities.

The use of accounting principles, auditing skills and investigative techniques in the analysis of accounting documentation during financial investigation is aimed at offering an insight into the real picture of financial business operations of a concrete legal person. Namely, it often happens that this picture is quite different from the real state of affairs, or to be more precise, it is almost never exactly the same as the state of affairs in the books, which suggests the wide range of abuses in economic relations. Accordingly, the analysis of balance sheet items in contemporary business environment represents an unavoidable basis for control of financial reports and successful revealing and proving of criminal activities during financial investigations.

Proper analysis of financial reports may suggest – concrete crimes; investment of illegally gained assets into legal business operations; use of off-shore financial center services; business operations with *inexistent* companies; companies and persons involved in criminal activities; business operations with related companies; questionable international financial transactions; hiding of income; location of illegally gained assets; time, place and scope of criminal profit transfer; tax evasion; abuse of authority; corruptive activities; money laundering; falsification of documentation; companies used as a cover for criminal activities and other information which may be of significance to prove the abuses in the operation of legal persons, but also for more efficient conducting of financial investigations and confiscation of illegally gained property.

Discovering criminal activities in financial reports means looking *beyond* the numbers, understanding an *essence* of the manner of abuse. It essentially requires a combination of accounting, auditing, investigative and analytical crime-investigative work, since financial reports are like a maze in which important material evidence is hidden which can be found only using other methods. The analysis of balance sheet items during financial investigations should enable simpler and faster detection of criminal activities. The efficient financial investigation should provide for quick orientation in discovering all weak spots in booking and following all trails which reveal abuses, which further enables the detection, understanding and proving of criminal activities in financial reports. Detection of criminal activities in financial reports requires a lot of knowledge, experience, analytical thinking, but also persistence.

REFERENCES

1. Andrić, M., Krsmanović, B., Jakšić, D. (2012). *Revizija – teorija i praksa.* Ekonomski fakultet, Subotica.
2. Bierstaker, J., Brody, R., Pacini, C. (2006). *Accountants' perceptions regarding fraud detection and prevention methods*, Managerial Auditing Journal, Emerald Group Publishing Limited, Vol. 21 Iss: 5, Bingley, 520-535.
3. Bošković G., Marinković D. (2010). *Metodi finansijske istrage u suzbijanju organizovanog kriminala*, NBP – Žurnal za kriminalistiku i pravo, Kriminalističko-policijska akademija, broj 2, Beograd, 63-78.
4. Bošković, G. (2005). *Pranje novca*. Beosing, Beograd.
5. Crumbley, L., Heitger, L., Smith,S. (2007). *Forensic and Investigative Accounting*. CCH, Chicago.
6. Golden, T., Skalak, S., Clayton, M. (2006). *A Guide to Forensic Accounting Investigation*. John Wiley & Sons, New Jersey.
7. Dimitrijević, D. (2012). *Metode i instrumenti forenzičkog računovodstva za otkrivanje prevara u finansijskim izveštajima*, Računovodstvo, Savez računovođa i revizora Srbije, vol. 56, broj 3-4, Beograd, 17-24.
8. Kaparavlović, N. (2011). *Uticaj kreativnog računovodstva na kvalitet finansijskog izveštavanja*. Ekonomski horizonti, vol. 13, br. 1, Kragujevac, 155-168.
9. Kranacher, M., Riley, R., Wells, J. (2010). *Forensic Accounting and Fraud Examination*. John Wiley & Sons, New Jersey.
10. Kulić M., Bošković G. (2010). *Nelegalno tržište: specifičnosti organizacije i funkcionisanje*, Ekonomika poljoprivrede, Institut za ekonomiku poljoprivrede, broj 4, Beograd, 655-670.
11. Milojević, D. (2010). *Finansijska revizija i kontrola*. Beogradska poslovna škola, Beograd.
12. O'Regan, P. (2006). *Financial Information Analysis.* 2nd ed., John Wiley & Sons, London.
13. Pearson, T., Singleton, T. (2008). *Fraud and Forensic Accounting in the Digital Environment*. Issues in Accounting Education, American Accounting Association, Vol. 23, No. 4, Sarasota, 545-559.
14. Pickett, K.H.S. (2007). *Osnovni priručnik za internu reviziju*. Savez računovođa i revizora Srbije, Beograd.
15. Ponsaers, P. (2002). *What is so organized about financial–economic crime? The Belgian case*. Crime, Law& Social Change, 37, 191-201.
16. Schelling, T. (1971). *What is the Business of Organized Crime?*. Journal of Public Law, Emory University Law School, vol. 20, No. 1, Atlanta, 71-84.
17. Škarić-Jovanović, K. (2007). *Kreativno računovodstvo – motivi, instrumenti i posledice*, Zbornik radova: *Mjestoi uloga računovodstva, revizije i finansija u novom korporativnom okruženju*, XI Kongres Saveza računovona i revizora Republike Srpske, Teslić, 51-70.
18. Wells, T. J. (2004). *Corporate Fraud Handbook*. John Wiley & Sons, New Jersey.

UDC: 657.632

THE ROLE OF THE ACCOUNTING PROFESSION IN THE PREVENTION AND DETECTION OF FINANCIAL STATEMENT FRAUD[1]

Marijana Ljubić, PhD[2]
John Naisbitt University, Graduate School of Business Studies, Belgrade
Vladan Pavlović, PhD
University of Pristina temporarily seated
in Kosovska Mitrovica, Faculty of Economics

Abstract: Frauds are part of business life and can be considered as an integral part of internal processes. Financial statements fraud are not the most common among other types of occupational fraud, but they have the greatest financial impact on the entity. After the financial scandals in the United States, the regulation has changed in this area, including the regulation of the auditing profession. However, the research shows that the number of committed frauds is even bigger than before the regulation has changed.

Key words: Financial statement fraud, legislative, internal auditing, external auditing

INTRODUCTION

The words of the Roman poet Martial "A good man has always something to learn in regard to fraud" are still true today, especially considering the fact that a 6% rise of fraud offenses from 2011 to 2012, and an additional 3% rise from 2012 to 2013, is reported by the FBI's National Incident-Based Reporting System[3] Fraud is ubiquitous; it does not discriminate in its occurrence.[4][5] A recent survey by Ernst & Young (2010) suggests that fraudulent activity has increased in the post financial crisis years while at the same time resources allocated to fight fraud have been cut.[6]

The research of fraud requires the definition of basic components of this phenomenon. As with many other definitions of phenomena that change through time, the fraud definition follows that rule as well. "The earliest recorded definition of fraud was made during the early fourteenth century, when it was defined as deceit, trickery, or intentional perversion for the purpose of inducing others to part with something of value. During the eighteenth century, England's Parliament added the concept of false pretenses to the definition of fraud in cover

1 This paper is part of the results of the research on Project 179001 supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia
2 E-mail: mljubic@nezbit.edu.rs.
3 Galletta, P. (2015): Basic Field Guide to Fraud, CPA Journal, 85(3), 54.
4 Galletta, P. (2015): Basic Field Guide to Fraud, CPA Journal, 85(3), 54-59.
5 The Association of Certified Fraud Examiners'2014 Report to the Nation on Occupational Fraud and Abuse, 2014, p. Website: http://www.acfe.com/rttn-download-2014.aspx
6 Purda, L., Skillicorn, D. (2015): Accounting Variables, Deception, and a Bag of Words: Assessing the Tools of Fraud Detection, Contemporary Accounting Research, 32(3), p. 1193.

an area of law previously untouched by larceny statutes. The modern American definition of fraud, as used in the Uniform Crime Reports and local law-enforcement agencies throughout the country, calls it deceitful conversion and the obtaining of money or property by false pretenses."[7] Financial Consumer Agency of Canada defines scam as: "A confidence game, swindle or other fraudulent scheme, especially for making a quick profit", a fraud as "An intentional deception made to secure unfair or unlawful gain or to damage another person".[8] Scams and frauds are schemes or deceptions designed to secure unfair or unlawful gain or to damage another person, These words can be used interchangeably.[9]

AICPA defined fraud as follows: An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception that results in a misstatement in financial statements that are the subject of an audit.[10]

There are various types of fraud classification. One of them classifies fraud using three basic categories: (1) fraud against the government (tax fraud, health care fraud, child-support fraud, bankruptcy fraud, social security fraud, and housing and welfare fraud), (2) corporate and financial fraud (securities, mail, wire, bank, mortgage, loan, check, credit card, and private health care fraud), and (3) consumer fraud (telemarketing fraud, Internet fraud, and identity theft).[11]

Occupational fraud is a universal problem for businesses around the world. Although frauds are by their nature difficult to identify and quantify, it is clear that fraud constitutes one of the most pervasive and costly crime problems in the United States.[12] One survey from the Association of Certified Fraud Examiners (ACFE) reported that 75% of employees had stolen at least once from their employer.[13] This is in line with the statement that 10% of people will always commit fraud, 10% of people will never commit fraud and 80% of people given the opportunity will commit fraud.[14] Based on the above mentioned survey results it seems that the occupational fraud was and still is one of the leading problems around the globe.

Collectively, fraud costs Americans hundreds of billions of dollars every year. By all accounts, the cost impact of white-collar crime is large. It has ballooned because of the relatively small chance of getting caught, the investigation and expense involved in bringing one case of fraud to justice, the basic trust most victims have in the transaction process, and the victims' belief that regulatory agencies are protecting them.[15] The real damage cannot be known because the nature of fraud means that much of its cost is hidden. Some frauds are never uncovered; many detected cases are never measured or reported and most frauds carry substantial indirect costs, including lost productivity, reputational damage and the related loss of business, as well as the costs associated with investigation and remediation of the issues that allowed them to occur.[16] In the corporate fraud context, the most common plaintiffs are shareholders.[17].

7 Murphy, M. (2015): Preventing and detecting fraud at not-for-profits, Journal of Accountancy, Vol. 220 (6), 77-83.
8 Financial Consumer Agency of Canada: http://www.fcac-acfc.gc.ca/.
9 Financial Consumer Agency of Canada: http://www.fcac-acfc.gc.ca/
10 AICPA, AU-C Section 240, 2015, p. 153
11 Murphy, M. (2015): Preventing and detecting fraud at not-for-profits, Journal of Accountancy, Vol. 220 (6), 77-83.
12 Murphy, L. L., Fraud, Salem Press Encyclopedia, January, 2015 (Item: 89405387). Website: www.salempress.com
13 Galletta, P. (2015): Basic Field Guide to Fraud, CPA Journal, 85(3), 54-59.
14 The Institute of Internal Auditors, Practice Guide – Internal Auditing and Fraud, December 2009): 2012, p. 14
15 Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc, p. 53.
16 The Association of Certified Fraud Examiners'2014 Report to the Nation on Occupational Fraud and Abuse 2014, p.8
17 Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc, p. 56.

According to the ACFE Report to the Nations on Occupational Fraud and Abuse in 2014, the most common type of fraud, namely occupational fraud, is committed in the United States, but the biggest median loss is noted in the Eastern Europe and Western/Central Asia ($383,000). It seems that the number of fraud cases is discovered in the US but the relative impact of these cases is larger in the Eastern Europe. For example, the median loss in the United States is about $100,000 which is about three times smaller than in the Easter Europe. A smaller number of scam in the Report does not necessarily means a lower level of criminal activities, but can also indicate a lower detection capability of occupational fraud.

As a reaction to a number of major corporate and accounting scandals, including those affecting Enron, Tyco International, Adelphia, Peregrine Systems, and WorldCom in the United States the regulation regarding fraud has changed but this implies the changes of the regulation around the globe. A number of significant legal, regulatory and standards-setting actions is combining to pressure all players in the financial-reporting process – from directors and senior management to internal and independent auditors – to step up their efforts to combat corporate fraud and misconduct.[18]

In the USA we are all witnesses of the large progress made in the area of Fraud Related Legislation. The most important changes come from passing the following acts such as the U.S Sarbanes-Oxley Act of 2002 and Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010. The Sarbanes Oxley Act of 2002 (SOX) created the PCAOB, which investigates possible violations of SOX. Also the professional accounting standards regarding the fraud are changed and SEC rules as well. Because the fraud affects the financial markets, the U.S. securities laws relating to the preparation and issuance of audit reports are changed.

Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 went into effect as responses to the financial crisis of 2007 –2010. These laws were created to increase the transparency and accountability within the financial industry. Like SOX, Dodd-Frank also protects whistleblowers in Title IX, "Investor Protections".[19] The SEC created three new initiatives in July 2013 within the Division of Enforcement (1) The Financial Reporting and Audit Task Force works to detect accounting and disclosure fraud; (2) The Center for Risk and Quantitative Analytics uses quantitative data to investigate and prevent transgressions harmful to investors; (3) The Microcap Fraud Task Force concentrates on abuses related to the Center for Risk and Quantitative Analytics issuance of securities by small companies.[20]

As a research area, fraud has often tended to fall between different research traditions including criminology, ethics (drawing on both psychology and philosophy), and business, including organizational corruption in organizational behavior and auditing or forensic accounting within accounting. Much research in the area has investigated a variety of biological and psychological pathologies, personality traits and the adverse effects of environmental and social conditions argued to be associated with criminality.[21]

CORPORATE AND FINANCIAL FRAUD

Financial fraud can have serious ramifications for the long-term sustainability of an organization, as well as adverse effects on its employees and investors, and on the economy as a whole.[22]

18 Price water house Coopers, The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risk, Internal Audit Services, 2004. www.pwc.com, p. 9
19 Galletta, P. (2015): Basic Field Guide to Fraud, CPA Journal, 85(3), , p.57
20 Galletta, P. (2015): Basic Field Guide to Fraud, CPA Journal, 85(3), , p.58
21 Murphy, L. L., Fraud, Salem Press Encyclopedia, January, 2015, p. 18. (Item: 89405387). Website: www.salempress.com
22 Abbasi, A., Albrecht, C., Vance, A., Hansen, J. (2012): Metafraud: A meta-learning framework for detecting financial fraud, MIS Quarterly, 36(4), , p. 1293

The types of fraud that affect organizations vary widely. When we consider the corporate and financial fraud we have in mind that these types of fraud can be viewed as occupational fraud, which is defined as: The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. Put more simply, occupational frauds are those schemes in which a person defrauds his or her employing organization. By its very nature, this form of fraud is a threat to all organizations that employ individuals to perform their business functions.[23] Occupational frauds can be classified into three primary categories: (1) asset misappropriations (a fraud scheme in which an employee steals or misuses the employing organization's resources); (2) corruption (a fraud scheme in which an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit); and (3) financial statement fraud (a scheme in which an employee intentionally causes a misstatement or omission of material information in the organization's financial reports). Nevertheless in the business practice, the committed fraud includes two or more of the three primary forms of occupational fraud.

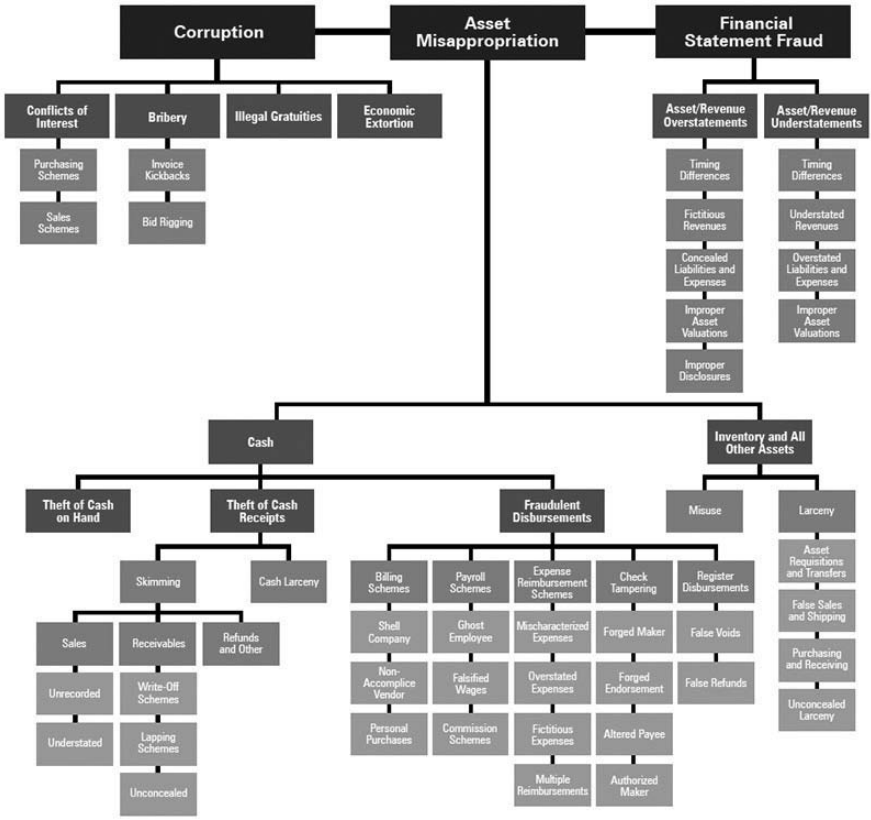


Figure 1: *Occupational Fraud and Abuse Classification System (Fraud Tree) Source: The Association of Certified Fraud Examiners'2014 Report to the Nation on Occupational Fraud and Abuse 2014, p.11*

23 The Association of Certified Fraud Examiners'2014 Report to the Nation on Occupational Fraud and Abuse 2014, p.7

Recent years, special attention is paid to securities frauds. Securities frauds come in many types and varieties. U.S. Securities and Exchange Commission states the following types of Securities frauds fraud: (1) Advance Fee Fraud; (2) Affinity Fraud; (3) High Yield Investment Programs; (4) Internet and Social Media Fraud; (5) Microcap Fraud; (6) Ponzi Scheme; (7) Pre-IPO Investment; (8) Scams; (9) Pyramid Schemes; (10) "Prime Bank" Investments; (11) Promissory Notes; and (12) Pump and Dump Schemes. (U.S. Securities and Exchange Commission; www.investor.gov)

Discussions of accounting fraud often revolve around civil law fraud, which requires a misrepresentation of a material fact, known by the perpetrator to be false, intended to be acted upon by the other party, justifiably relied upon by the other party, and resulting in a loss. We can emphasize the significance of the fact that the fraud cases exist under both civil and criminal law which differ based upon the level of intent, and at both the federal and state level.[24]Corporate fraud could be seen as a form of organized crime..[25]

FINANCIAL STATEMENT FRAUD

The asset misappropriations are the most common, but the financial statement fraud has the greatest financial impact. According to the Association of Certified Fraud Examiners that published the Report to the Nation on Occupational Fraud and Abuse in 2014. In that report financial statement fraud had median loss of $1 million.[26]

The US National Commission on Fraudulent Financial Reporting (1987) defines fraudulent financial reporting as an "intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statements".[27]. According to Mulford and Comiskey (2002) for financial reporting to be considered fraudulent, there must be a preconceived intent to deceive financial statement users in a material way. Technically, accounting practices are not considered to be fraudulent until the intent to deceive has been alleged in an administrative, civil, or criminal proceeding.

It turns out that the distinction between the financial reporting fraud and earnings management cannot easily be made[28]. This is because in some cases, they share the same objective, both of which are deliberate actions taken by the management to achieve private gains, and both having the potential to cause material loss or damage for the shareholders by relying on false information. Although literature regarding earnings management and financial reporting fraud do not provide one general accepted framework facilitating the distinction between them to be made, they all implicitly or explicitly indicate that compliance with standards and management intent are the most important factors. AAER bulletins issued by the SEC, taking their distinctions between fraud and truth to identify financial reports.[29]

24 Galletta, P. (2015): Basic Field Guide to Fraud, CPA Journal, 85(3),p. 54.
25 Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc, p.50.
26 The Association of Certified Fraud Examiners'2014 Report to the Nation on Occupational Fraud and Abuse 2014, p.7
27 Marai, A., Pavlović, V. (2014): An overview of earnings management measurement approaches: Development and evaluation, Facta universitatis - series: Economics and Organization, vol. 11(1), 21-36
28 Marai, A., Pavlović, V. (2014): An overview of earnings management measurement approaches: Development and evaluation, Facta universitatis - series: Economics and Organization, vol. 11(1), 21-36
29 Marai, A., Pavlović, V. (2014): An overview of earnings management measurement approaches: Development and evaluation, Facta universitatis - series: Economics and Organization, vol. 11(1), 21-36

FRAUD DETECTION

Fraud detection methods can be passive or active. Active measures include controls that require the assertive involvement of management and by their nature are designed to detect or assist in detecting fraud within an organization[30].

The active detection methods include:

- hotlines,
- management review procedures,
- employee monitoring mechanisms,
- data mining,
- targeted audits through hot spot analysis,
- internal audits,
- quality assurance, and
- the analysis of management accounting reports.

Passive measures include controls or activities that do not require the active and ongoing involvement of management, but exist as a means by which fraud is detectable within an organization.

The passive detection methods include:

- confession,
- notification by law enforcement,
- external audit, and
- by accident.

Passive detection methods tend to take longer to bring fraud to management's attention, which allows the related loss to grow. Consequently, proactive detection measures - such as hotlines, management review procedures, internal audits and employee monitoring mechanisms - are vital in catching frauds early and limiting their losses.[31].

For many years, organizations have been using hotlines to detect theft and fraud with great[3233]. Organizations should implement hotlines to receive tips from both internal and external sources[34]. It is considered that tips are the most common detection method. The most important source of tips are: employee, customer, anonymous, vendor, shareholder/owner, competitor and perpetrator's acquaintance. The presence of a telephone information line has a considerable impact on the initial fraud detection method. Some organizations provide an internally managed hotline as an option for employees who are uncomfortable discussing issues face-to-face. Only a fraction of employees who discover fraud report this information[35]. Employees, suppliers, consumers and other stakeholders are more likely to use a hotline to report an issue that makes them uncomfortable. An external hotline provides greater safeguards of anonymity and avoids even the appearance of impropriety.[36]

30 The Australian National Audit Office & KPMG, Fraud Control in Australian Government Entities, Better Practice Guide, March 2011, p. 53

31 The Association of Certified Fraud Examiners'2014 Report to the Nation on Occupational Fraud and Abuse 2014, p.5

32 Muminović, S., Ljubić, M. (2013): Prevencija pranja novca u Srbiji – iskustva i izazovi, *Revizor*, 16(61), Institut za ekonomiku i finansije, Beograd, str. 9-23.

33 Malone, T., Childs, R., Best Practices in Ethics Hotlines, The Network, 2008., p.23.

34 Pickett, S., Fraud Smart, John Wiley & Sons Ltd., 2012.

35 Kaplan, S, Pope, K., Samuels, J. (2015): An Examination of the Effects of Managerial Procedural Safeguards, Managerial Likeability, and Type of Fraudulent Act on Intentions to Report Fraud to a Manager, Behavioral Research in Accounting, 27(2),p. 77.

36 Malone, T., Childs, R., Best Practices in Ethics Hotlines, The Network, 2008., p.7.

There are a number of 'red flags' or early warning signs of fraud activity which can be used to help profile possible internal perpetrators. These early warning signs could be summarized as those shown in Table 1. that follows

Table 1: *Early warning signs for staff and/or workplaces at risk of fraud**

Early warning signs: people	Early warning signs: areas or activities
Unwillingness to share duties; refusal to take leave.	Financial information reported is inconsistent with key performance indicators.
Refusal to implement internal controls.	Abnormally high and increasing costs in a specific cost centre function.
The replacement of existing suppliers upon appointment to a position or unusually close association with a vendor or customer.	Dubious record keeping.
A lifestyle above apparent financial means; the provision of gifts to other staff members.	High overheads.
Failure to keep records and provide receipts.	Bank reconciliations not up to date.
Chronic shortage of cash or seeking salary advances.	Inadequate segregation of duties.
Past legal problems (including minor previous thefts).	Reconciliations not performed on a regular basis.
Addiction problems (substance or gambling).	Small cash discrepancies over a period of time.

* The Australian National Audit Office & KPMG, Fraud Control in Australian Government Entities, Better Practice Guide, March 2011, p. 56 – 57. Adapted from The Audit Office of NSW – *Fraud Control Volume 2 Strategy* and Association of Certified Fraud Examiners, *Report to the Nations on Occupational Fraud and Abuse, 2010 Global Fraud Survey.*

AICPA in the Appendix C-Examples of Circumstances That Indicate the Possibility of Fraud (Ref: par.11, A11, and A56) states the following are examples of circumstances that may indicate the possibility that the financial statements: (1) Discrepancies in the accounting records, (2) Conflicting or missing evidence that include missing documents; documents that appear to have been altered; unusual balance sheet changes, or changes in trends or important financial statement ratios or relationships; for example, receivables growing faster, large numbers of credit entries and other adjustments made to accounts receivable records; unexplained or inadequately explained differences between the accounts receivable subledger and the control account, (3) Conditions relating to governmental entities or not-for-profit organizations such as significant transfers or transaction, abnormal budget conditions, procurement conditions, program conditions, grant and donor funding conditions, such as - noncompliance with grant requirements - unclear grant requirements - grants not reaching the intended recipient - complaints from intended recipients or interest groups, and lack of monitoring of grantee compliance with applicable law or regulation; (4) problematic or unusual relationships between the auditor and management, including the following: denial of access to records, facilities, certain employees, customers, vendors, or others from whom au-

dit evidence might be sought; (5) other circumstances, including the following: unwillingness by management to permit the auditor to meet privately with those charged with governance; accounting policies that appear to be at variance with industry norms etc.

THE ROLE OF INTERNAL AND THE EXTERNAL AUDITING IN THE PREVENTION AND DETECTION OF FRAUD

The collapse of Enron Corp. in the fall of 2001 had a peculiar side effect: accounting became front page news. For the next year, accounting fraud at a long series of Fortune 500 companies made head lines.[37]

The primary responsibility for the prevention and detection of fraud is in the hands of managers. Sarbanes-Oxley and corresponding regulatory changes have raised the stakes for senior management and the board of directors, who must now view fraud and misconduct as a broad-based threat and address fraud issues in far greater detail.[38]

The internal audit committee, the internal auditor, and the external (or independent) auditor are three separate actors contribute to the audit.[39]

The roles and responsibilities of this subject have been changed through time as well as the way we see fraud today. Traditional views have resulted in a fragmented (not integrated / holistic) risk framework and reactive approach to fraud. In the traditional way, fraud risk were considered as follow[40]

- Fraud risk and controls considered as separate, secondary objectives of internal audit and internal control;
- Fraud not perceived to be an internal control failure;
- Fraud training and awareness not really necessary;
- Information and Communication disparaged;
- Fraud risk monitoring not perceived as a positive cost-benefit allocation of resources.

Current view aims to manage fraud risk holistically and proactively. The actual point of view is:[41]

- Fraud risk and controls considered an objective of internal control activities
- Fraud perceived to be potential internal control failures
- Fraud training and awareness necessary
- Information and Communication aggregated, concise, and timely
- Fraud risk monitoring perceived as positive cost/benefit (protects revenue and/or recoups losses)

In the past, many internal audit groups have focused their resources and efforts primarily on the detection of frauds involving the misappropriation of assets[42]. Today, roles and responsibilities of internal auditor for fraud prevention and detection are[43]:

37 Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc
38 Price water house Coopers, The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risk, Internal Audit Services, 2004. www.pwc.com, p.43
39 Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc.p.21
40 Institute of Internal Auditors, Fraud and Internal Audit: Current Views, Examples, and Resources, BBVA Compass September 2012, p.6.
41 Institute of Internal Auditors, Fraud and Internal Audit: Current Views, Examples, and Resources, BBVA Compass September 2012, p.11.
42 Price water house Coopers, The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risk, Internal Audit Services, 2004. www.pwc.com, p.9.
43 The Institute of Internal Auditors, Practice Guide – Internal Auditing and Fraud, IIA, December 2009

- Evaluates risks based on audit plans with appropriate testing,

- Be alert to the signs and possibilities of fraud within an organization and detects the symptoms that accompany fraud,

- Assists in the deterrence of fraud by examining and evaluating the adequacy and the effectiveness of internal controls,

- Assists management in establishing effective fraud prevention measures,

- Initially or fully investigates the suspected fraud, root cause analysis and control improvement recommendations,

- Monitors of a reporting/whistleblower hotline,

- Conducts proactive auditing to search for misappropriation of assets and information misrepresentation (Source: Practice Guide – Internal Auditing and Fraud, IIA I)

Internal audit can assist an entity to manage fraud control by advising on the risk of fraud and the design or adequacy on internal controls. It can also assist in detecting fraud by considering fraud risks as part of its audit planning and being alert to indicators that fraud may have occurred.[44]

Internal Audit Standards which are relevant for fraud prevention and detecting are:

- II A Standard 1200: Proficiency and Due Professional Care 1210.A2 – Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud";

- II A Standard 1220: Due Professional Care

- 1220.A1 – Internal auditors must exercise due professional care by considering the:… Probability of significant errors, fraud, or noncompliance;

- II A Standard 2060: Reporting to Senior Management and the Board "The chief audit executive (CAE) must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board."

- II A Standard 2120: Risk Management. 2120.A2 –"The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk."

- II A Standard 2210:Engagement Objectives. 2210. A2 – "Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives."[45]

The expectations of internal audit are shifting in response to the new environment is in prevention and detection of fraudulent financial reporting (Price water house Coopers, 2004)[46].

Of all the players in the financial-reporting supply chain, internal audit is quite possibly the group most affected by the new emphasis on fraud prevention and detection. Internal audit is uniquely juxtaposed between the audit committee and senior management, having either a direct or dotted-line relationship to both groups (Price water house Coopers, 2004)[47].

44 The Australian National Audit Office & KPMG, Fraud Control in Australian Government Entities, Better Practice Guide, March 2011

45 Institute of Internal Auditors, Fraud and Internal Audit: Current Views, Examples, and Resources, BBVA Compass September 2012, p.30.

46 Price water house Coopers, The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risk, Internal Audit Services, 2004. www.pwc.com, p.9..

47 Price water house Coopers, The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risk, Internal Audit Services, 2004. www.pwc.com, p.9..

Sarbanes-Oxley, the SEC, and the stock exchanges have brought about major changes in the regulation of auditors. The legal approval of outsourcing the Internal Audit to an External Auditor is one of those changes. The outsourcing dilemma is not new, i.e. what is the best solution for Internal Auditing? Proponents of outsourcing cite "improved services at lower costs" as the primary reason to permit outsourcing of the internal audit.[48] However, some studies do not confirm the idea that this cost saving is significant. For example, Johnson and Ponthieu finds that the direct cost savings associated with outsourcing are generally small (1999, p.5). Some leaders in the field, however, support a ban on outsourcing internal audit work to an external auditor stating that in-house auditors are more likely than external auditors to uncover fraud within the corporation.[49] The KPMG survey from 1998 shows that internal auditors are among the entities most likely to detect fraud within their organizations, while external auditors were among the least likely.[50] Rittenberg, Moore and Covaleski, M. (1999)[51] cited that "most of the outsourced internal audit departments we encountered appeared to have lost their focus on adding value and improving company governance. It is widely understood in the academic and professional auditing literature that it is not the auditor's duty to guarantee that the financial statements are accurately represented[52].

The auditor's responsibilities relating to fraud in an audit of financial statements are defined by the relevant auditing standards. The auditing standards do not, and have never, indicated that detecting all material financial statement fraud is possible[53].

"An auditor conducting an audit in accordance with GAAS is responsible for obtaining reasonable assurance that the financial statements as a whole are free from material misstatement, whether caused by fraud or error. Due to the inherent limitations of an audit, an unavoidable risk exists that some material misstatements of the financial statements may not be detected, even though the audit is properly planned and performed in accordance with GAAS" (AICPA, AU-C Section 240, 2015, p. 152). As it is stated in the SAS, "the potential effects of inherent limitations are particularly significant in the case of misstatement resulting from fraud…because fraud may involve sophisticated and carefully organized schemes designed to conceal it, such as forgery, deliberate failure to record transactions, or intentional misrepresentations being made to the auditor". When obtaining reasonable assurance, the auditor is responsible for maintaining professional skepticism throughout the audit, considering the potential for management override of controls, and recognizing the fact that audit procedures that are effective for detecting error may not be effective in detecting fraud.[54]

An auditor conducting an audit in accordance with ISAs (UK and Ireland) is responsible for obtaining reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error[55].

The objectives of the auditor are to:

a) identify and assess the risks of material misstatement of the financial statements due to fraud;

b) obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement due to fraud, through designing and implementing appropriate responses; and

48 Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc.p.21.
49 Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc.p.22.
50 Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc.p.p.22,23.
51 Rittenberg, L., Moore, W., Covaleski, M. (1999): The Outsourcing Phenomenon, Internal Auditor, 56(2), p.44.
52 Albrecht, S., Hoopes, J. (2014): Why Audits Cannot Detect All Fraud, CPA Journal, 84(10),p.14.
53 Albrecht, S., Hoopes, J. (2014): Why Audits Cannot Detect All Fraud, CPA Journal, 84(10),p.21.
54 AICPA, AU-C Section 240, 2015, p. 152
55 IFAC Handbook, International standard on auditing 240, p. 1

c) respond appropriately to fraud or suspected fraud identified during the audit.[56]

Fraudulent financial reporting may be accomplished by the following:

a) Manipulation, falsification (including forgery), or alteration of accounting records or supporting documentation from which the financial statements are prepared;

b) Misrepresentation in, or intentional omission from, the financial statements of events, transactions, or other significant information;

c) Intentional misapplication of accounting principles relating to amounts, classification, manner of presentation, or disclosure.[57]

Fraud can be committed by management overriding controls using such techniques as the following:

a) Recording fictitious journal entries, particularly close to the end of an accounting period, to manipulate operating results or achieve other objectives;

b) Inappropriately adjusting assumptions and changing judgments used to estimate account balances;

c) Omitting, advancing, or delaying recognition in the financial statements of events and transactions that have occurred during the reporting period;

d) Concealing, or not disclosing, facts that could affect the amounts recorded in the financial statements;

e) Engaging in complex transactions that are structured to misrepresent the financial position or financial performance of the entity;

f) Altering records and terms related to significant and unusual transactions.[58]

"The auditor's ability to detect a fraud depends on factors such as the skillfulness of the perpetrator, the frequency and extent of manipulation, the degree of collusion involved, the relative size of individual amounts manipulated, and the seniority of those individuals involved."[59] The external auditors do not discover frauds, in the most of cases. According to the ACFE Report to the Nations on Occupational Fraud and Abuse in 2014 external audits are among the least effective controls in combating occupational fraud. "Such audits were the primary detection method in just 3% of the fraud cases reported to us, compared to the 7% of cases that were detected by accident. Further, although the use of independent financial statement audits was associated with reduced median losses and durations of fraud schemes, these reductions were among the smallest of all of the anti-fraud controls analyzed in our study. Consequently, while independent audits serve a vital role in organizational governance, our data indicates that they should not be relied upon as organizations' primary anti-fraud mechanism".[60] The other researches show that material financial fraud only occurs at the rate of about three financial frauds per 1,000 annual public company audits. Some of them indicates that 40% of audit partners never encounter a single material irregularity (defalcations or management fraud) during their entire careers, and those who do only see the problem on 1.3% of their audit engagements.[61] Based on the above mentioned research results we can cite Kee's attitude towards the idea that auditors' techniques' lack of discovering fraud. Kee (2014, p. 28) argues that despite the fact that the current auditing standards require auditors

56 AICPA, AU-C Section 240, 2015, p. 152-153; IFAC Handbook, International standard on auditing 240, p. 4
57 AICPA, AU-C Section 240, 2015, p. 162
58 AICPA, AU-C Section 240, 2015, p. 162
59 AICPA, AU-C Section 240, 2015, p. 155
60 The Association of Certified Fraud Examiners'2014 Report to the Nation on Occupational Fraud and Abuse 2014, p.5.
61 Loebbecke, Eining, Willingham, 1989, pp. 1–28, Kee, 2014, p. 28.

to assess the risk of material misstatement due to fraud, the auditors' lack of direct experience with financial fraud makes it difficult for them to both identify relevant fraud risk factors and weigh them[62].

The need to strengthen auditor independence rules was one of the key conclusions drawn by congressional investigators into the post-Enron scandals.[63] Sarbanes-Oxley created the Public Company Accounting Oversight Board (PCAOB) to regulate public auditing[64]. A 2013 PCAOB report on inspections of 455 audit firms with public clients indicated that a common deficient noted in the inspections was audit procedures related to fraud risk[65].

Consideration of fraud inevitably raises the question of auditor's responsibilities for detecting it. An expectation gap exists between what regulators, the public, and investors believe that a financial statement audit is intended to do and what the auditing standards state that financial statement audits are required to do[66]. This gap is not new.

The auditor is primarily concerned with fraud that causes a material misstatement in the financial statements. Two types of intentional misstatements are relevant to the auditor-misstatements resulting from fraudulent financial reporting and misstatements resulting from misappropriation of assets. Although the auditor may suspect or, in rare cases, identify the occurrence of fraud, the auditor does not make legal determinations of whether fraud has actually occurred[67].

Auditors are expected by the public to find financial statement fraud, even though U.S. GAAS has long held that they might not be able to detect all frauds.[68]

Certain factors can make fraud nearly impossible to discover, even when a competent GAAS audit is performed, and certain factors are often present when auditors should have detected fraud[69].

Epstein and Geiger found that more than 70% of the investing public expected absolute assurance from auditors against material fraud in financial statements[70]

CONCLUSION

Responsibility for managing the risk of fraud, like responsibility for managing all risks, rests with management as part of its ongoing responsibilities. In this paper we thoroughly investigate the types of fraud committed with the specific emphasis on corporate and financial statement fraud and their prevention. Corporate fraud and financial statement fraud are integral part of the occupational fraud. Occupational fraud comprise financial statement fraud, asset misappropriation fraud and corruption. Asset misappropriation is the most common but financial statement fraud has the most significant impact on company and its performance. Specific emphasis was made to the fraud detection techniques and these techniques are classified into active and passive detection methods. Among active methods the most im-

62 Ljubić, M., Šiljanoska. S., (2015), Interna revizija u funkciji ublažavanja negativnih efekata bankarskih rizika, Međunarodnoa naučna konferencija o društvenom i ekonomskom istraživanju i razvoju – SERDA 2015, „Društveni i tehnološki razvoj u eri globalizacije, Zbornik radova 77-89.
63 Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc.p.24.
64 Price water house Coopers, The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risk, Internal Audit Services, 2004. www.pwc.com. p.5.
65 Kee, 2014, p. 28
66 Albrecht, S., Hoopes, J. (2014): Why Audits Cannot Detect All Fraud, CPA Journal, 84(10),p.14.
67 AICPA, AU-C Section 240, 2015, p. 151
68 Albrecht, S., Hoopes, J. (2014): Why Audits Cannot Detect All Fraud, CPA Journal, 84(10),p.13.
69 Albrecht, S., Hoopes, J. (2014): Why Audits Cannot Detect All Fraud, CPA Journal, 84(10),p.13..
70 Albrecht, S., Hoopes, J. (2014): Why Audits Cannot Detect All Fraud, CPA Journal, 84(10),p.14.

portant seems to be hotlines. Passive include accident as the most important. The fraud is discovered if managers do not overcome the early warning signs of fraud activity such as unwilling to take a leave, refusal to implement the internal control, the replacement of the existing suppliers etc. Circumstances that may indicate the possibility of fraud are part of the AICPA regulation which is one of the most important for the accountants. Among other changes that have the status of the law we present the requirements imposed by the Sarbanes Oxley Act. The primary importance for discovering the fraud lie on the internal and external auditors. The role of the internal auditor seem to exceed the role of other professions in this area. The contemporary view on this topic extend the role of the internal auditor to the area in which this auditor has a responsibility to evaluate the risks based on auditing plans and to assist in the deterrence of fraud by examining the effectiveness of internal control. The role of the external auditor has changed over time but the fraud committed are usually not discovered by the external auditor. This is due to the lack of experience, difficulties to identify risks and fraud risk factors for the specific client and because the auditor is not independent enough. There is a large expectation gap between the auditor responsibility, public and investors.

REFERENCES

1. Abbasi, A., Albrecht, C., Vance, A., Hansen, J. (2012): Metafraud: A meta-learning framework for detecting financial fraud, MIS Quarterly, 36(4), 1293-1397
2. Albrecht, S., Hoopes, J. (2014): Why Audits Cannot Detect All Fraud, CPA Journal, 84(10),12-21
3. Blewitt, A, "Strengthen the Sign-off," Financial Times, Jan. 22, 2004
4. Free, C., Murphy, P. (2015): The Ties that Bind: The Decision to Co-Offend in Fraud, Contemporary Accounting Research, Vol. 32(1), p18-54
5. Galletta, P. (2015): Basic Field Guide to Fraud, CPA Journal, 85(3), 54-59.
6. Institute of Internal Auditors, Fraud and Internal Audit: Current Views, Examples, and Resources, BBVA Compass September 2012
7. Jickling, M. (2009). Barriers to Corporate Fraud. New York: Nova Science Publishers, Inc
8. Johnson, J. L., Ponthieu, L. D. The Long-Term Impact and Cost-Effectiveness of Outsourcing. Project Summary Report 1829-S, Transportation Research Center, University of North Texas, December 1999.
9. Kaplan, S, Pope, K., Samuels, J. (2015): An Examination of the Effects of Managerial Procedural Safeguards, Managerial Likeability, and Type of Fraudulent Act on Intentions to Report Fraud to a Manager, Behavioral Research in Accounting, 27(2), 77-94
10. Kassem, R. Higson, A. (2015): Combating fraud: Is Egypt ready? Insights from the literature, Journal of Emerging Trends in Economics and Management Sciences, 6(5), 290-298
11. Knežević, G., Mizdraković, V., Arežina, N. (2012): Menadžment kompanije kao uzrok i instrument suzbijanja primene kreativnog računovodstva. Management: Journal for Theory and Practice Management, 17(62), 89-95.
12. Ljubić, M., Šiljanoska. S., (2015), Interna revizija u funkciji ublažavanja negativnih efekata bankarskih rizika, Međunarodnoa naučna konferencija o društvenom i ekonomskom istraživanju i razvoju – SERDA 2015 , „Društveni i tehnološki razvoj u eri globalizacije", 09. Maj Bijeljina, IZDAVAČ: Slobomir P Univerzitet, Slobomir, Zbornik radova 77-89.
13. Muminović, S., Ljubić, M. (2013): Prevencija pranja novca u Srbiji – iskustva i izazovi, Revizor, 16(61), Institut za ekonomiku i finansije, Beograd, str. 9-23.

14. Malone, T., Childs, R., Best Practices in Ethics Hotlines, The Network, 2008
15. Marai, A., Pavlović, V. (2013): Earnings Management vs Financial Reporting Fraud – Key Features for Distinguishing, Facta universitatis - series: Economics and Organization, vol. 10(1), p. 39-47
16. Marai, A., Pavlović, V. (2014): An overview of earnings management measurement approaches: Development and evaluation, Facta universitatis - series: Economics and Organization, vol. 11(1), 21-36
17. McKee, T. (2015): Evaluating Financial Fraud Risk During Audit Planning, CPA Journal. Oct2014, Vol. 84 Issue 10, p28-31
18. Murphy, L. L., Fraud, Salem Press Encyclopedia, January, 2015 (Item: 89405387). Website: www.salempress.com
19. Murphy, M. (2015): Preventing and detecting fraud at not-for-profits, Journal of Accountancy, Vol. 220 (6), 77-83.
20. Pickett, S., Fraud Smart, John Wiley & Sons Ltd., 2012.
21. Pricewaterhouse Coopers, The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risk, Internal Audit Services, 2004. www.pwc.com
22. Purda, L., Skillicorn, D. (2015): Accounting Variables, Deception, and a Bag of Words: Assessing the Tools of Fraud Detection, Contemporary Accounting Research, 32(3), p1193-1223
23. Rittenberg, L., Moore, W., Covaleski, M. (1999): The Outsourcing Phenomenon, Internal Auditor, 56(2), 42-46
24. The Institute of Internal Auditors, Practice Guide – Internal Auditing and Fraud, December 2009):
25. Trompeter, G., Carpenter, T., Jones, K., Riley J, Richard A. (2014): Insights for Research and Practice: What We Learn about Fraud from Other Disciplines, Accounting Horizons, 28(4), 769-804

INTERNET SOURCES

26. Association of Certified Fraud Examiners. Website: http://www.acfe.com/rttn-download-2014.aspx
27. COSO guidance on governance and http://www.coso.org/guidance.htm operational performance, internal controls, enterprise risk management, and fraud deterrence

UDC: 343.85:343.359.2(4-672EU)

THE FIGHT AGAINST TAX EVASION IN THE EUROPEAN UNION[1]

Cvjetana Cvjetković, PhD[2]
University of Novi Sad, Faculty of Law
Goran Milošević, PhD
University of Novi Sad, Faculty of Law
Luka Baturan
University of Novi Sad, Faculty of Law

Abstract: In this paper the authors consider measures against tax evasion in the European Union. Due to the fact that tax evasion results in a serious loss of revenues and undermines the principle of fairness, it is not surprising that the institutions of the European Union intensify activities in order to fight tax evasion. In addition, the member states on own initiative undertake various unilateral measures. Tax evasion occurs within the European Union and globally. On the one hand, the functioning of a common market created numerous possibilities for tax evasion, on the other the existence of non-cooperative tax jurisdictions, i.e. tax havens makes the phenomenon of tax evasion actual in relation to third countries.

Key words: tax evasion; European Union; tax havens.

INTRODUCTION

In recent years, we have witnessed the increasing number of financial transactions whose primary goal is a total or partial non-payment of taxes, i.e. tax evasion. The internationalization of financial markets, removal of borders between countries, advances in science and technology, etc. pose a challenge for each form of legal activity. Illegal business segments are working as a shadow of legal ones, and they are very flexible and adjustable to all social and economic conditions.

Members of the European Union are no exception in this regard, especially because this phenomenon is pronounced in relation to both member states and non-member states. On the one hand, the establishment of the common market within the European Union has created ideal conditions for tax evasion, and on the other hand, the existence of low tax jurisdictions makes the phenomenon of tax evasion present in relation to the third countries as well. However, one should not disregard the fact that low tax jurisdictions exist within the European Union, despite general position of the Union's institutions on adverse effects of unfair tax competition.

The main goal of this paper is to analyze the most important measures against tax evasion in the European Union**.** This is also a relevant topic for tax policy-makers in Serbia, not just because of the fact that Serbia is a candidate country for membership in the Union, but because of widespread tax evasion. Therefore, taking appropriate measures against this phenomenon, in conditions of the decline of economic activities and budget deficit, is presented as necessity.

1 This paper is the result of the project 'Legal Tradition and New Legal Challenges' which is financed by the Novi Sad Faculty of Law.
2 E-mail: c.cvjetkovic@pf.uns.ac.rs.

NOTION AND TYPES OF TAX EVASION

The word 'evasion' comes from the Latin word 'evadere', which means escape or get away. In tax law this term signifies various ways for not paying taxes. The essence of this phenomenon is resistance to paying taxes, i.e. efforts of taxpayers to annul or diminish their tax obligation. The consequences of tax evasion are not only seen in loss of revenues and violation of the principle of fairness, but also in social stratification, distrust of citizens in the government, damage to the reputation of the country, etc.

Tax evasion can be both legal and illegal. Illegal tax evasion includes actions of taxpayers which violate tax laws, and as such they are sanctioned in the field of criminal law and torts. Legal tax evasion (tax avoidance) exists when a taxpayer reduces its tax obligation without violating tax law. It exists in two forms: legitimate (e.g. refraining from using taxed products) and illegitimate minimizing of tax obligation, where the law has not been violated but the goals, for which the law has been adopted, cannot be achieved,[3] by using legal vacuum or discrepancies of the tax law. In theory and practice it is not easy to distinguish between these two forms of tax avoidance, but it could be concluded that the legitimate tax avoidance is in compliance with intentions of the legislator, while the illegitimate is not. The illegitimate tax avoidance is often labeled as aggressive tax planning.[4]

THE MOST IMPORTANT MEASURES AGAINST TAX EVASION IN THE EUROPEAN UNION

Tax evasion is a serious problem in the European Union, primarily due to participation of national economies in the international economic relations. According to certain estimations, the member states lose circa 100 billion dollars annually due to tax evasion.[5] Therefore tax authorities strive to reduce these losses, i.e. to reveal and sanction non-compliance with the tax law as a tax tort or tax criminal offence. However, fight against international tax avoidance demands adoption of appropriate measures in the field of the tax law. The most important among these is the legislation on controlled foreign corporation – CFC legislation and legislation on thin capitalization.

The problem with these unilateral measures is the fact that they can come into conflict with freedoms guaranteed by the primary Union law. CFC legislation, which is focused on preventing tax evasion arising from transferring profit in low tax jurisdictions, can restrict the freedom of establishment, which means that residents of the member states can legitimately establish companies in other member states for the sole purpose of using tax reliefs, if they perform substantial economic activity. The situation is similar with the rules on thin capitalization, which will be in accordance with the Union law only if they prescribe the same tax consequences, regardless of residency. In other words, according to these rules, a member state cannot treat residents of other member states differently than its own residents. The Court of Justice of the European Union has expressed its position on discrepancy between the CFC legislation and rules on thin capitalization with the Union law in several cases.[6]

3 D. Popović, *Poresko pravo*, Pravni fakultet u Beogradu, Belgrade 2011, 45.
4 O. Farni *et al.*, *Tax Avodiance, Tax Evasion and Tax Havens*, Medieninhaber, Wien 2015, 4.
5 Discussion Paper on Possible Future Measures Against Non-Cooperative Jurisdictions and Aggressive Tax Planning and a Possible Strategy at EU Level – Seminar July 17 2012.
6 *Cadbury Schweppes plc, Cadbury Schweppes Overseas Ltd v Commissioners of Inland Revenue*, Case C-196/04; Lankhorst-Hohorst GmbH v Finanzmt Steinfurt, Case C-324/00.

However, fight against tax evasion, apart from unilateral measures, demands appropriate measures on the Union level. The most important among them are cooperation in tax matters, fight against tax havens and introduction of anti-abuse clauses in tax directives.

COOPERATION IN TAX MATTERS

Cooperation between tax administrations is one of the key elements in the fight against tax evasion. While taxpayers are not bound by national borders, tax authorities must respect these borders when performing their functions, so if they want an efficient implementation of tax laws, they have no other choice but to rely on legal assistance of other countries. The institutions of the Union were aware of this, so during the 1970s they initiated adoption of the rules addressing tax cooperation.

In the member states of the European Union there is plurality of legal sources regarding cooperation in tax matters. They can be classified into three groups: legal sources of the European Union, international and national legal sources.[7] The most important legal instrument in the area of direct taxation is Directive on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC – Directive 2011/16/EU.[8]

Directive 2011/16/EU has removed numerous deficiencies of the previously applicable legislation. In the context of fight against tax evasion, the provision that lays down that the member states can no longer refuse to supply information just because it is held by financial institutions is very important. Despite opposition of certain member states that were for preservation of the principle of bank secrecy, this principle was abandoned, because fight against tax evasion, i.e. ability to pay principle demands access to all financial transactions of taxpayers. Furthermore, this solution is in compliance with the principle of minimizing administrative costs, because tax authorities have direct access to this information, instead of reaching it by following the path of financial transactions of taxpayers.

Beside exchange of information, Directive 2011/16/EU provides for other forms of tax cooperation such as participation in administrative enquiries, simultaneous controls, notifications to each other of tax decisions and sharing of best practices. The most important and the most common form of tax cooperation is the exchange of information (on request, automatic and spontaneous), because it implies a minimum commitment of human and material resources and the least surrender of fiscal sovereignty. For a long time, within the framework of the European Union, the potential of automatic exchange of information was not fully used because its application depended on the agreement between competent tax authorities. It was the Directive 2011/16/EU that prescribed that the following information are subject to the automatic exchange: income from employment, director's fees, life insurance products not covered by other directives, pensions, ownership of and income from immovable property. The automatic exchange of information on savings income in the form of interest payments that a individual – resident of a member state realize in another member state, has been done ac-

7 K. D. Drüen, *Implementation of Provisions of Mutual Assistance in Tax Affairs*, EATLP Congress, Santiago de Compostela, 4-6 June 2009, 4.

8 Council Directive 2011/16/EU of 15 February 2011 on Administrative Cooperation in the Field of Taxation and Repealing Directive 77/799/EEC, *Official Journal of the European Union* L 64/1 of 11 March 2011; Council Directive 2014/107/EU of 9 December 2014 Amending Directive 2011/16/EU as Regards Mandatory Automatic Exchange of Information in the Field of Taxation, *Official Journal* L 359/1 of 16 December 2014; Council Directive 2015/2376 of 8 December 2015 amending Directive 2011/16/EU as Regards Mandatory Automatic Exchange of Information in the Field of Taxation, *Official Journal* L 359/1 of 18 December 2015.

cording to the Savings Directive,[9] which aimed at effective taxation of interest payments in the state of residence of the beneficial owner, and thus protect revenues of the state of residence, ensure fairness, and prevent distortions in capital movement. However, since amendments of the Directive 2011/16/EU from 2014 expanded the scope of application of the automatic exchange of information to interest payment,[10] the Savings Directive was abolished. Namely, since two legal instruments established the same system of exchange of information, in order to achieve higher degree of simplicity, transparency and efficiency, it was necessary that one of them be abolished. Directive 2014/107/EU has remained in force due to its wider scope and implementations of the global OECD standards in respect of the exchange of information.[11] Standardization in exchange of information contributes to simpler, cheaper and more efficient application of the tax laws, i.e. to optimal use of the obtained information in order to efficiently apply national tax laws. In order to prevent corporate tax avoidance, in 2015 Directive 2011/16/EU was amended by extending the cooperation between tax authorities to cross-border tax rulings and advance pricing arrangements.

On the level of the European Union there are also legal instruments on administrative cooperation in the field of indirect taxation.[12] Tax cooperation in the field of VAT and excise duties has several forms: the exchange of information, simultaneous controls, presence in administrative offices and participation in administrative enquiries. In order to facilitate multilateral cooperation in the fight against VAT fraud member states have also established a network for the swift exchange of targeted information – Eurofisc.

In the context of fight against tax evasion it is important to mention Directive 2010/24/EU[13] which prescribes the rules by which member states must provide assistance for the recovery of any claims relating to taxes, duties and other measures levied in another EU country.

FIGHT AGAINST TAX HAVENS

Globalization has had an impact on the emergence of competition in the field of taxation. On the one hand, it can encourage countries to offer an optimal level of public services with the lowest possible level of tax burden (fair tax competition), but on the other hand, it can lead to a situation where the higher degree of economic competitiveness is achieved through transforming tax jurisdictions into tax havens.[14]. As their number grows, the competition between them also grows, in the sense that they become specialized for certain types of oper-

9 Council Directive 2003/48 EC of 3 June 2003 on Taxation of Savings Income in the Form of Interest Payments, *Official Journal* L 157 of 26 June 2003; Council Directive 2014/48/EU of 24 March 2014 Amending Directive on Taxation of Savings Income in the Form of Interest Payments, *Official Journal* L 111 of 15 April 2014.

10 The information which is required to be exchanged should concern not only interests, dividends and similar types of income, but also account balances and sale proceeds from financial assets.

11 *https://home.kpmg.com/xx/en/home/insights/2015/11/tnf-eu-savings-tax-directive-is-repealed-replaced-by-new-standard.html*, 23 January 2016.

12 Council Regulation N° 904/2010/EU of 7 October 2010 on Administrative Cooperation and Combating Fraud in the Field of Value Added Tax, *Official Journal* L 268 of 12 October 2010; Council Regulation N° 389/2012 of 2 May 2012 on Administrative Cooperation in the Field of Excise Duties and Repealing Regulation N° 2073/2004, *Official Journal* L 121/1 of 8 May 2012.

13 Council Directive 2010/24/EU of 16 March 2010 Concerning Mutual Assistance for the Recovery of Claims relating to Taxes, Duties and other Measures, *Official Journal* L 84/1 of 31 March 2010.

14 OECD developed criteria for the detection of jurisdictions that have status of tax havens: no or nominal taxes, lack of effective exchange of information, lack of transparency, the absence of a requirement that the activity be substantial. *Harmful Tax Competition: An Emerging Global Issue*, OECD, Paris 1998, 27.

ations.[15]According to some estimates at the end of 2008 the world's tax havens have attracted between $5 trillion and $7 trillion in assets.[16]

Tax havens were especially drawing attention of tax authorities during the economic crisis of 2008, as one of its causes, so the fight against them was one of the goals of international meetings. During the G20 meeting in London it was stressed that appropriate measures would be taken against 'non-cooperative jurisdictions' on the level of the Union.[17]

Due to the fact that direct taxes in the European Union are not harmonized, it is possible that certain member states try to attract investors to their territories with low taxes. One of the ways to oppose the harmful tax competition within the Union is the provisions of the primary law of the European Union on prohibition of state aid.[18]

The main reason for prohibition of state aid lies in the fact that granting state funds to certain economic entities or economic sectors can distort competition, which is incompatible with the internal market of the Union. State aid in the form of the reduction of public revenues (e.g. reducing tax base, delaying tax debt) can be marked as a fiscal state aid.[19] In order to characterize a measure as a fiscal state aid, certain conditions must be met cumulatively. Firstly, the measure must ensure favorable tax treatment. Secondly, the advantage must be granted through state resources. Thirdly, it must affect or threaten to affect competition and trade between member states. Fourthly, it must be selective, i.e. limited to certain regions, sectors or economic activities. Therefore, one cannot discuss selective measures if it equally favors all enterprises on a national territory.[20] For example, special depreciation relief or reduced rate of corporation income tax only for some economic activities constitutes fiscal state aid. Even very broadly defined sector may be caught by the state aid prohibition. Thus, the Commission decided that 10% tax rate (general rate was 32%) for the whole of the Irish manufacturing sector constituted state aid because it was part of 'harmful strategy',[21] i.e. it excluded trades and services and in fact favored foreign investors.[22] Therefore, member states, in principle,[23] are not allowed to attracat investments on their territories by establishing special tax regimes for certain sectors of economy and businesses.

In the context of fight against tax havens, i.e. harmful tax competition within the Union, the special importance is given to the *Code of Conduct*,[24] which is not a binding act, but act that has a political power, which means that by violating the principle of fair competition, consequences occur solely in the political sense. By adopting it, the member states agreed not to introduce new tax measures that would lead to harmful tax competition, as well as that they will review current legislation and practice and amend them if they can lead to harmful tax competition.

15 Đ. Popov, 'Neke karakteristike ofšor poslovanja', *Zbornik radova Pravnog fakulteta u Novom Sadu* 1/2011, 41-42.
16 Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee - Promoting Good Governance in Tax Matters, COM 2009/201, 4.
17 J. L. E. Diaz-Berrio, *The Fight against Tax Havens and Tax Evasion: Progress since London G20 Summit and the Challenges Ahead*, Madrid 2011, 18, 21, 26.
18 Articles 107-109 of Consolidation Version of the Treaty on Functioning of the European Union, *Official Journal* C 326/49 of 26 October 2012.
19 D. Popović, G. Ilić-Popov, 'O pojmu poreske državne pomoći u pravu Evropske unije i uticaju na srpsko pravo', *Strani pravni život* 2/2015, 26.
20 B. Terra, P. Wattel, *European Tax Law*, Kluwer Law International, Alphen aan den Rijn 2008, 115-116.
21 A. Haupt, W. Peters, 'Restricting Preferential Tax Regimes to Avoid Harmful Tax Competition', *Regional Science and Urban Economics* 5/2005, 494-495.
22 B. Terra, P. Wattel, 116.
23 There are certain exemptions from the state aid prohibition. See: D. Popović, G. Ilić-Popov, 26-28.
24 Council Conclusions of the ECOFIN Council Meeting on 1 December 1997 concerning Taxation Policy, *Official Journal C/21*of 1 December 1997.

Having in mind positive effects of the fair tax competition, the *Code of Conduct* strives to identify only the measures that lead to harmful tax competition, i.e. measures which affect or may affect, in significant way, the location of business activity in the Union and which provide for a significantly lower effective level of taxation, including zero taxation, than those levels which generally apply in the member state in question.[25] The definition of harmful tax competition is not precise, so the Code of Conduct lists the following characteristics as crucial for the qualification tax measure as harmful:

- A measure is available only for non-residents or in respect of transactions carried out with non-residents;
- The measure does not affect the domestic tax base;
- The tax advantage is granted even without actual economic activity;
- Rules for profit determination do not follow internationally accepted standards;
- Lack of transparency.[26]

Based on the report of the so called *Primarolo Group,* which identified harmful national tax measures, the member states and their dependent and associated territories have abolished over 100 tax measures that have been qualified as harmful.[27] It is important to emphasize that the task of *Primarolo Group* was hard because the border between fair and unfair tax competition is not easy to identify.[28]

Problems with the implementation of the *Code of Conduct* occur due to its non-binding character. Namely, it seems that its adoption was the line of least resistance, because for many states it was easier to sign generally formulated, legally non-binding act, than to commit to take measures that would eliminate harmful tax competition. The previous statement is especially true for states like the Netherlands, Ireland and Luxembourg, which experienced economic boom mostly owing to favorable tax regimes. Therefore, it can be concluded that the *Code of Conduct* is a compromise between the states that have opposing interests in this issue due to 'influx' or 'reflux' of economic activities.

One of the ways to fight against tax havens on the Union level is to promote the principles of 'good governance' in tax matters, which means that the goal of the Union is to introduce principles of transparency, exchange of information and fair tax competition in taxation,[29] both in relation to the member states and non-member states. In order to promote these principles the Commission recommends the adoption by member states of a set of criteria to identify third countries not meeting minimum standards of good governance in tax matters, as well as appropriate measures against them (e.g. suspension of double tax conventions).[30] As a result of great pressures by the European Union and USA, a number of tax havens have concluded exchange of tax information agreements, what is certainly a change in their tax policy.[31]

The European Union makes efforts to enhance the application of principles of 'good governance', through financial support, in developing countries and countries included in the European neighborhood policy. In the context of fight against tax havens, it is important to mention the fact that provisions on prohibition of state aid are also being applied in relation to some non-member states, especially with the EEA states and with Switzerland.[32]

25 *Ibid.*
26 *Ibid.*
27 Promoting Good Governance in Tax Matters, 6.
28 C. M. Radaelli, 'The Code of Conduct against Harmful Tax Competition', *Public Administration* 3 /2003, 513-531.
29 Promoting Good Governance in Tax Matters, 5.
30 Communication from the Commission to the European Parliament and the Council - An Action Plan to Strengthen the Fight against Tax fraud and Tax Evasion, COM 2012 (722) final.
31 R. Seer, I. Gart, *European and International Tax Cooperation: Legal Basis, Practice, Burden of Proof, Legal Protection and Requirements*, Bulletin for International Practice February 2011, 88, 92.
32 Promoting Good Governance in Tax Matters, 7-8

THE USE OF GENERAL ANTI-ABUSIVE CLAUSES IN TAX DIRECTIVES

For a long time, activities of the Union's institutions were focused on the fight against double taxation. However, due to the fact that taxpayers have used appropriate mechanism whose goal was to circumvent the tax law, the other extreme has been reached – double non-taxation. Therefore, numerous deficiencies of the legislation have enabled tax evasion, and their removal emerged as an imperative for the Union's institutions. The solution has been found in introducing a general anti-abusive clause in tax directives, which means that member states may withdraw the benefits of tax directives in the case of transactions for which the principal motive or one of the principal motives is tax evasion, i.e. transactions which do not reflect economic reality.[33]

INSTEAD OF CONCLUSION

The fight against tax evasion is the condition for creating fair, abundant and efficient tax system. Therefore it is not surprising that the Union's institutions attempt to make it more effective. However, the fact that the Union law can be an obstacle for the implementation of unilateral measures against international tax avoidance should not be ignored. This shows that the goal is not to keep revenues within the borders of individual states, but within the Union, i.e. the stance of the Union's institutions is that taxpayers can exercise guaranteed freedoms in a member state which is most suitable for them in terms of taxation.

Conducted research has shown that the Union's institutions treat tax cooperation as a key element in fight against tax evasion. This is why the amendment of the Union legislation in this field was initiated. This primarily refers to increasing the scope of the automatic exchange of information on different categories of financial and non-financial income, enabling more direct contact between tax officers of the member states, as well as abolishing the principle of bank secrecy. On the other hand, the Union's institutions encourage tax cooperation with third countries, predominantly with tax havens. However, it seems that achieving this goal will be a long process, because many tax jurisdictions do not have anything else to offer but a favorable tax regimes, therefore, despite the pressure, they will not agree to implement the principles of 'good governance' in tax issues.

REFERENCES

1. *Cadbury Schweppes plc, Cadbury Schweppes Overseas Ltd v Commissioners of Inland Revenue*, Case C-196/04.
2. Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee – Promoting Good Governance in Tax Matters, COM 2009/201.
3. Communication from the Commission to the European Parliament and the Council – An Action Plan to Strengthen the Fight against Tax Fraud and Tax Evasion, COM 2012 (722) final.
4. Consolidation Version of the Treaty on Functioning of the European Union, *Official Journal* C 326/49 of 26 October 2012.

33 See: Council Directive 2015/121/EU of 27 January 2015 amending Directive 2011/96/EU on the Common System of Taxation Applicable in the Case of Parent Companies and Subsidiaries of Different Member States, *Official Journal* L 21/1, 28 January of 2015; Council Directive 2003/49/EC of 3 June 2003 on a Common System of Taxation Applicable to Interest and Royalty Payments Made between Associated Companies of Different Member States, *Official Journal*, L 157/49 of 26 June 2003, etc.

5. Conclusions of the ECOFIN Council Meeting on 1 December 1997 concerning Taxation Policy, *Official Journal C/21* of 1 December 1997.
6. Council Directive 2003/48 EC of 3 June 2003 on Taxation of Savings Income in the Form of Interest Payments, *Official Journal* L 157 of 26 June 2003.
7. Council Directive 2014/48/EU of 24 March 2014 Amending Directive on Taxation of Savings Income in the Form of Interest Payments, *Official Journal* L 111 of 15 April 2014.
8. Council Directive 2003/49/EC of 3 June 2003 on a Common System of Taxation Applicable to Interest and Royalty Payments Made between Associated Companies of Different Member States*, Official Journal*, L 157/49 of 26 June 2003.
9. Council Directive 2010/24/EU of 16 March 2010 Concerning Mutual Assistance for the Recovery of Claims relating to Taxes, Duties and other Measures, *Official Journal* L 84/1 of 31 March 2010.
10. Council Directive 2011/16/EU of 15 February 2011 on Administrative Cooperation in the Field of Taxation and Repealing Directive 77/799/EEC, *Official Journal of the European Union* L 64/1 of 11 March 2011.
11. Council Directive 2014/107/EU of 9 December 2014 Amending Directive 2011/16/EU as Regards Mandatory Automatic Exchange of Information in the Field of Taxation, *Official Journal* L 359/1 of 16 December 2014.
12. Council Directive 2015/2376 of 8 December 2015 amending Directive 2011/16/EU as Regards Mandatory Automatic Exchange of Information in the Field of Taxation, *Official Journal* L 359/1 of 18 December 2015.
13. Council Directive 2015/121/EU of 27 January 2015 amending Directive 2011/96/EU on the common system of taxation applicable in the case of parent companies and subsidiaries of different Member States, *Official Journal* L 21/1, 28 January of 2015.
14. Council Regulation N° 904/2010/EU of 7 October 2010 on Administrative Cooperation and Combating Fraud in the Field of Value Added Tax, *Official Journal* L 268 of 12 October 2010; Council Regulation N° 389/2012 of 2 May 2012 on Administrative Cooperation in the Field of Excise Duties and Repealing Regulation N° 2073/2004, *Official Journal* L 121/1 of 8 May 2012.
15. Drüen K. D.*, Implementation of Provisions of Mutual Assistance in Tax Affairs*, EATLP Congress, Santiago de Compostela, 4-6 June 2009.
16. Discussion Paper on Possible Future Measures Against Non-Cooperative Jurisdictions and Aggressive Tax Planning and a Possible Strategy at EU Level – Seminar July 17 2012.
17. Escario Diaz-Berrio J. L., *The Fight against Tax Havens and Tax Evasion: Progress since London G20 Summit and the Challenges Ahead*, Madrid 2011.
18. Farni O. *et al*., *Tax Avodiance, Tax Evasion and Tax Havens*, Medieninhaber, Wien 2015.
19. Harmful Tax Competition: An Emerging Global Issue, OECD, Paris 1998.
20. Haupt A., Peters W., 'Restricting Preferential Tax Regimes to Avoid Harmful Tax Competition', *Regional Science and Urban Economics* 5/2005.
21. https://home.kpmg.com/xx/en/home/insights/2015/11/tnf-eu-savings-tax-directive-is-repealed-replaced-by-new-standard.html.
22. Lankhorst-Hohorst GmbH v Finanzmt Steinfurt, Case C-324/00.
23. Popov Đ., 'Neke karakteristike ofšor poslovanja', *Zbornik radova Pravnog fakulteta u Novom Sadu* 1/2011.
24. Popović D., Ilić-Popov G., 'O pojmu poreske državne pomoći u pravu Evropske unije i uticaju na srpsko pravo', *Strani pravni život* 2/2015.
25. Popović D., *Poresko pravo*, Pravni fakultet Unoverziteta u Beogradu, Belgrade 2011.
26. Radaelli C., 'The Code of Conduct against Harmful Tax Competition', *Public Administration* 3 /2003.
27. Seer R., Gart I., *European and International Tax Cooperation: Legal Basis, Practice, Burden of Proof, Legal Protection and Requirements*, Bulletin for International Practice February 2011.
28. Terra B., Wattel P., *European Tax Law*, Kluwer Law International, Alphen aan den Rijn 2008.

UDC: 657.62

ANALYZING FINANCIAL STATEMENTS AS A TOOL FOR DETECTING FINANCIAL PATHOLOGY[1]

Aleksandar Petković, PhD[2]
Ministry of the Interior of the Republic of Serbia
Aleksandar Čudan, PhD
Academy of Criminalistic and Police Studies, Belgrade

Abstract: Financial statements are the end product of the accounting cycle and they can be viewed as summaries of all the transactions that occurred during a specific period of time. When a company's financial statements are prepared with integrity, changes in account balances from one reporting period to another have logical explanations. However, if a company is operated on fraud and economic crime, the perpetrators may attempt to disguise that fact by manipulating financial statements. The use of analytic techniques and procedures based on financial statement information is useful tool in detecting financial pathology because of their characteristics of identifying the unexpected relations that do not make sense. Because of these characteristics, they may be a supporting pillar at the start of a pre-investigation phase of criminal proceedings and help to identify suspicious areas of business, and also, during investigations, to make conclusions based on evidence found. The main goal of this article is to explore and elaborate the basic types of financial statements analyses and analytical procedures as a useful way in identifying fraud and criminal acts in financial statements.

Keywords: ratio analysis, vertical analysis, horizontal analysis, current ratio, quick ratio, collection ratio

INTRODUCTION

When a company's financial statements are prepared with integrity, changes in account balances from one reporting period to another have logical explanations. But, if a company is built or operated on fraud, however, the perpetrators may attempt to disguise that fact by manipulating financial statements to conceal missing assets or to understate liabilities. Due to the volume of transactions processed by a company every day, it is not possible for management, the auditor, or eventually law enforcement agents to examine every transaction. When fraud becomes so large that it affects not only specific assets or liability accounts, but also results in misleading or incorrect financial statements, an analysis of the financial statements of the company may identify potential problem areas. A law enforcement agent dealing with a financial crime will rarely, if ever, need to review or to reconstruct a complete set of business records. He will, however, be working daily with financial records and documents, for ex-

1 This paper is the result of the research on project: "Crime in Serbia and instruments of state responce", which is financed and carried out by the Academy of Criminalistic and Police Studies, Belgrade - the cycle of scientific projects 2015-2019.
2 tejana.ap@gmail.com

ample, analyzing ledger entry records by breaking a ledger balance into its component parts, listing those figures that make up balance, and checking to see if they are comparable with the account to which they were charged. The investigator should scrutinize those documents used to derive the figures in the ledgers, looking for alterations or for lack of a legitimate business purpose. The investigator can than compare and evaluate different sources for accuracy or proper recording while looking for any items that appear irregular or out of the ordinary. Remember that as an investigator looking beyond the obvious is necessary. Unfortunately, there exist no step-by step rules or formulas to guide investigators in researching the complete set of financial statements concerning fraud and financial crime. Auditors, however, have created financial techniques called analytical procedures to help them in checking and verifying financial data contained in financial statements, which can also be useful for financial investigators in connecting financial transactions to various kinds of criminal activity, especially in pre-investigation phase of criminal proceedings. Auditors have also found that financial statement analysis through using analytical procedures is the single best audit technique for discovering material errors and frauds. These experiences can successfully be used by police officers in detecting financial crime cases.

DEVELOPING EFFECTIVE ANALYTIC PROCEDURES

Analytical procedures mean "evaluations of financial information through analysis of plausible relationships among both financial and non-financial data. It's also encompass such investigation as is necessary of identified fluctuations or relationships that are inconsistent with other relevant information or that differ from expected values by a significant amount."[3]The use of analytic techniques based on financial statement information is fairly pervasive in business. Managers used them to monitor performance and to communicate with external investors, securities analysts use them to rate and value companies, bankers use them to determine whether to grant a loan or to monitor business results that may lead to the identification of troubled loans and auditors may use these techniques to identify areas of fraud risk and to determine whether financial statements are stated fairly. In the development of effective analytic procedures, law enforcement agents should go through the four phases[4]: 1)In phase one of the analytical review process, it is necessary to develop expectations of what amounts should appear in financial statement account balances. Expectations are the estimations of recorded accounts or ratios and are based on several factors such as industrial, economic, or environmental which can improve the predictive ability of analytical procedures. Data about prior year financial statements, budgets, industry information and non-financial information can be also very useful.2)Phase two of the analytical review process(identification) means comparing expected values with the recorded amounts, considering the materiality of the account balances being analyzed, the risk of misstatement associated with these account balances, and even the controls surrounding that account balances. Each of these factors may have an impact on defining the significant difference. In this phase, it is also necessary to take into account the overall materiality of the financial statements, because a small fraudulent change in a larger balance sheet item could have a material impact in the overall financial statements. Efficiency and effectiveness of this phase depends on financial investigators competency in recognizing fraud patterns in financial data and in hypothesizing likely causes of those patterns to serve as a guide for further testing.3)In phase three of the analytical review process (investigation), it is necessary to prepare the actual mathematical

3 International Standard on Auditing-ISA 520 "Analytical procedures"

4 Thomas W.Golden, Steven L.Skalak, and Mona M. Clayton: *A Guide to Forensic Accounting Investigation,* John Wiley&Sons, 2006, page 366

analysis or analytic procedure. In the creation of the mathematical analysis, it is critical to consider the validity and completeness of the underlying information on which the analysis is based. Fraudulent transactions quite typically do not go through the normal checks-and-balances system. 4) In phase three it is necessary to investigate the difference in order to draw appropriate conclusions. A basic premise of using analytical procedures is that there exist plausible relationships among data contained in financial statements and these relationships can reasonably be expected to continue. Where differences between expectation and recorded amounts are found, the first step is usually to ask management for an explanation, and to undertake an investigation of possible explanations for the expected/recorded amount difference. When possible, explanations from management should be corroborated by other evidence or corroborated by other company personnel not in the financial –reporting chain.

TYPES OF ANALYTICAL PROCEDURES

It is important to understand that financial analysis will not prove most effective if the only data analyzed are as of a single point in time. Financial information should include current and past performance, results, and balances, as well as projected and/or forecasted financial information, creating a picture of what the entity might do in the future. Financial statement analysis generally falls into five categories[5]:

- Vertical analysis,
- Horizontal analysis,
- Ratio analysis,
- Reasonableness testing and
- Analysis through data mining.

Vertical analysis is a technique for analyzing the relationships between items appearing as lines on the income statement or balance sheet by comparing elements of the financial statements with a common base item and then expressing these elements as percentages[6]. Usually, in a vertical analysis, the total assets line, or total liabilities plus equity line on a balance sheet is assigned a value of 100 percent and on an income statement, the revenue line is assigned a value of 100 percent. All other items on the statements are then expressed as a percentage of those two numbers. As with ratio analysis, vertical analysis is useful only if fraud is large enough materially to affect the balances on the financial statement. These percentages are then compared against prior-period percentages or against industry or comparable company percentages.Performing the same analysis on a disagregated basis by business unit or by geography often gives a deeper insight into which business unit is driving an unusual relationship or whether one particular business unit is an outlier.The analysis can be further disaggregated through analysis of a particular financial statement line item by component. For example, cost of goods sold can be analyzed by business unit and by component: materials, labor, overhead, and variances. Again, this analysis may uncover an unusual trend in material costs, which would have been masked by opposite trends in other components of cost of goods sold. Vertical analysis can also be effective when a practitioner is performing analysis of the balance sheet, For example, comparing percentage of accounts receivable aging categories across business units may indicate cash collection deterioration in a particular business unit.

5 Thomas W.Golden, Steven L.Skalak, and Mona M. Clayton: *A Guide to Forensic Accounting Investigation,* John Wiley&Sons, 2006, page 366
6 See:Howard E. Williams: *Embezzlement and Financial Fraud,* Charles C. Thomas Publisher, LTD, Springfild, Illinois, USA, 1997, page 83

Table 1:*Vertical Analysis-Crazy Eddie, Consolidated Statement of Operations*[7]

	Year Ended	%[1]	Year Ended	%	Year Ended	%	Year Ended	%
	03/03/85		03/03/86		03/01/87		02/28/88	
Net Sales	167147	100%	262268	100%	352523	100%	315539	100%
Cost of Goods Sold	127619	76,35%	194371	74,11%	272255	77,23%	346791	109,90%
Gross profit	39528	23,65%	67897	25,89%	80268	22,77%	(31252)	9,90%
Selling, general&administrative expence	26431	5,81%	2975	16,39%	61341	17,40%	96195	30,49%
Operating income	13097	7,84%	24922	9,50%	18927	5,37%	(127447)	(40,39)%
Other income	1418	0,85%	3210	1,22%	7403			
Interest expense	(572)	-0,34%	(820)	-0,31%	(5233)	-1,48%	(5972)	(1,89)%
Income before pension								
Contribution and income taxes	13943	8,34%	27312	10,41%	21097	5,98%	(133419)	(42,28)%
Pension contribution	600	0,36%	800	0,31%	500			
Income before income taxes	13343	7,98%	26512	10,11%	20597	5,84%	(133419)	-42,28%
Income taxes	6976	4,17%	13268	5,06%	10001	2,84%	(24321)	-7,71%
Net income	6367	3,81%	13244	5,05%	10596	3,01%	(109098)	-34,58%
Earnings per share	1.10		0.48		0,34			
Weighted average number of shares	5796		27664		31204			

Horizontal analysis is a technique for analyzing the percentage change in individual income statement or balance sheet items from one reporting period to the next. Accounts that are increasing or decreasing at rates significantly higher or lower than the majority of the account balances-and especially compared with related accounts-might be subject to further scrutiny. For example, if sales increased 25 percent during the base period but if cost of goods sold increased only 12 percent, further analysis of both accounts might be warranted Looking at trends on a quarterly, monthly, or even weekly basis can also assist in identification of areas to be pursued. Horizontal analysis supplements ratio and vertical analysis and allows learning whether any particular item has changed in an unusual way in relation to the change in net sales or total assets from one period to the next. As with any other financial statement analysis, the horizontal analysis, by itself, does not incriminate anyone or prove that fraud or embezzlement exists.

Implementation of horizontal and vertical analyses can be clearly viewed in fraud case „Crazy Eddie". Namely, U.S Securities and Exchange Commision filed and action against the founder and chairman of Crazy Eddie,Inc, and six other officers, directors, and employes, at

7 Source:Crazy Eddie Annual Report, 1985,1988, Securities and Exchange Commision, 10-K Reports (note: in thousands except for share data)

the chairman,s direction, falsified financial records to overstate the company,s pretax income by $2 million in 1986 and to show pretax earnins of $20,6 million instead of a net loss in 1987. Four defendants also allegedly sold over $60 million of Crazy Eddie stock while aware that the price of the stock did not reflect the actual value of the company. Three defendants consented to the entry o injunctions against them.[8] Because of the fact that, generally speaking, authorised officers of the Ministry of Interior dealing with economic crimes , do not implement analytical procedures in conducting pre-investigation phase of criminal proceedings, we are forced to present this case in the two tables indicated in this article.

Table 2: *Horizontal Analysis-Crazy Eddie, Consolidated Statement of Operations*[9]

	Year Ended	Year Ended	Change	Year Ended	Change	Year Ended	Change
	03/03/85	**03/03/86**	**85-86**	**03/01/87**	**86-87**	**02/28/88**	**87-88**
Net Sales	167147	262268	56,91%	352523	34,41%	315539	(10,49)
Cost of Goods Sold	127619	194371	52,31%	272255	40,07%	346791	27,38%
Gross profit	39528	67897	71,77%	80268	18,22%	(31252)	(138,93)%
Selling, general&administrative expence	26431	42975	62,59%	61341	42,74%	96195	56,82%
Operating income	13097	24922	90,29%	18927	(24,06)%	(127447)	(773,36)%
Other income	1418	3210	126,38%	7403	130,62%		
Interest expense	(572)	(820)	43,36%	(5233)	538,17%	(5972)	14,12%
Income before pension							
Contribution and income taxes	13943	27312	95,88%	21097	(22,76)%	(133419)	(732,41)%
Pension contribution	600	800	33,33%	500	(37,5)%		
Income before income taxes	13343	26512	98,70%	20597	(22,31)%	(133419)	(747,76)%
Income taxes	6976	13268	90,19%	10001	(24,62)%	(24321)	(343,19)%
Net income	6367	13244	108,01%	10596	(19,99)%	(109098)	(1129,61)%
Earnings per share	1.10	0.48	-56,36%	0,34	(29,17)%	(3,52)	(1135,29)%
Weighted average number of shares	5796	27664		31204		30957	

A SUMMARY OF KEY FINANCIAL RATIOS REGARDING FRAUD: HOW THEY ARE CALCULATED AND WHAT THEY SHOW

Financial ratios illustrate and analyze relationships within the financial statements elements, and it represents the comparison of relationships between financial statement accounts, the comparison of an account with non-financial data, or the comparison of rela-

8 U.S Securities and Exchange Commission Annual Report 1989, U.S Government printing office, Washington, DC, Page 8

9 Source.Crazy Eddie Annual Report, 1985,1988, Securities and Exchange Commision, 10-K Reports (note: in thousands except for share data)

tionships between firms in an industry. Ratio analysis is most appropriate when the relationships between accounts is fairly predictable and stable (e.g. the relationship between sales and accounts receivable). This analysis is primarily used to compare a company's financial figures over a period of time, a method sometimes called trend analysis. Ratios reflect relevant information about a business by quantifying the relationship among selected items on financial statements. A company,s ratios can be compared with ratios from a different period or periods, with a competitor,s ratios, and with an industry, s ratios. Anomalies in the form of erratice or unexplained changes or differences from the industry may be investigated further. It is instructive to calculate liquidity, activity, leverage, and profitability ratios and figures.[10] When unexpected changes occur, source documents and related accounts can be researched and examined ih more detail. Literally thousands of ratios can be calculated, but more is not necessarily better. Generally speaking, the nine key ratios can be deemed most useful in determination of the existence of fraud will be further explored[11]:

- Current ratio
- Quick ratio
- Inventory turnover ratio
- Average-number-of days-in-inventory ratio
- Receivable turnover ratio
- Collection ratio
- Debt-to equity ratio
- Profit margin ratio
- Asset turnover ratio

Considered as one of the best indicators of a company,s ability to pay its bills, the current ratio, expressed as current assets divided by current liabilities, measures the ability of a business to meets its current obligations from its current assets. Current assets are generally comprised of cash and cash equivalents, accounts receivables inventories, and prepaid expenses, while current liabilities are comprised of short-term borrowings, accounts payable and accrued expenses. It is the standard measure of an entity,s financial health, regardless of size and type[12]. A current ratio higher than 1 indicates that current liabilities can be covered with existing current assets. The current ratio, like the quick ratio, described below, is a liquidity ratio and „common" current ratio for a healthy business is recognized as around 2, meaning it has twice as many assets as liabilities.

$$\text{Current Ratio} = \frac{\text{Current Assets}}{\text{Current Liabilities}}$$

Poor receivables, fictitious or low inventory turns, or fictitious inventory, limit the usefulness of the current ratio. For that reason, this ratio must be reviewed in conjunction with ratios of those activities. Embezzlement will generally reduce the current ratio as cash declines, while unreported liabilites will result in a more favorable ratio. In some instances, embezzlers may hide their theft by reducing liabilities with a debit to accounts payable, which would

10 Normah Omar, Ridzuan Kunji Koya, Zuraidah Mohd Sanusi, Nur Aima Shafie: *Financial statement fraud-a case examination using beneish model and ratio analysis,* International Journal of trade, economics and finance, vol 5, No 2, April 2014

11Association of Certified Fraud Examiners: How to detect and prevent financial statment fraud, https://www.acfe.com

12 Howard Silverstone, Michael Sheetz, Stephen Pedneault, Frank Rudewich: *Forensic Accounting and Fraud Investigation for non-experts,* John Wiley&Sons-Third Edition, 2012, page 79

improve the current ratio. A high current ratio could also be a red flag, though, as it could signify obsolete inventory or uncollectable accounts receivable. This ratio should be considered in conjunction with earlier year results and in juxtaposition with comparable companies within the same industry.

Similar to the current ratio, the quick ratio(also known as the „acid test"), measures a business liquidity. However, many analysts prefer it to the current ratio because it excludes inventories when counting assets and therefore applies an entity,s assets in relation to its liabilities.The higher the ratio, the higher the level of liquidity, and hence it is a better indicator of an entity,s financial health.The accepted optimal quick ratio is 1 or higher. The formula is expressed as: current assets less inventory divided by current liabilities or cash plus marketable securities plus accounts receivable. The quick ratio compares the most liquid assets of the business with liabilities. Because inventories are typically the least liquid of a company,s current assets, the quick ratio is the measure of a firm,s ability to pay off short-term obligations without relying on the sale of inventories. The quick ratio thus represents a more conservative measure of liquidity than the current ratio. A dramatic decline in the quick ratio may require a closer review of accounts receivable or accounts payable.

$$\text{Quick Ratio} = \frac{\text{Current assets} - \text{inventories}}{\text{Current Liabilities}}$$

Potential creditors like to use this ratio because it reveals a company's ability to pay off under the worst possible conditions.

Inventory turnover ratio measures how often inventory turns over during the course of the year(or depending on the formula, another time period). In financial analysis, inventory is deemed to be the least liquid form of an asset.Typically, a high turnover ratio is positive;however, an unusually high ratio compared with the market for that product could mean loss of sales, with an inability to meet demand. The formula is expressed as: cost of goods sold divided by the average value of inventory(beginning inventory plus ending inventory, divided by two). This ratio helps determine whether inventory is overstated or cost of goods sold is understated.[13] Generally, overstating inventory has the effect of decreasing this ratio because the denominator is increased. Similarly, understanding cost of goods sold also decreases this ratio.A higer ratio is considered a favourable indicator of greater efficiency in generating sales. However, inventory theft or diversion will lower ending inventory(less inventory on hand) and increase cost of goods sold (from writing off stolen inventory), thereby causing this ratio to be abnormally high. Substantial changes in this ratio from one period to the next should be analyzed to determine whether they are being caused by inventory fraud.

$$\text{Inventory Turnover Ratio} = \frac{\text{Cost of Goods Sold}}{\text{Average Inventory}}$$

The Average-Number-of Days-in-Inventory ratio is the inventory turnover ratio expressed in number of days. This ratio is important because days in stock increase the risks of obsolescence, price reductions, and additional expences for storage. Significant changes or increase in the ratio can be indicators of inventory or purchasing schemes that results in fictitious inventory.

13 W.Steven Albrecht; Chad Albrecht: *Fraud Examination&Prevention,* Thomson South-Western: 2004, page 277

$$\text{Average-Number-of Days-in-Inventory Ratio} = \frac{365}{\text{Inventory Turnover}}$$

The Receivable turnover ratio measures the time between on-account sales and the collection of those sales and shows how quickly credit customers paying to the company. The greater the number of times receivables turn over during the year, the shorter the time between the sale and collecting the cash for that sale. Receivable turnover will increase in a fictitious sales scheme, because the fictitious sales will not be collected. Changes in the ratio may also be the results of failing to record bad debt reserves. A good receivables turnover ratio implies that the company is able to efficiently collect its receivables.

$$\text{Receivable Turnover Ratio} = \frac{\text{Net Sales on Account}}{\text{Average Net Receivables}}$$

The collection ratio, or days sales outstanding,measures the average number of days it takes a company to collect its receivables. A lower ratio generally indicates fasters receivables collection. Significant fluctuation in this ratio could results from changes in billing policies or collection efforts or could result from inflated or fictitious sales. If sales are inflated or fictitious, the ratio will rise. It is possible for sales to be inflated or fictitious of the receivables are consistently re-aged, because the ratio would not be adversely affected.

$$\text{Collection Ratio} = \frac{365}{\text{Receivable Turnover}}$$

Debt to Equity Ratio provides an indicator as to how much the company is in debt, by comparing debt to assets.[14]The debt-to-equity ratio is frequently used by creditors to manage the level of business risk assumed, because it measures the degree of ownership resources invested in the business, as compared with debt. It is sometimes referred to as a leverage ratio, because it shows the relative use of borrowed funds as compared with resources invested by owners. Unexpected increases in the ratio that correspond to an increase in accounts payable sholud be investigated further. Conversely, unexpected decreases in this ratio, perhaps to meet debt covenants and typically a decrease to account payable, should be investigated futher too. Debits to accounts payable may be indications that unauthorized expenses are being moved from the income statement to the balance sheet. A high Debt to Equity ratio can be considered an indicator of default risk. As with the current Ratio, Debt to Equity Ratios must be analyzed in the context of historical performance and industry comparability. A high ratio here means less protection for creditors.

$$\text{Debt to Equity Ratio} = \frac{\text{Total Liabilities}}{\text{Total Equity}}$$

Profit margin ratio measures the profit margin achieved by selling the company's products, [15]and is very useful

In assessing financial health of the company. A high profit margin indicates that management has a healthy pricing strategy and that a higher percentage of every euro that compa-

14 Howard Silverstone, Michael Sheetz: *Forensic Accounting and Fraud Investigation for non-experts,* John Wiley&Sons.Inc, 2004, page 70

15 Thomas W.Golden, Steven L.Skalak, and Mona M. Clayton: *A Guide to Forensic Accounting Investigation,* John Wiley&Sons, 2006, page 374

ny earns is going toward company's bottom line. A negative profit margin occurs when net income for a given period of time is negative rather than positive. Negative profit margins indicate that expenses outweighed the amount of Income Company generated. The formula is expressed as: net income divided by net sales.

$$\text{Profit Margin Ratio} = \frac{\text{Net Income}}{\text{Net Sales}}$$

Analyzing this ratio is important for the detection of various inventory-related scehemes or possible fictitious sales of cut-off issues.Companies that run into financial difficulty may attempt to "fudge" the number from time to time, as was the case with Enron in early 2000s. Profit margin analysis can be used, along with other ratios, as a means of fraud detection. However, if the company's earnings before interest and other expenses are positive, it may be that the company is using accounting tricks or outright fraud to make the business appear profitable, when it's not. Falling prey to this temptation can have serious legal repercussions.

The asset turnover ratio measures how effectively a company uses its assets, and the effectiveness of the usage of assets in terms of generating sales.[16] The higher the ratio, the more efficient the company is utilizing its assets. If the asset turnover ratio is increasing due to increases in sales, that could be the result of fictitious sales transactions. Where assets are used more in one year than the next with no apparent explanation, you must look at both the Financial Statements and source documents.

$$\text{Asset Turnover Ratio} = \frac{\text{Net Sales}}{\text{Average Assets}}$$

Many other ratios exist in the course of financial analysis, but these are deemed to be some of the most commonly used and understood. It must be remembered that ratios need to be considered in their entirety; unlike in the past, even ratio analysis alone is not to be considered the most useful information.

REASONABLENESS TESTING AND DATA MINING ANALYSIS

Reasonableness testing is the analysis of account balances or changes in account balances within an accounting period in terms of their "reasonableness" in light of expected relationships between accounts. This involves the development of an expectation based on financial data, non-financial data, or both. It is used to benchmark the results recorded in the financial statements against an independent expectation. For example, it is possible to calculate expected interest expense for a given period by multiplying the average outstanding debt balance by the average published index upon which the interest is based. Any unusual fluctuations identified when comparing this independent view with the amount recorded in the financial statements should be investigated. Reasonableness testing is usually more effective if the underlying information is disaggregated.For example, using the number of employees hired and terminated, the timing of pay changes, and the effect of vacation and sick days, the model could predict the change in payroll expense from the previous year to the current balance within a fairly narrow currency range. In contrast to both trend and ratio analyses

16 Frimette Kass-Shraibman; Vijay S. Sampath, *Forensic Accounting for Dummies,* Wiley Publishing, Inc., 2011, page 81

(which implicitly assume stable relationships), reasonableness tests use information to develop an explicit prediction of the account balance.

Data mining analysis is a set of computer-assisted techniques that use sophisticated statistical analysis, including artificial intelligence techniques, to examine large volumes of data with the objective of indicating hidden or unexpected information or patterns.Being able to examine and manipulate large volumes of electronic data is an essential ingredient of an effective fraud investigation. Much literature has surfaced over the past few years emphasizing the importance of data mining, both as part of due diligence procedures as weel as part of a fraud investigation, whether proactive or reactive.[17] But what exactly is data mining, and how does it work?It might include all of the following:[18]

- scanning transaction listings
- identifying gaps in check runs or shipping documents
- identifying duplicate invoice numbers, payments, or payroll transactions
- to the same payee
- matching return dates and credit memos to test for proper cutoff
- comparing recent invoice prices with costs on the perpetual inventory records
- filtering to identify all new suppliers, nonstandard journal entries, accounts under
- dispute, and the like
- stratifying or grouping customers accounts by balance size or employees by overtime pay.

Consideration of data mininig should be made at the outset of an investigation specifically to determine what relevant data might be available, what skills are available within the team and how will the data analysis fit in with the wider investigation.Because of that there are two inherent limitations to data mininig, The first is that analysis will be limited by the quality and quantity of information within the files provided. Simply stated, It can be analyzed or mined only what the company provides in the files. The second limitation is that the analyses are limited by the examiner,s experience and level of creativity. Finally, data-mining analytics are different from the other types of analytic procedures in that they are queries or searches performed within accounts or other client data to identify anomalous individual items, while the other types use aggregated financial information.

CONCLUSION

Financial pathology has been occurring as long as financial statements have been prepared and issued, but the financial scandals show that not even the largest and most important companies in the economy can remain untainted. Knowing where to look for fraud is a key component in detecting one. The need for investigators to understand the company and its business is evident: The key factors that influence the business operations may be expected to affect company's financial information. Changes in amounts, ratios, trends, or relationships can be accurately interpreted only in that context. But unexpected changes, or no change when a change was expected, may be due to error, fraud, and sometimes simply to random occurrences. To detect fraud through financial statements, law enforcement agents can focus

17 See:Clifton Phua, Vincent Lee, Kate Smith, Ross Gayler:*A comprehensive survey of data mining-based fraud detection research,* School of Business Systems, Faculty of Information Technology, Monash University, Australia

18 Thomas W.Golden, Steven L.Skalak, and Mona M. Clayton: *A Guide to Forensic Accounting Investigation,* John Wiley&Sons, 2006, page 370

on unexplained changes, but to understand how financial statements can signal fraud, one must be familiar with the nature and types of basic analytical procedures. Financial analysis techniques can help law enforcement agents do discover and examine unexpected relationships in financial information and concerning that to discover unexpected deviations which may indicate illegal acts or fraud. Unfortunately, it is very rare, practically unnoticed in the practice of authorised police officers employed in the Ministry of the Interior of the Republic of Serbia, to perform analytical procedures during pre-investigation and investigation phase of criminal proceedings. Such being the case, application of these techniques indicated in this article, may be useful tool for law enforcement agents works at Serbian police, in combating all forms of financial crime cases.

REFERENCES

1. Association of Certified Fraud Examiners: *How to detect and prevent financial statment fraud, https://www.acfe.com*
2. Clifton Phua, Vincent Lee, Kate Smith, Ross Gayler:*A comprehensive survey of data mining-based fraud detection research,* School of Business Systems, Faculty of Information Technology, Monash University, Australia
3. Normah Omar, Ridzuan Kunji Koya, Zuraidah Mohd Sanusi, Nur Aima Shafie: *Financial statement fraud-a case examination using beneish model and ratio analysis,* International Journal of trade, economics and finance, vol 5, No 2, April 2014
4. Frimette Kass-Shraibman; Vijay S. Sampath, *Forensic Accounting for Dummies,* Wiley Publishing, Inc., 2011
5. Howard Silverstone, Michael Sheetz, Stephen Pedneault, Frank Rudewich: *Forensic Accounting and Fraud Investigation for non-experts,* John Wiley&Sons-Third Edition, 2012
6. Howard Silverstone, Michael Sheetz: *Forensic Accounting and Fraud Investigation for non-experts* John Wiley&Sons.Inc, 2004,
7. IFAC-International federation of accountants: *International standard on auditing- ISA 520 "Analytical procedures", https://www.ifac.org/*
8. Thomas W.Golden, Steven L.Skalak, and Mona M. Clayton: *A Guide to Forensic Accounting Investigation,* John Wiley&Sons, 2006,
9. W.Steven Albrecht; Chad Albrecht: *Fraud Examination&Prevention,* Thomson South-Western: 2004
10. U.S Securities and Exchange Commission Annual Report 1989, U.S Government printing office, Washington, DC 20402

UDC: 343.95
343.91:159.923.3
343.91:316.752

EXAMINATION OF CORRELATION BETWEEN PERSONALITY TRAITS AND VALUE ORIENTATIONS OF PERPETRATORS OF CRIMINAL ACTS

Sanja Đurđević
University of Belgrade, Faculty of Special Education and Rehabilitation[1]
Rosa Šapić
University of Bijeljina
Dragana Daruši
Private General Practice of Novi Sad

Abstract: Criminological Science attaches particular importance to the interaction of personality traits and value orientation to the aetiology of criminal behaviour, because the personality traits and value orientation are very important phenomena when committing crimes and also for criminal career lengths and severity of the acts they commit. **The aim** of the study was to determine the correlation of personality traits and value orientation with the offenders who have committed a crime. **Method:** The sample in the study consisted of the convicts from the prison ward of the Correctional Institution Požarevac - ZABELA (N = 152). A set of predictor variables consisted of conative personality dimensions which were the subject matter: 1) Extroversion (EPSILON), 2) Hysteria (HI), 3) Anxiety (ALFA), 4) Aggressiveness (SIGMA), 5) Dissociativeness (DELTA), 6) Social integration (ETA). These personality traits were tested using the battery of tests KON-6 by Momirović et al. A set of criterion variables consisted of four value orientations: 1 - Hedonistic orientation, 2 - Economic utilitarian orientation, 3 - Altruistic orientation, 4 - Activist orientation. Basic statistical methods used in the processing and analysis of the data collected included: descriptive statistics (mean and standard deviations), factor analysis of variance, canonical discriminant analysis. The **results** show that there is a statistically significant correlation between personality traits aggressiveness and hedonistic value orientation ($c = .183$, $p < .05$) and in the negative direction between Dissociative and activist value orientation ($c = -.168$, $p < .05$). The findings indicate that the group of offenders find as the most appropriate value the orientation of economic-utilitarianism ($M = 3.78$; $SD = 1.18$) and found as the least accepted hedonistic one ($M = 2.99$; $SD = 1.33$). **Conclusions:** Both in the prevention and the treatment of crime, considerable attention must be given to changes in personality, and in particular value-orientation because these are fundamental conditions for abandonment of criminal behaviour patterns.

Keywords: crime, personality traits, value orientations.

1 E-mail: djurdjevic.sanja26@gmail.com

INTRODUCTION

In a judicial proceeding, during the phase of proving guilt, weighing penalty and passing a sentence on the type of sanctions to be enforced, as well as in the process of classification of the convicted person within correctional institutions, a significant role is attributed to personality traits and the life style, i.e. value orientations of the offender.

Personality traits are one of the most important elements of personality structure and they describe a relatively long lasting and stable tendency to think, feel and behave consistently. Personality traits and value orientations are important etiology factors of primary and repeated criminal acts. The research conducted by some authors proved that aggressiveness and hedonism are predictors of violent acts and criminal acts of proprietary nature saturated with violence.[2], [3] The examination of the interaction between personality traits and value orientations is important not only for understanding criminal behaviour etiology but also for the treatment of the offender, since the alterations of personality and value orientations are foundations for abandoning criminal behaviour patterns.[4], [5] Modern psychological experience shows that plenty of personality traits are resistant to changes while the criminal sanctions are in effect and that the emphasis must be put on the values and their interaction with personality traits. By altering the offenders values, we actually achieve alterations of these interactions. The alterations can result in completely different behaviour patterns and cessation of criminal activities. This can happen on condition we are familiar with personality traits and value orientations of the people being sanctioned and who are in the process of undergoing these sanctions.

THE CONCEPT OF VALUE ORIENTATION

Value orientations are considered to be an important component of all types of behaviour. The analysis of relevant literature shows that there is a large number of definitions of values, even up to eighteen criteria were used by authors in attempt to define this concept.[6] Most frequently used definition is the definition of Milton Rokeach, according to whom the values are "a steady belief that certain specific behaviour patterns or existence states are personally or socially more desirable than the opposite or reverse behaviour pattern or existence".[7] Our authors define the values as relatively stable, general and hierarchically organized characteristics of an individual or a group, formed by mutual interaction of historical, current social and individual factors, which due to attributed desirability direct behaviour of their exponents to certain goals[8] or like a lasting, distinctly positive relation the person has with certain objects rated as important and for whose achievement there is a distinct personal engagement.[9] Besides all these things, among the researchers engaged in defining values, there is a general consensus that the values are integrated social attitudes, *having a three-component-structure (cognitive, affective and conative component) and influencing different behaviour patterns.*[10], [11] In case there is a significant scope of personality traits variance in the structure of value orientations, then it is logical to presume that these traits are intervening variables between the

2 Radovanovic, 1992.
3 Radulovic, 2006.
4 Cochrane, 1971, 73-87
5 Froggio et al., 2010, 581-596.
6 Pantic, 2005, 49-69.
7 Rokeach, 1973:5 in Alargic, 2012:16.
8 Pantic, op.cit.
9 Rot & Havelka,1973.
10 Schwartz & Bilsky,1990, 878–891.
11 Sram, 2003, 91-114.

values and behaviour. The examination of value orientations, can be often found in research works performed on samples of non-criminal population, while the values of prison subculture were, as a rule, researched in the population of those sentenced to imprisonment.[12] Very interesting is the research into value orientations performed on the population of juvenile and adult offenders prior to enforcement of a criminal sanction. This is how Radulovic, Vucinic and Gojkovic (1997)[13] proved in their study on the degree of immorality of juvenile and adult delinquents that juvenile delinquents are not only conative more disorganized but also more immoral than the delinquents of legal age, and the research conducted by Radulovic[14] showed that the value structure of the examinees inclined to use psychoactive substances consists of hedonistic and materialistic value orientations.

THE CONCEPT OF PERSONALITY TRAITS

A theoretical personality concept which was the starting point of the research is Momirovic's personality concept (1992),[15] which belongs to the so-called psychobiological or psychoneurological concept of personality research. According to this concept, personality traits are primarily of a neurological origin or more precisely the result of functioning of neurological regulative systems. Variations in the functioning, functional disorder in the first place, result in six habitual ways of reacting, namely six personality traits. All regulative systems are part of a whole, i.e. the same neurological space and thus there is a certain degree of parallel functioning. The six traits are extraversion-introversion, hysteria, anxiety, aggressiveness, dissociation and social integration.

PREVIOUS RESEARCHES

Although there are only a few researches into values in the world, they are mainly focused on the young population and comparison of their values to the non-criminal population. Our paper refers to the results of Ajdukovic's research (1989)[16] that researched into acceptance of hedonistic and utilitarian orientation in juvenile delinquents. The results of this research confirm the thesis that young offenders are in the first place of hedonistic and utilitarian orientation and that these are their central value orientations. Research into alterations of value orientations during the institutional treatment of juvenile offenders in the same paper discovered that the duration of exposure to a resocializing treatment does not in any way bring positive changes of these value orientations but, on the contrary, these values change in the opposite direction. Practically the same tendency of value orientations, including hedonistic lifestyles, was established in the work of Adzijevic (2009)[17] also with the juveniles on the institutional treatment. Finally, we are going to quote the work of Anic (2004)[18] which compares the values of male juvenile offenders in institutional treatment with the values of a non-delinquent group. According to the acquired results, significant differences were discovered in the value concepts such as escape from everyday duties, integration into social life and self-confidence. Although this research is important to us, we have to point out that there are not many research attempts to establish value orientations of adult offenders sentenced to prison.

12 Radovanovic, op.cit.
13 Radulovic et al., 1997, 101-114.
14Radulovic,op.cit
15 Momirovic et al. 1993.
16 Ajdukovic, 1989.
17 Adžijevic, 2009.
18 Anic, 2004.

There are more researches into the relation between values and personality traits. In our country, remarkable researches are the ones conducted by Sram (2003)[19] and Radulovic (2006)[20]. Sram's research into value orientations showed that a relatively small percentage of anxiety neurosis can be explained by value orientations, while on the other hand, value orientations have a significant role in the variance of hostility and psychopathic aggressiveness. By examining the possibility of differentiation between psychopaths, Radulovic came to a conclusion that a high degree of psychopathic deviation can be related to the value orientations such as immorality, hedonism, egocentric ruthlessness. Special importance is given to the research into the traits referring to psychopathic structure of a personality. Since this type of structure is responsible for a huge percentage of violent offences and terrorism, it can be easily said that nowadays this type of research is dominant in the sphere of criminology, psychology and criminal psychology.

Our study was examining correlations between value orientations, described as preferred life styles, and personality dimensions amongst prisoners. The aim was to determine what the correlations are of hedonistic, economic-utilitarian, altruistic and activist value orientations with personal dimensions: Extraversion, Hysteria, Anxiety, Aggressiveness, Psychoticism and Integration.

METHODS

Subjects Sample

The research was conducted in a male prison Zabela in Pozarevac, the Republic of Serbia. The Ethical Committee of the Ministry of Justice gave consent for the research conducted in accordance with the ethical standards of the Helsinki Declaration. All subjects were informed about the objectives of the study and gave their consent. The criteria of anonymity is also fully complied. The study involved 152 prison offenders. The average age of the respondents was 34.93 years (SD = 7.96), the majority of respondents has secondary school qualifications (57.8%), the average length of sentence was 3.74 years (SD= 0.18).

Measures

In the study we used the CON-6 battery of conative personality tests construed on the basis of the cybernetic model of the functioning of the primary conative regulators.[21] The battery comprises six subtests enabling the assessment of six basic regulation systems: test "EPSILON" refers to the regulator of activity (in psychological terms this regulator is identified as Extraversion), test "HI" refers to the regulator of organic functions (in psychological terms this regulator is identified as Hysteria), test "ALPHA" refers to the regulator of defence reactions (in psychological terms this regulator qualifies as Anxiety or Neuroticism), test "SIGMA" refers to the regulator of attack reactions (this regulator is identified as Aggressiveness), test "DELTA" refers to the system for coordination of regulatory functions (this regulator is identified as Dissociation or Psychoticism. Test "ETA" refers to the system for integration of regulatory functions and system for excitation and inhibition (this regulator is identified as Integration in the social field). In these six tests there are180 items grouped, the format of answering is the Likert five-point scale. The items content is designed so that a higher score indicates a greater disintegration and less control over the regulatory functions. The calculation of results is simple addition to any items, and the result of each test can range from 30 to

19 Sram, op.cit.
20 Radulovic, op.cit.
21 K. Momirovic, B. Wolf and Z. Dzamonja, „*The KON–6 Cybernetic Battery of Conative Tests.* Belgrade: Association of Psychologists of Serbia", pp.37, 1993. Katalog psiholoških instrumenata: *http://www.dps.org.rs/images/stories/cpp/katalog%20testova%202014.pdf*

150 points. The test result can be converted into normative values in four ways (converted into z-values, t-values, percentiles or classification groups). Metric characteristics of the tests are: Reliability 0.95-0.98; Representation 0.90-0.97; Homogeneity 0.50-0.69; Validity 0.95-0.97[20].

Value orientations are formulated through a comprehensive description of the four life-styles, modelled on Joksimović's research:[22]

The first style - hedonistic orientation: *One must enjoy direct pleasures. Money is to be spent on achieving more satisfaction in life.*

The second style - economic and utilitarian orientation: *To acquire material goods and aim for material security.*

The third style - altruistic orientation: *To help other people, to devote one's life to others. Being good and generous to other people, to sacrifice oneself for others.*

The fourth style - activist orientation: *Being active in changing the situation and relations in the environment and wider society. Fighting for distant goals and ideas.*

The respondents were asked to assess the lifestyles with marks ranging from 1 to 5.

Data Analysis Models

Data analysis was performed firstly through descriptive statistical methods. After that, correlation between value orientations and personality traits is analysed using a Pearson Correlation.

RESULTS AND DISCUSSION

The results in Table 1 present the arithmetic mean of test scores (M) and standard deviation (SD) on Battery CON-6.

Table 1: *Distribution of personality dimensions (M and SD) on Battery CON-6 subtests*

Subtest	M	SD
EPSILON	109.31	19.06
HI	66.55*	30.13
ALFA	86.76	25.73
SIGMA	104.16*	22.63
DELTA	68.18	27.49
ETA	68.48*	17.17

* higher average scores

The results showed higher average scores on the scales that measured Hysteria (HI), Aggressiveness (SIGMA), and Integration (ETA). Dimensions of scale, which measures Extraversion (EPSILON), Anxiety (ALFA) and Dissociative (DELTA) manifested the average functioning. The results tell us that at the core of criminal behaviour lies in poor integration into the social field, high aggression and hysteria. These results correspond to the findings of previous studies that have already shown that in prison one can find considerable number of aggressive, anxious, socially poorly integrated and pre-psychotic similar individuals.[23], [24]

22 Joksimovic et al. 2008.
23 Eysenck & Gudjonsson, 1989.
24 Miller & Lynam, 2001, 765-798.

Our finding of pronounced hysteria as a personality trait of criminals matches the Eysenck's findings on hysteria as a predictor of criminal behaviour. In their papers, Radovanovic and Radulovic[25] reported poor social integration as a feature that distinguishes offenders. Also, in Cale's[26] study we find that in criminals who committed serious criminal acts personality traits that point to problems in social relations occur. The link between aggression and criminal behaviour has been demonstrated in numerous psychological and criminological studies.[27], [28]

The degree of preference of individual value orientations shown in the form of arithmetic mean (M), i.e. in the average acceptance of each value orientation (on a scale of 1 to 5), with the following information on the standard deviation (SD) (Table 2).

Table 2: *Preference of value orientations*

	Mean	Std. Deviation
Hedonistic orientation	2.99	1.46
Economic-utilitarian orientation	3.78	1.29
Altruistic orientation	3.35	1.24
Activist orientation	3.62	1.35

An economic-utilitarian value orientation is the most likable in prison population (M=3.78), while the hedonistic orientation is the least accepted and thus ranked last (M=2.99). A high activist orientation is noticeable (3.62). The finding that the economic and utilitarian orientation is dominant within the group of convicts is not different from most studies of the lifestyle of the members of the general population in which we find that in recent years a lifestyle that involves the acquisition of material goods and economically secure future becomes more and more popular.[29] However, it can be assumed that this value orientation in a number of offenders (e.g. the perpetrators of theft) determines their criminal behaviour. The explanation for the low preference of hedonistic orientation may be found in the supremacy of these values due to the specific conditions in which the inmates are currently (prison environment). The finding that concerns a highly valued active orientation is very intriguing, and it includes a commitment to distant targets and actively changing relationships in the immediate environment. It is possible that the findings realistically reflect the adopted value orientations, but because of the specific conditions in which our respondents found themselves in (prison) and the possibility of giving socially desirable answers there is, to some extent, the problem of the reliability of the findings.

The correlation between the value orientations and personality traits is presented in Table 3.

In Table 3 it is obvious that there is a statistically significant correlation between a hedonistic orientation and aggressiveness as a personality trait ($r = 0.183$, $p = 0.024$), while the activist value orientation is connected with dissociation (psychoticism) ($r = - 0 .168$, $p = 0.039$) and in the negative direction. Other traits are not in a statistically significant correlation with value orientations. Increased aggressiveness and tendency towards hedonism are the traits of a psychologically unstable personality. This correlation between hedonism and aggression shows that aggressive, often reckless behaviour and focus on personal satisfaction and fulfilment of the current desires comes out of the basically criminal behaviour. If we know that a high-degree aggression is always found in psychopaths, our result is similar to a study by Radulovic[30]on psychopathic deviances, which says that the high level of psychopathic devi-

25 Radovanovic et Radulovic, op. cit.
26 Cale, 2006, 250-284.
27 Burt & Donnellan, 2008, 53-63.
28 Otasevic et al. 2014, 765-798.
29 Joksimovic et al., op. cit
30 Radulovic, op.cit.

ance is associated with hedonism and with egocentric ruthlessness. We find the same results found in a study that examined the relationship between the so-called Dark Triad traits (i.e. Machiavellianism, narcissism, and psychopathy) and values in the members of the general population, showing that there is a correlation between personality traits and hedonism as a life value. Thus, in this study a significant interconnectedness was found between Hedonism and Machiavellianism (r = 0.28) and Psychopathy (r = 0.34).[31] Our findings and conclusions are congruent with Međedović's that the predictors of criminal behaviour are basic personality traits and amorality. Amorality, according to this author consists of hedonism, laziness and low impulse control.[32]

Table 3: *Pearson Correlation between the value orientations and personality traits*

		Epsilon	Hi	Alfa	Sigma	Delta	Eta
Hedonistic orientation	Pearson Correlation(r)	.147	.074	.049	.183	.115	-.012
	Sig. (p)	.071	.362	.546	**.024***	.159	.879
Economic-utilitarian orientation	Pearson Correlation(r)	.018	-.016	.112	-.077	-.004	.013
	Sig. (p)	.823	.847	.170	.343	.964	.872
Altruistic orientation	Pearson Correlation(r)	.106	-.053	.060	-.126	-.061	-.060
	Sig. (p)	.195	.517	.465	.121	.459	.461
Activist orientation	Pearson Correlation(r)	.047	-.088	-.081	.051	-.168	-.094
	Sig. (p)	.565	.283	.320	.531	**.039***	.249

*p < 0.05

CONCLUSION

Investigation of the values and personality traits on a sample of 152 convicts showed the following most important results:

1. All four tested value orientations have a relatively high degree of acceptance. Basic tendencies were observed in the value orientations of the convicted persons. Value orientation that was most widely accepted was the economic and utilitarian one, and the lowest level of acceptance was towards hedonistic orientation. Interestingly, the orientation towards materialistic values, to personal profit and gaining the economic empowerment was the value orientation that is otherwise proved to be the most acceptable one also in young people from the general population (see: studies Joksimović et al.). Also, this value orientation is not statistically significant for the studied personality traits. This could mean that the materialistic lifestyle is a generally accepted value in our society. Also, this value orientation is probably determined by the different variables (deprivation of freedom, the degree of integration into the prison environment, the length of the sentence).

2. It was found that there are pathological conative tendencies in a sample of the convicts: poor social integration, high aggressiveness, expressed psychoticism and increased levels of

31 Kajonius et al. 2015, 173-178.
32 Medjedovic et al., 2012, 277-294

hysteria. Only in the domain of the trait extraversion-introversion there are average results. Also the results of other authors as well as the meta-analytical studies (see: Radovanovic, Miler and Lynam, Burt and Donnelan) confirmed that within the structure of personality offenders there are usually exactly these pathological tendencies and that they highly correlate with the manifestation of criminal behaviour.

3. A significant association between hedonistic lifestyle and aggressiveness was found. This finding is even more significant if one bears in mind that in our sample of convicts, the score on a scale that measures the aggressiveness was elevated. Therefore, it is the pathologically aggressive persons with such a trait who are certainly not able to postpone their current need for satisfaction.

4. It has been proven that in a sample of convicts activism is significantly associated with psychoticism and in the negative direction, too, which means that people with high psychoticism have low pronounced activism and vice versa. This result is quite logical, given that people with high psychoticism are cruel and inhuman, insensitive to the needs of others. It is exactly by committing offences that the offenders endanger others, or at least do not think about the consequences of their behaviour on other people.

So, it is determined that amongst the persons from our sample group, in the structure of hedonism as value-orientation we found a significant volume of variance of aggressiveness as personality trait. Our findings suggest that with these people aggressiveness will be mediating variable between value-orientation and behaviour. Our findings may have practical significance for planning of offenders' corrective treatments, regarding on which characteristics and values corrective methods should be directed.

The limitation of this study is that other variables are not included, such as group influence, treatment, alcohol abuse, etc. Furthermore, the future studies should adopt a more versatile approach to examining value-orientations, by using more than one instrument. Despite these limitations, the findings of our study show the importance of value orientation and conative personality dimensions, and they provide a basis for further research. Repeating researches like this one can add to better viewing of regularities that personality characteristics and values are important phenomenon for committing crimes and the length of criminal carrier, also for the weight of criminal act committed.

REFERENCES

1. Ajduković, M. „ *Vrijednosne orjentacije i očekivanja maloljetnih delinkvenata*". Zagreb, Narodne novine, 1989.
2. Adžijević, D. *Vrijednosne orjentacije adolescenata u institucionalnom tretmanu*. Zagreb, Edukacijsko-rehabilitacijski fakultet, 2009.
3. Alargić, D. "*Karakteristike pojedinca kao činioci sistema vrednosti pripadnika Vojske Srbije*". Doktorska disertacija, pp 16, 2012.
4. Anić, K. *Usporedba vrijednosti adolescenata nedelinkvenata i delinkventne populacije u instituciji*, Zagreb, Edukacijsko-rehabilitacijski fakultet, 2004.
5. Burt, S. A. & Donnellan, M. B. "Personality correlates of aggressive and non-aggressive antisocial behavior", *Personality and Individual Differences, vol.* 44(1), pp. 53-63, 2008.
6. Cale, E.M. "A quantitative review of the relations between the "Big 3"higher order personality dimensions and antisocial behavior". *Journal of Research in Personality,* vol. 40, pp. 250–284, 2006.
7. Cochrane, R. "The structure of value systems in male and female prisoners". *British Journal of Criminology*, vol. 11, 73-87, 1971.

8. Eysenck, H.J. & and Gudjonsson, G.H. "*The causes and cure of criminality*". New York: Plenum Press, 1989.
9. Froggio, G. & Lori M. Deviance. "Among Young Italians Investigating the Predictive Strength of Value Systems". *International Journal of Offender Therapy and Comparative Criminology.*vol.5, no.4, 581-596, 2010.
10. Joksimović, S. i Janjetović, D. "Pojam o sebi i vrednosne orijentacije adolescenata". *Zbornik Instituta za pedagoška istraživanja,* vol. 40, pp.288-305, 2008.
11. Kajonius P. J., Persson B. N. and Jonason P. K. Hedonism, Achievement, and Power: Universal values that characterize the Dark Triad, Personality and Individual Differences 77 (2015) 173-178).
12. Kluckhohn, C., "Values and Value Orientation in the Theory of Action", *In: Parsons, T., Shills, E., Toward a General Theory of Action, Harper and Rowe*, New York: 391-436. 1962.
13. Miller, J.D. & Lynam, D. "Structural models of personality and their relation to antisocial behavior: a meta-analytic review", *Criminology,* vol. 39, pp. 765-798, 2001.
14. Medjedovic, J, Kujacic, D. and Knezevic, G. "Personality-related determinants of criminal recidivism", *Psychology,* vol. 45 (3), pp. 277-294, 2012.
15. Momirović, K., Wolf, V. i Džamonja, Z. „ KON-6 Kibernetička baterija konativnih testova". Beograd. Savez Društava psihologa Srbije, pp. 37, 1993.
16. Otasevic, B., Jovanov, M. and Oljaca, M. "Differences in dimensions of aggressiveness between violent and non-violent offenders and general population", *Primenjena psihologija,* vol. 7(4), pp. 565-579, 2014.
17. Pantić, D. "Da li su vrednosti bivših komunističkih zemalja slične". Beograd. *Zbornik matice srpske za društvene nauke*, pp.49-69, 2005.
18. Radovanović, D. "*Čovek i zatvor*". Beograd. Institut za sociološka istraživanja. 1992.
19. Radulović, D. "*Psihologija kriminala - psihopatija i kriminal*". Beograd. FASPER &IKSI. 2006.
20. Radulović, D., Vučinić, B. i Gojković, V. "O stepenu amoralnosti maloletnih I punoletnih prestupnika", *Časopis za kliničku psihologiju I socijalnu patologiju,* vol.4, pp.101-114, 1997.
21. Rot, H. i Havelka N. *"Nacionalna vezanost i vrednosti kod srednjoškolske omladine*". Institut za psihologiju i Institut društvenih nauka. Beograd. 1973.
22. Šram, Z. "Vrednosne orijentacije i struktura ličnosti: relacije na srednjoškolskom uzrastu završnog razreda*", Pedagogija*, vol.3-4, pp 91-114, 2003.
23. Schwartz, S. H. & Bilsky, W. "Toward a Psychological Structure of Human Values: Extensions and Cross-Cultural Replications", *Journal of Personality and Social Psychology,* vol. 58, pp.878–891, 1990.

UDC: 336.226.331:339.192(497.11)

COMPARATIVE OVERVIEW OF THE IMPACT OF THE EXCISE TAX PRICE INCREASE ON THE INCREASE OF EXCISE GOODS SMUGGLING AND TRAFFICKING

Igor Pejovic, PhD[1]
College of Economics and Administration, Belgrade
Sinisa Dostic, PhD[2]
Ministry of the Interior of the Republic of Serbia

Abstract: In the Republic of Serbia in previous years the excise tax on cigarettes, pipe tobacco, alcohol, alcoholic beverages, coffee, oil and petroleum products has been increased several times. From January 1, 2016, a new increase in excise duties entered into force and excise taxes were introduced to some new products such as low alcohol beverages containing more than 1.2% alcohol. On the other hand, as a result of increasing the rate of taxation of these products, increased smuggling and illegal trade of excise goods can occur as a negative effect. The aim of this paper is to show the comparative analysis of the impact of increasing excise taxes on smuggling and trafficking of excise goods. Comparative analysis of these changes in years, which will be parts of the statistical collection, will be a good basis for comparison of one component, the price increase of excise duties with the other component of the research, such as unlawful acts of smuggling and illicit trade in excise goods.

Key words: the Republic of Serbia, excise tax, excise goods, smuggling, trafficking

INTRODUCTION

Excise taxes represent a specific type of additional, very highly set sales tax, mainly on monopolistic kinds of goods for which there is considerable demand caused by mass consumption. Historically, excise appears as the oldest form of consumption tax. In many countries, excise tax exists parallel with the sales tax, so the consumption of specific types of excise products is taxed twice, once with the excise tax, and the second time with the sales tax. Certainly it is not rare that the excise tax is applied and on luxury goods and motor vehicles, too.[3]

Using excise, the country adds to its budget in an easy and effective manner. According to the current Law on Excise Tax,[4] excise is taxed on the following products: oil derivatives, biofuels and bioliquids, tobacco product, alcoholic drinks, coffee, liquid filling of electronic cigarettes, electricity for end use. From January 1, 2016, despite an increase in the excise tax, government expanded the list of products subject to excise tax, so low alcohol beverages

1 dr.ipejovic@gmail.com
2 sinisa.dostic@mup.gov.rs
3 Milošević, G., Javne i monetarne finansije, KPA, 2010. p. 252.
4 Član 2. Zakon o akcizama, "Sl. glasnik RS", br. 22/01...55/15

containing more than 1.2% alcohol have been added to the list. In the paper we will analyse only three types of "the most interesting" type of smuggling of excise goods, such as fuel, alcohol and cigarettes, as well as the specific subcategories of these products that are the most frequent subject of smuggling and illicit trafficking. So far, the smuggling of excise goods was very interesting mainly due to lower prices of these products in neighbouring countries, but this increase and the introduction of new taxes could lead to a further increase and expansion of illegal activities.

This paper will present scientific synthesis and comparison of increase in excise duties in the previous period and the impact of increasing excise taxes on the goods to an increase of illegal trade and smuggling. The first part of the paper will present and analyse excise and financial increase of levies on certain products per year, while in the second part of the paper, we shall present and empirically analyse the increase or decrease in smuggling and illegal trade of these products. Finally, we will bring a conclusion whether the increase in excise duties rapidly affects the increase in smuggling and trafficking of excise goods.

EXCISE AND EXCISE STAMPS

Excise taxes are additional taxation of certain products.[5] According to the law, the obligation to pay excise duty arises at the moment when one country produces goods that fall under the regime of excise taxes, or when in that country the goods are imported which the country of domicile considers as excise goods. The Ministry of Finance approves the issuance of excise stamps, which mark the excise goods, and which are printed under the supervision of the National Bank of Serbia at the Institute for Manufacturing Banknotes and Coins in Belgrade. The National Bank of Serbia also keeps records and controls the issuance of excise stamps. The Government of the Republic of Serbia issues a regulation on the appearance of the control excise stamp which must be located on any excise product, the type of data stored on the stamp, the manner and procedure of approval and issuance of stamps, keeping records of approved and issued stamps and labelling of cigarettes and alcohol.

EXCISE DUTY ON OIL DERIVATIVES

The fiscal effect of excise tax in our tax system is undeniable.[6] From January 1, 2016, the excise tax on petroleum products is increased once again compared to the previous year, and it is now 2.5 dinars per litre of fuel. Although it was logical (as cause-and-effect relationship of increasing excise rates) fuel in our country has not increased in price, even the price of fuel compared to the previous period decreased. The reason for this is the global decline in oil prices at the world market. In early 2016, a barrel of oil was $ 40, until the end of January of the same year when it dropped to only $ 28. As the oil is stock exchange commodity, the current fluctuations in oil prices per barrel at the beginning of February 2016 amount to about $ 30. If we look at the Serbian market, we have to notice that the price of fuel is significantly higher compared to the neighbouring countries. Significantly lower fuel prices in the neighbourhood attract illegal import of fuel in our country and allow for smuggling of these goods.

5 Fabris, N., Pejović,I., Ekonomska politika teorija i praksa, Beograd, 2013., p.139.
6 Milošević, G. Teorija i praksa finansijskog prava, KPA 2011, p. 257.

Table 1: *Fuel prices per country*

Type of fuel / country	SRB	CG	BiH	MK	BG	RO	H	CRO
Diesel	1,029	0,820	0,823	0,633	0,946	1,044	0.960	0,962
Unleaded	1,030	1,020	0,874	0,933	0,982	1,077	1,027	1,128

The graph and Table 1 show how big is the amplitude of differences in the price of fuel in our country and the neighbouring countries, because it is exactly from these countries that the goods are illegally imported into our country. As the price of fuel is lower in the neighbouring countries, there is a potentially large possibility of illegal smuggling and trade in such goods in the countries where the fuel is much less expensive. Looking at the wholesale price that is significantly lower than retail, given that the neighbouring countries have their resources in the illicit smuggling, this problem is a potentially high risk for trafficking.

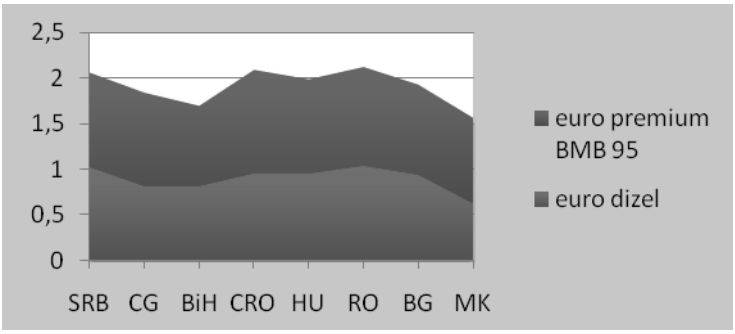


Figure 1: *The price of fuel per countries*

The price of fuel is significantly lower in all countries except Romania and Croatia, if we consider only unleaded gasoline. The lowest fuel price by far is in the FYR of Macedonia, but other countries in the region also have a lower cost of these products, so it can be concluded that there is a reasonable danger of smuggling these types of fuel from almost all the countries in the region. If around 60% of the price of fuel goes into the budget of the Republic of Serbia, and if a larger budget deficit increases the demand for capital, the reduction of price of excise might be a good way to reduce smuggling and trafficking in this type of excise goods. Given that the price of fuel is lower in almost all the countries in the region, it is cost-effective for the population in the entire border zone of the Republic of Serbia on all sides to tank the fuel in the neighbouring countries, rather than in their own country, which additionally highlights the subject of decreasing the excise on fuel, and is something that the creators of economic policy in our country should reconsider.

Table 2: *Price movements of excise taxes per year*

Fuel/year	2013	2014	2015	2016
Dizel	42	46	50	50
BMB 95	49,60	50	52,50	52,50

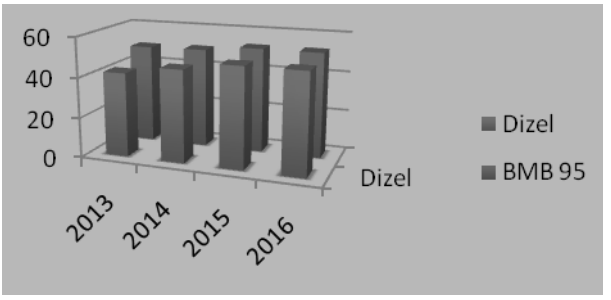


Figure 2: *The movement of excise price per year*

The table and graph show that the excise tax increases every year, and this growth trend suggests that in the next period we can expect price increases of excise duties. The growth trend has benefits for the increase in the budget of the Republic of Serbia, but other variables should also be analysed to reflect the justification for continuing increases in excise taxes on fuel. The additional problem is that the Republic of Serbia is a candidate for entering the EU, therefore it must predict the process of harmonization of the excises with the currently existing excises in the EU, which are significantly higher than the current prices in Serbia – which altogether demands a thorough preparation and timely harmonization. Customs unions and free trade areas start with the removal of trade barriers among the Member States,[7] so the Republic of Serbia must be prepared for the same procedure and the regime.

EXCISE TAX ON ALCOHOL

At the beginning of 2016, the excise taxes on alcoholic beverages and tobacco increased by 12.20%. Alcohol drinks include drinks which, depending on the raw material from which they are produced and the ethanol content in them, are placed on the market in one country. According to this law, alcoholic drinks are divided into the strong alcoholic and light alcoholic drinks and the beverages containing more than 1.2% vol alcohol. The excise tax on alcoholic beverages is paid per litre of the alcoholic beverage. The price of excise taxes is harmonized annually according to the consumer price index in the calendar year preceding the year in which the harmonization is performed, according to the data of the Republic authority responsible for statistics. In the following part of the paper, we will present the table of movements of excise taxes per year and per type of product.

7 Hitris, T. Ekonomika Evropske unije., Institut za ekonomiku i finansije, 2003., p. 8.

Table 3: *Price movements of excise taxes per year and per type of product*

Type of alcoholic beverages	2014	2015	2016
Brandy, fruit, grapes, wine and other fruit brandy	117	122	124
Brandies made of grain and other agricultural raw materials	298	309	316
Other spirits	190	198	203
Low-alcohol beverages	19	20	21
Beer	22	23	24

It is noticeable that the new categories are introduced, and also permanent increase of excise duties each year. The Government of the Republic of Serbia has explained the increase in excise duties on alcoholic beverages and the introduction of excise duty on low alcoholic drinks and beer as one of the measures to reduce consumption of alcohol, especially the consumption among the younger population, which should be praised. But when we look at the rate of smuggling and trafficking of alcoholic products, we must consider the possibility of reducing the price of excise duties as one of the options for combating trafficking.

EXCISE TAX ON CIGARETTES

The harmfulness of tobacco and tobacco products is undeniable, and the high levies that affect the final retail price of these products as well as the ban on smoking in public places certainly positively effect that cigarettes are less used. Unfortunately, there is a noticeable huge difference in the price of cigarettes sold by us and in the neighbouring countries, especially in the European Union where the price of cigarettes is significantly higher. Excise taxes are calculated as a percentage relative to the amount of the weighted average retail selling price of cigarettes. The weighted average retail selling price (Pmc), calculated as a ratio of the total value of the entire smoking tobacco and other tobacco products released for marketing at retail prices (Uv), the total quantity of smoking tobacco and other tobacco products released on the market in the Republic of Serbia in the previous half-year. (Uk), which can be mathematically expressed as:

$$\text{Pmc} = \frac{Uv}{Uk}$$

The Government of the Republic of Serbia, at the proposal of the competent ministry semi-establish the amounts of the average weighted retail price and the amount of the minimum excise duty. Looking at the consolidated balance state and the movement of excise saw a steady trend of growth of government revenue from excise duties.

Table 4: *Increases in excise taxes per year*

Goods/Years	2010	2011	2012	2013	2014	2015 Jan-Sep
Total excises	152.167	170.949	181.097	204.761	212.474	167.330
Excise duties on oil derivatives	80.376	89.049	90.702	107.176	121.331	91.361
Excise duties on tobacco	60.771	69.186	76.424	83.752	87570	64.938

SMUGGLING OF EXCISE GOODS

Smuggling of goods involves the transfer of illegal goods across the state border. Smuggling is not closely related only to excise goods, but also to all other types of goods which can be obtained in other countries in various manners. Common to all types of contraband is that significant profit can be made by importing and selling these goods in one country. Global loss of tax revenues from cigarette smuggling is between 40 and 50 billion US dollars per year, and the loss of tax revenue in the EU in 2012 is estimated at about 12.5 billion euros.[8] The methods of smuggling are constantly improving and adapting to the current social and economic conditions; and the goods smugglers very efficiently and wisely make use of the conditions at the market, which certainly defines the selection of goods intended for smuggling.[9] Smuggling in our country is recognized by Article 230 of the Criminal Code which provides for three cases and sanctions for:

- Persons who carry goods across the customs line, avoiding measures of customs control,
- Persons who by avoiding measures of customs supervision, transfer goods across the customs line armed, in groups, or using force or threats, and
- Persons engaged in the sale, distribution or concealment of goods not cleared by customs, or who organize a network of dealers or middlemen for distribution of such goods.

Customs Administration of the Republic of Serbia through its customs offices monitors and controls the entry of all kinds of goods into the country. According to Article 5 of the Customs Code of the Republic of Serbia,[10] customs control is a set of measures taken by the customs authority for the application of customs and other regulations on goods subject to customs supervision. Customs control includes specific actions carried out by the customs authority regarding goods, such as examining goods, verifying the existence, validity and authenticity of documents; review of accounting and other documents, examination and search of vehicles, inspection and search of personal luggage and other goods that persons carry with them or on them, and the conducting of official procedures and other similar activities in order to ensure the proper application of customs and other regulations.

The smuggling of goods and avoiding customs supervision and control can be carried out at the official border crossing and it is accomplished by hiding the goods, camouflaging goods (deliberate wrong display of facts), the transfer of goods outside the border crossing and the corruption of border security subjects (customs, border police, border inspection services, etc.).

If we consider the excise goods, we can say that the Western Balkan region, given its geographical location and the specific political and economic conditions which govern it, is very suitable for smuggling. In the neighbouring countries there are different tax rates for excise goods, which is one of the most important reasons for the emergence of so-called high-excise goods smuggling across the state border. By high taxation of excisable goods in one country and selling the same in the other, where the excise taxes are higher, significant unlawful financial benefit can be achieved. In addition, large amounts of high excise goods which have not been taxed arrive through illegal routes, which is especially the case with cigarette smuggling.

Cigarette smuggling in Croatia, for example, has been detected lately at the seaside via the local motorboats, and at the entry and transit through Croatia from the direction of Serbia, by

8 INTERPOL, Legal Handbook Series Tobaco En
9 Kulić, D: Krijumčarenje preko državne granice –metodika otkrivanja istraga, Bezbjednost, policija, gradjani br.2, Banja Luka 2006., p. 779.
10 Carinski zakon, Službeni glasnik RS, br. 18/2010, 111/2012 i 29/2015

pick-up trucks or privately owned cars. In relation to Bosnia and Herzegovina the illegal trade of cigarettes is more and more present in the parts bordering with Montenegro, and less in the parts bordering with Serbia and Croatia. Through Serbia the cigarettes are smuggled originating from Serbia, the Autonomous Province of Kosovo and Metohija (APKIM), and Albania via Montenegro by trucks in the direction of Croatia, Hungary, or Romania, or more frequently by train towards Bulgaria. For the smugglers from the FYROM the route of cigarette smuggling towards Bulgaria is interesting due to high price resulting from huge excise taxes.[11]

Serbia's geographical position in the central part of the Balkan Peninsula, on the important routes linking Asia and Europe represents a transit area for smuggling tobacco products into illegal markets of the countries in the region or in Western and Central Europe. Smaller amounts of these products are distributed on the black market and in our country. Cigarettes are smuggled into our country mostly from Montenegro, the FYR Macedonia, and Bosnia and Herzegovina. In addition, cigarettes are transported from the area of the APKIM towards the territory of central Serbia. Smugglers use especially made containers inside the cargo, passenger vehicles and pick-up trucks, but they smuggle the goods by regular bus and train routes, towards Romania, Hungary, Bulgaria, and Croatia with the final destination in Western and Central Europe, where the price of cigarettes is several times higher. There are several modes of smuggling the cigarettes with or without excise stamps. The cigarettes produced in our country and exported for example to the FYROM, are transported to the APKIM, and then via the illegal smuggling channels they are returned to the territory of central Serbia, with Macedonian excise stamps. Then the smuggled cigarettes are further smuggled through our country to the territory of Hungary, Romania or Croatia and/or to Western Europe. The cigarettes predestined for the illicit markets in Western and Central Europe are bought in smaller quantities in retail or wholesale facilities in our market, and then smuggled to the north of the country. From there, via the illegal smuggling channels they are transferred to the territory of Hungary, where they are stored in warehouses or repackaged to be transported to the countries of final destination, mainly to France, Germany, Switzerland, Great Britain and the Nordic countries.[12]

Another interesting way of smuggling is the illicit trade of the so-called "illicit white cigarettes" or "cheap white cigarettes". They represent the second largest category of illegal products in our market. They are mainly produced in the Middle East and in Asian countries, and are shipped to the ports in the Adriatic Sea, from where they are smuggled through our country from the direction of Montenegro and the APKIM into Hungary and Romania. It is estimated that these cigarettes make up 27.9% of the total illegal markets in the EU, provided that their concentration is the greatest at its borders. It is estimated that, with the increase in the purchasing power of the population, they will retain a significant place in the market due to attractive packaging, quality and retail price in the market.[13]

The research conducted in our country shows that smuggling of goods has several characteristics:

1. Transactions involving smuggling were mostly if not entirely, based on the spoken agreements between the partners involved in smuggling, as the partners always paid one another in cash, and the amount was rarely discussed.
2. It rarely happened that associates of a trafficking kingpin use violence towards other smugglers.
3. Self-preservation permeates the world of smugglers.

11 Procjena opasnosti od teškog i organizovanog kriminala u Crnoj Gori, MUP Crne Gore, Uprava policije, Podgorica, February 2014, p. 63.
12 Procena opasnosti od teškog i organizovanog kriminala u Srbiji, MUP Republike Srbije, Beograd, December 2015., p. 90-91
13 Ibid

4. Secrecy was standard protocol of the operations.

5. Smugglers have used different methods of corruption.[14]

Smuggling of high excise goods in Serbia is increasingly taking on the characteristics of organized crime, given the fact that quite organized heterogeneous groups deal with it, which have an international character. These criminal groups have a built hierarchy and internal organization and good material and technical resources. All means of transport are used for transfer of the contraband across the border. The smuggled goods are often followed by the so-called companions who have the task to provide the entire transport, to organize trans-shipment of goods, or to prevent any surprise, both from the competitors in the business, or by the control authorities.[15]

COMBATING SMUGGLING OF EXCISE GOODS

Combating smuggling and illicit trafficking of excise goods is one of the priorities in the fight against the grey economy and economic crime. After establishing the quality control system by marking the petroleum products (2014), the illegal sales of these products in Serbia has significantly been reduced. In the past, a part of the oil and petroleum products arriving to our market used to arrive by illegal smuggling channels. A comparative analysis of the increase in excise duties and smuggling of excise goods, we can see that the biggest risk is the appearance of illicit trafficking and smuggling of oil and oil products from the neighbouring countries using river vessels, primarily of inland waterways, where the international regime of navigation takes place, but also other waterways, given the much lower price of these products in the countries neighbouring with the Republic of Serbia. One of the modes of smuggling in the previous period was the purchase of oil and petroleum products from the refineries in Serbia for the companies originating from the APKIM, and then diverting and reselling the same goods on illegal markets. Alcohol, alcoholic beverages and coffee are smuggled in small quantities, primarily from Montenegro and the APKIM. The most common form of trafficking and smuggling is illegal trafficking of tobacco and tobacco products. Due to different socio-economic factors, there was an expansion of these criminal activities. Statistically speaking, there is information that a total of 64.5% of Serbia's population aged 18 to 64, during their lifetime smoked or tried to smoke cigarettes. Daily consumption of cigarettes is almost equally spread among genders and age groups.[16] These data show how the smuggling of these types of products is a lucrative business, but also a significant income to the country through excise taxes on cigarettes and similar products.

According to data of the Ministry of Finance, the Department of Tobacco, in 2014 225 tons of tobacco leaf and cut tobacco were seized, while the police officers seized nearly 94 tons. Due to the spreading of illegal markets of cut tobacco and otherwise comminuted tobacco and tobacco products, in 2014 there was a nominal decline of 7.4% in the revenues from excise taxes on tobacco products. The largest seizures of cut tobacco were carried out on the territory of Sabac, Sremska Mitrovica, Belgrade, Novi Sad, Pancevo and Kraljevo. In the control procedure, in addition to tobacco, the machines for cutting and moisturizing tobacco, the scales for weighing, motor vehicles and a certain amount of accessories for smoking were also seized. In 2014, a total of 31.92 tons of cigarettes were confiscated. In 2014, the Ministry

14 Milošević, M. i dr.: Organizovani kriminal i terorizam-osvrt na pojavne oblike u Republici Srbiji, Zbornik radova sa naučnog skupa o organizovanom kriminalu – stanje i mere zaštite, Beograd, 2005., pp. 43-47.

15 Krecoja, M.:Kriminalistika za osnovno policijsko obrazovanje, Yugo-Pirs, Novi Sad, 2006., p. 488.

16 Procena opasnosti od teškog i organizovanog kriminala u Srbiji, MUP Republike Srbije, Beograd, decembar 2015. godine, p. 87.

of Interior seized a total of 80,644 boxes of different cigarettes or 221 carton of cigarettes a day. Those were mainly the cigarettes without excise stamps. The value of the seized cigarettes in 2014 was over 111 million dinars.[17]

The Ministry of Interior's[18] data in the area of the protection of the state border during the past two years indicate that the smuggling and illegal trade of excise goods has increased. Regarding that, below is the table that shows the smuggling of cigarettes, oil and alcohol.

Table 5: *Smuggling of excise goods by type of products and years*

Goods/Years	2014	2015
Cigarette (box)	14446	16524
OIL (tons)	3.04	8.03
Alcohol (litre)	370	493

In 2015 compared to 2014 there was an increase of cigarette smuggling recorded by 14.38%, an increase in smuggling oil by 164.14%, and an increase in smuggling alcohol by 33.26%.

When it comes to combating the smuggling of excise goods, it is necessary to emphasize the importance of international cooperation among border services (border police, customs, border inspection services, etc.), which contributes to more effective prevention of cross-border crime.[19]

Joint actions (operations) of border services contribute to a great extent to the effectiveness of combating smuggling of excise goods. Joint actions have the purpose to suppress all forms of cross-border crime, improve inter-agency and international cooperation, address common security threats on the border, more effective use of human and technical resources for border services and focus on the implementation and implementation of the Concept of the integrated border management. The presumption of the success of joint operations is to engage quality staff at all levels, as well as the precise definition of their responsibilities.[20]

When it comes to international police reaction in combating this form of cross-border crime, as an example, it should be noted that the Task Force SECI Centre for the fight against smuggling and fraud, periodically conducted, operational action codenamed "Shadow",[21] in which all 13 member states took active part with the aim to prevent the smuggling of cigarettes through Southeast Europe, where attention was focused on all types of goods transport (road, air, sea and rail).

The transformation of the SECI Regional Centre for Combating Trans-border Crime, established in 1999 in Bucharest (Southeast European Centre for Combating Trans-border Crime) lead to creating "SELEC" (Southeast European Law Enforcement Centre) - Centre for law enforcement in Southeast Europe. The legal framework was the signing of the "SELEC" Convention in Bucharest, on 1 December 2009.[22] The main characteristic, which makes

17 Ibid.

18 Work reports of the MoI of the Republic of Serbia for the period 2010-2015, http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/izvestaji.h preuzetodana 10.02.2015. godine

19 Milošević, M.; Dostić, S: Modaliteti medjunarodne saradnje graničnih službi izapadnog Balkana, Zbornik radova sa medjunarodnog naučno-stručnog skupa sa medjunarodnim učešćem "Suzbijanje kriminala u okviru medjunarodne policijske saradnje", KPA i Hans Zajdel fondacija, Tara, 2011., pp. 52-53.

20 Ibid, p. 54.

21 More details on the result of the "Shadow" action, see at selec.org/anual report

22 SELEC Convention provides a broad legal basis for a more significant regional cooperation in conducting investigations and court proceedings, and creating basis that the Centre can receive significantly greater legal authorizations to combat cross-border organized crime, terrorism, smuggling of people and goods. SELEC Center establishes and develops mechanisms based on cooperation

the SELEC Centre different from other bodies responsible for enforcing regulations, is joint operational work of police and customs and direct exchange of information and documents among liaison officers delegated to the SELEC Centre by their respective member states, and contact person at the national level.[23] Customs data network for combating trafficking uses the database and communication via e-mail, with a view to speed up and facilitate the cooperation in combating smuggling and exchange of information and intelligence. All relevant data related to seizures made by the customs service of a country as well as the photographs that illustrate the ways of concealing goods are entered into the database.[24]

COMPARATIVE ANALYSIS

By analysing the statistical data, tables and graphs, it is evident that there is a link between the increase in excise taxes and the increase in smuggling of excise goods. As the excise tax increases every year, the rate of smuggling of excise goods increases. The government in cooperation with the Ministry of Interior, the Customs and the judicial authorities undoubtedly do their best at combating smuggling of excise goods or statistically speaking, the smuggling of excise goods is growing. Its cause can be found in the price of excise goods in the countries of the region that is significantly lower than in our country, but also in the fact that the excise tax is also large, so the damage for the state is significant.

The analysis of fuel prices in the country and in the region indicates that the country also suffers major loss of public revenues due to the fact that fuel import is not controlled in passenger cars and commercial vehicles in regular tanks. If it is known that in the FYR of Macedonia, fuel is almost twice as cheaper than in the Republic of Serbia, and it is considerably cheaper in other countries in the region, and that only one truck has a reservoir tank of 1,400 litres of fuel, without taking into account the cars that pour the cheaper fuel in the neighbouring countries for their needs, you can see how huge the loss to the country is on a daily basis.

By reducing the excise tax, the government would reduce the state revenues in the budget, but on the other hand, it would reduce the smuggling of excise goods, therefore the level of revenues would be restored to a similar or better position. In this respect, there is an option to tighten controls at borders and combat new methods of smuggling which would then have the effect, as well as the regulations on the maximum fuel tanking in the means of transport. In the European Union, for example, there is a law for trucks, that no truck can enter the EU with more than 200 l of fuel. Each litre entered above this limit is taxed, and the driver must pay not only taxes, excise taxes, but also the misdemeanour fine. Such treatment may be one way to at least partially reduce the endangerment of budget revenues of the Republic of Serbia.

If we look at the market and seizure of cigarettes which increased in percentage similarly to the increase in excise tax rates (around 15%), we will notice that it is approximately by the same amount as the increased prices that the rate of cigarette smuggling increased.

Taking this data as the basis of comparative analysis, it is clear that in proportion to the increase in excise taxes, the smuggling of cigarettes increased. This fact can be a guideline for

between the Member States in the implementation of the law, which the country can still be used in order to provide mutual assistance and support in the prevention, detection and application of legal mechanisms for sanctioning cross-border crime. Also, the Centre provides assistance to the member states to harmonize legislation on law enforcement with the standards and requirements of the EU, and supports the Member States in improving the cooperation among law enforcement institutions. Cited according to- Law Enforcement Centre in South East Europe (SELEC), http://www.mfa.gov.rs/sr/index.php/spoljna-politika/eu/regionalna-saradnja/selec?lang=lat,.

23 http://www.upravacarina.rs/lat/medjunarodnasaradnja/Stranice/ClanstvoUMedjunarodnimOrganizacijama.aspx donloaded on February 9, 2016.

24 Ibid, downloaded on February10, 2016.

economic policy makers to influence the reduction of excise tax in order to see whether there will be a reduction in smuggling of excise goods in future. Currently, there is a positive growth trend in both observed categories, which still leaves room for some new analysis.

CONCLUSION

Economic crime in the sphere of smuggling of excise goods is a serious problem for Serbia, considering the damage in the form of the evaded excise tax which is inflicted upon the country's budget, as well as to the society as a whole. The largest number of the investigated cases in this area which are related to the criminal activities are those related to the import and the trade of goods. According to the exact indicators, illegal import of the so-called high excise goods is dominant - oil, alcohol and the like, where, in addition to illegal import across the border (smuggling), other methods are also used, such as documents fraud during import (customs fraud), etc.

In order to effectively counter this form of crime, it is necessary to act promptly to its causes. In this regard, countries should respect the agreed minimum level of excise tax on the trade of these goods. Otherwise there is a significant difference in price compared to other countries in the region, which affects the increase in trafficking, thereby negatively affecting the planned revenues in their budgets. Also, it is necessary to know the organizational structure, the channels and routes of smuggling, and the methods of storage and distribution of contraband. Effective border control and state border security are important aspects in the fight against all forms of cross-border crime including trafficking in excise goods. Well-organized protection of state borders, carried out by border security authorities, border police and customs, in cooperation with other relevant bodies responsible for the internal security of the country, can be an effective "filter" in preventing the illicit cross-border activities of mostly organized criminal groups in connection with the illegal crossing of the state border and the activities in the border area. The common, intensive control of passengers and goods (and accompanying documentation) required for crossing the border contribute to this process, and the use of modern technical means, as well as the implementation of modern evidentiary actions detection (surveillance and recording of telephone and other communications, simulated legal affairs, controlled delivery, etc.).

Finally, effective counteracting the smuggling of excise goods implies intensive international police and customs cooperation in the Western Balkans region and beyond. In this area, the border police and the customs of our country have made good bilateral and multilateral cooperation with the entities of border security in the Western Balkans, which is manifested through the exchange of information on offenders, taking actions for the benefit of another country, joint actions with the police and customs authorities in other countries and mutual technical assistance.

REFERENCES

1. Carinski zakon, Službeni glasnik RS, br. 18/2010, 111/2012 i 29/2015
2. Fabris, N, Pejović,I, Ekonomska politika teorija i praksa, Beograd, 2013., p. 139.
3. Hitris, T. Ekonomika Evropske unije, Institut za ekonomiku i finansije, 2003., p. 8.
4. INTERPOL, Legal Handbook Series Tobaco En
5. Krivični zakonik, Službeni glasnik RS, br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013 i 108/2014

6. Kulić, D: Krijumčarenje preko državne granice – metodika otkrivanja istraga, Bezbjednost, policija, gradjani br. 2, Banja Luka 2006., p. 779.
7. Milošević, G, Javne i monetarne finansije, KPA 2010, p. 252.
8. Milošević, G. Teorija i praksa finansijskog prava, , KPA 2011., p. 257.
9. Milošević, M. i dr.: Organizovani kriminal i terorizam-osvrt na pojavne oblike u Republici Srbiji, Zbornik radova sa naučnog skupa o organizovanom kriminalu – stanje i mere zaštite, Beograd, 2005., pp. 43-47.
10. Milošević, M.; Dostić, S: Modaliteti medjunarodne saradnje graničnih službi zapadnog Balkana, Zbornik radova sa medjunarodnog naučno-stručnog skupa sa medjunarodnim učešćem "Suzbijanje kriminala u okviru medjunarodne policijske saradnje," KPA i Hans Zajdel fondacija, Tara, 2011., pp. 52-54.
11. Pejovic, I. Osnovi ekonomije, Visoka škola za ekonomiju i upravu, Beograd 2013., p. 268.
12. Pejović, I. Spoljno trgovinsko poslovanje, Visoka škola za ekonomiju i upravu, Beograd, 2014., p.158.
13. Procena opasnosti od teškog i organizovanog kriminala u Srbiji, MUP Republike Srbije, Beograd, December 2015, p. 87, 90,91.
14. Procjena opasnosti od teškog i organizovanog kriminala u Crnoj Gori, MUP Crne Gore, Uprava policije, Podgorica, February 2014, p. 63.
15. Zakon o akcizama, "Sl. glasnik RS", br. 22/01...55/15
16. Kresoja, M.:Kriminalistika za osnovno policijsko obrazovanje, Yugo-Pirs, Novi Sad, 2006., p. 488.

INTERNET SOURCES

17. http://www.mfa.gov.rs/sr/index.php/spoljna-politika/eu/regionalna-saradnja/selec?lang=latpreuzetodana 9.02.2016.
18. http://www.upravacarina.rs/lat/medjunarodnasaradnja/Stranice/ClanstvoUMedjunarodnimOrganizacijama.aspxpreuzetodana 9.02.2016.

UDC: 343.97
314.15(4)

LOST LIVES ALONG BORDER LINES: MOBILITY, CRIMMIGRATION LAW AND PUNISHMENT

Angelina Stanojoska, PhD[1]
University "St. Kliment Ohridski", Faculty of Law, Bitola

Abstract: Migration following the globalization process was an inevitable product in such environment and conditions. It does not mean that it didn't exist before, but after being globalized it got a "modern" shape wrapped under the shadow of continents – fortresses. Unfortunately, today more than ever individual characteristics, such as the sense of belonging, are defined by borders and sense of security is connected to those borders and their closeness. In time of the biggest migration flow to the European Union, migrants are seen as danger, they are excluded, their religion without any doubt is connected to destruction and terrorist attacks. Illegality of migration is the result of other similar forms of criminalization of acts in international area, under protection of key state players, who have the power to make a transition of a phenomenon from "normal" to a "deviant" one.

This process and those of creating crimmigrants and immcarceration are just a small part of a question *Are we moving to a criminology of mobility?*

Keywords: crimmigrants, migration, mobility, prohibition, punishment.

INTRODUCTION: MIGRATION AS A "DNA SEQUENCE"

The term migration originates from the Latin *migrare* which means moving people from one place to another. Today it means even more than movement of people, because it also describes moving data between computer systems, movement of microorganisms between people, animals and plants, and, of course, the movement of animals. It is an essential process regarding many life aspects, and also a process which includes organization, change and adjustment.[2] Migration is a part of every human being's free will, which as a result of the poor development of his/her country of origin will choose to emigrate.[3] People are in constant movement over international borders, crossing them illegally, without documents, because of different reasons. Some of them are under the pressure of political violence, others are moving because of an ethnical conflict, natural disasters, poor economic conditions, looking for better opportunities in another country. In such way, they become illegal migrants.

Migration's history starts somewhere at the beginning of human civilization, in Africa, between 1.5 million ago and year 5000 BC, when Homo erectus and Homo sapiens migrated to Europe and then to the other continents.

Greek colonization and Roman expansion were directly connected to migration processes, during which others were also happening outside of Europe, in Mesopotamia, and in the Empires of Incas and Hindu nations.

---

1 E-mail: angiest22@gmail.com.
2 Thanh-Dam Truong. Des Gasper. *Transnational Migration and Human Security: The Migration–Development–Security Nexus.* (London-New York: Springer, 2011). p .4.
3 Елизабета Рози, "Кон усогласување на одредбите за трговија со луѓе и крумчарење мигранти: Борба против трговијата со луѓе, стратегии и соработка во истрагата", *Twinning project: Fight against Organized Crime and Corruption Unit – Public Prosecutor's Office, Collection of texts (2009):* 375.

Going back to the transatlantic movement of slaves and their forced migration to the European continent, it is inevitable to mention the second trip of Columbus over the Atlantic Ocean after which he brought back to Spain hundreds of Taino Indians. During the year 1443, Spanish crusades destroyed and enslaved thousands of natives. Those who were brought to Europe started dying under the strike of many European diseases. That's why King Carlos of Spain gave his royal approval for the start of the movement of slaves from Africa. At the end it became a 350-years long and painful trip for African people.

Voluntary migration was in its peak in the period of Europe's expanding, especially when some of colonial forces, such as Great Britain, the Netherlands, Spain and France, promoted migration to their colonies. Everyone was permitted to move, from workers, to beggars, retired soldiers, prisoners, orphans.

The next important period of migration is the one to the USA, in the period between 1850 and 1930. Because of the America's expansion as an industrial force and developed country, it became a destination for many potential migrants.

An inevitable mention are the migration flows during the First and Second World War when millions of European civilians were uprooted and moved. By some estimates, a total number of around 60 million Europeans were displaced and migrated during the entire World War II. Between the end of the War and 1951, a million of people had yet to find a place to settle.

Also, another important wave of migrations is the one after the end of the World War II, when workers were needed in processes of development of post-war economies in Europe, North America and Australia. This is a period when many Turks moved to Germany and many Africans from North Africa to France and Belgium.

The last known and current flow started somewhere in 2010, with the first dawn of the so-called Arab Spring, and worsened with the Libyan Civil War. But what became even worse was the movement of people after the start of the Syrian Civil War and the situation in Afghanistan and Iraq.

Macedonia has rarely been perceived as a destination to immigrants, knowing its political, economic and social background. Mostly migrants or, better said, refugees (in the core meaning of migration they are migrants, but of course with a special status) used its territory as a shelter from bombs and death. Maybe the best example is the movement of Kosovo citizens during the war on their land. In late March 1999 Kosovo citizens started fleeing towards Macedonia, after the start of the NATO's air strikes campaign against Serbia. In a period of 9 weeks, 344 500[4] refugees entered Macedonia. The international community lacked action and support for this small Balkan country, leaving it all alone with a high influx of costs and burden to its weak budget. Most of that number of individuals repatriated in 2000, after the end of Kosovo War, but according to the UNHCR data, 21 000 stayed and after the following year the number has dropped to 9050.[5]

On the other hand, Macedonia's emigrational processes have always been everyday life on its territories – under the lashes of the World War II, the search for employment, opposition of Yugoslav communism, the devastating 1963 earthquake in Skopje (the Macedonian capital). Today, Macedonian immigrants are part of communities in Toronto, Canada; Wollongong, Sydney and Melbourne, Australia; Locarno, Switzerland; and other Western European countries.

The paper will try to make an overview of the most important criminological theories regarding migration and its involvement in the criminal processes. Also, it's aiming towards analysing crimes of mobility, the process of criminalizing immigrants and building a crimmigrant's model.

4 Donev. D. S. Onceva. I. Gligorov. "Refugee Crisis in Macedonia during the Kosovo conflict in 1999" *Croat Med J 43(2):* 184–189.

5 Although other data show higher number of Kosovo refugees who claimed Macedonian citizenship.

CRIMINOLOGICAL (THEORETICAL) PERSPECTIVES: ARE WE MOVING TOWARDS A LOMBROSO'S "BORN" IMMIGRANT?

Analyzing something from a criminological point of view inevitably entails the mentioning of the father of Criminology, Cesare Lombroso. Although his work is not accepted today and has been proven to be wrong for most of his conclusions, his work gave to all of us criminologists the possibility to analyse, find new non-researched areas, ask questions and try to find the answers to them.

Working on his *homo criminalis* theory, Lombroso, in his fifth edition of *L'uomo Delinquente* wrote: "Recent statistics for the United States, document high rates of crime in states which large numbers of immigrants, especially from Italy and Ireland. Out of 49 000 arrests in New York, 32 000 were immigrants. Immigrants belong to the human category with the greatest incentives and fewest barriers to committing crime. Compared to the resident population, newcomers have greater economic need, better developed jargon, and less shame; submitted to less surveillance, they more easily escape arrest. Thieves are almost always nomads."[67] Even long before Lombroso's research, people, especially Greeks during the existence of their cities *poleis*, used the word "barbarians" for those coming from the other side, meaning from other land, beyond borders. People, who are not speaking their language, cannot speak at all, they are just "barking".[8]

Migrants or in other words strangers have always been the unknown area for natives, having that meaning of different, change and danger for already established way of life. It's like migrants never try to adjust themselves to cultural norms and everyday life in their country of destination, it's like all they want is to destroy and survive by committing crimes.

Using Lombroso's research regarding physical characteristics and criminality, Earnest Hooton published his *The American Criminal: An Anthropological Study* and *Crime and the Man*. In his first published work he analysed the "white" criminal from USA, whose parents or one of them is immigrant and the "black" criminal. His conclusions were brought after a study of more than 17 000 people from which 14 000 were prisoners. His attempt was to prove and renew the theory of *homo criminalis.* His conclusions say that criminals have characteristics which make them different then non-criminals. Of course in those lists, as a result of Hooton's researches, being an immigrant is a characteristic which makes people destined to commit crime.

Years after the first explanations of criminal behaviour done by Lombroso and other phrenologists, the criminologists and sociologists who were part of the known Chicago School

6 Lombroso, Cesare. *Criminal Man (translated by Mary Gibson and Nicole Hahn Rafter).* (Duke University Press: Durham and London, 2006), p. 317.

7 Studies of emigration resolve a contradiction apparent in Italy and France: that certain crimes do not increase with rising birth-rates. For example, thefts, which increase with greater population density, should increase with higher natality. Yet in France, where rapes and murders do increase in relation to density, thefts are inversely proportional to the birth-rate. However theft does not decrease with falling birth-rates if immigration provides a countervailing force to swell the overall population. The opposite is true in Italy, which has an emigration rate of 193 per 100 000 inhabitants. Regions known for crime and poverty almost always have the highest birth-rates. Between 1876 and 1888, the birth-rate for southern Italy was 40 per 1 000 compared to 36 per 1 000 for the rest of the peninsula. Yet as Del Vecchio has noted, higher mortality rates and emigration have prevented high population density in the south. For example, average family size is 4.10 persons in Sicily and 4.5 persons in the southern province of Basilicata, in contrast to 5.17 in the Veneto and 4.92 in Tuscany, both Northern provinces. (Lombroso C. *Criminal Man*).

8 As mentioned in Dario Melossi's *Crime, Punishment and Migration.* (SAGE: London, 2015).

will try to explain the connection between crime and migration, using cultural norms and the existing conflicts between different cultures, especially in moments when those two clash on the border lines between countries or nationalities.

In the United States, after the initial nativist moral panic about immigration, the Chicago School of sociology eventually produced a more balanced and "normalized" view of the relationship between migration processes and deviance according to which criminal behaviour was connected to societal disorganization. This was not specific to immigrant groups but had to do with the very processes of migration, assimilation and integration into American society. The Chicago School authors were also quick to point out that generally "first generation" migrants tended to reproduce the criminal habits of the society of origin, whereas second generations were slowly assuming the levels and types of criminality typical of the environment in which they found themselves. In fact, public concern began to shift towards the issue of the integration of successive generations of immigrants, and their possible contribution to the phenomena of deviance and crime.[9]

The first explanations which are part of the above mentioned Chicago School are the ones of Torsten Sellin. Being an American with a Scandinavian origin, Sellin tried to explain criminal activities using cultural conflicts.

Conduct norms are cultural rules that require certain types of people to act in certain ways in certain circumstances.[10] What is eventually happening within a society with such norms? In a society with a homogeneous structure all those rules are brought with a consensus of all participants in existent community, so they are respected, people mostly never do anything to try to change them or to not obey the way of life they promote. But, problems emerge on the surface in societies where beside natives, there are other communities, other cultures, which promote different rules, relations and everyday life. Such societies are known by the primary cultural norms which are happening. Those conflicts are occurring between two different cultural backgrounds. Such conflicts territorially could occur in border areas where two different cultures overlap, then on colonized territories, in cases when laws of one of the cultures are expanded over the territory of another culture, and of course, what for us is the area of interest, in cases of migration, when the cultural norms which were brought by immigrants now interact and significantly differ from the ones existing from before. And that is the moment when criminal activities occur, in the culmination of those cultural conflicts. On the other hand, Sellin also speaks about secondary cultural conflict, defining it as a conflict within one culture. Namely, it is happening in times when a culture divides itself in several subcultures and each of those parts has its own conduct norms. Having their own conduct norms, cultural behaviour ends with possibilities for future conflicts. In such an environment there is also an existence of inability to interact. In times when a society becomes more complex because of the processes of differentiation, the potential for conflict increases. The necessity of adjustment to heterogeneous frameworks also increases the possibilities for a conflict, and of course produces higher criminal rates in a society.

Sellin in his work recognizes that the criminal law also reflects values of the dominant interest group or dominant culture, and at the same time the values of the other social groups are very different. This is mostly in cases of ethnical minorities and immigrants. And when your values are different than those of the native ones, even if you try, the moment you'll make a mistake you'll be labelled as deviant.

9 Melossi, Dario. "The Borders of the European Union and the processes of criminalization of migrants" *The Routledge Handbook of European Criminology.* (2013): 501–502.
10 Thomas J. Bernard. Jeffrey B. Snipes. Alexander L. Gerould. *Vold's Theoretical Criminology.* (Oxford University Press: New York, 2010), p. 247.

The Labelling theory at first is connected to the name of Frank Tannenbaum, who in 1938 published his work *Crime and the Community* where he explains that deviant behaviour is not a result of deficiency of adjustment on cultural rules (in this case of immigrants). Crime is a consequence of the collision between community and a certain group. When a person is caught *in flagranti* he is labelled as deviant.[11] Howard Becker's opinion is that deviance is different in the eyes of different groups. For some to be labelled as deviant, the deviant behaviour must be noticed and afterwards not accepted by the group which ends with labelling someone as deviant.

In 1951, Edwin Lemert published his *Social pathology*, where he draws a line between primary and secondary deviation. It is a process in which a criminal offender at the beginning does not accept an identity as deviant, but after a time in which he continues with his criminal behaviour (although knowing it is not acceptable) starts the secondary deviation, as an identity mostly given to immigrants in times of migration flows.

Having it connected to migration and its connection to crime, sociologists used communities' inability for accepting changes and of course the conclusion regarding legal norms in a society. Every legal norm is never a reflection of a consensus in a community, but the opposite. It is just a mirror's reflection of the dominant culture, which will fulfil what it takes to suppress every other cultural norm and try to assimilate all of them.

The "culture of poverty" thesis where low income people adapt to their structural conditions in ways that perpetuate their disadvantaged condition is an example of a cultural explanation. Thus, engaging in crime as a means of acquiring social status draws children away from schoolwork, which reduces the probability of future economic development. A variant of this explanation for crime, the "subculture of violence" thesis, suggests that violence can become a "normal" and expected means of dispute resolution in economically disadvantaged areas.[12] Such areas are always associated with immigrants living in them, and because they are residing in such areas conflict theories are used to explain the deep connection between immigration and crime.

As already mentioned, cultural conflicts in accordance to immigration are a result of diverse cultural background. Some authors conclude that cultural traditions do not influence over crime rates in diverse minority and migrant neighbourhoods (especially violent crime rates), but the ones which influence are structural conditions of society. On the other hand, there are authors, among which Sutherland and Sellin, who argued that immigrant had predispositions toward certain types of crimes. Those predispositions have a cultural nature.

Also, using Sutherland's differential association theory, Quinney argued that different segments of society have different normative systems and different patterns of behaviours, all of which are learned in their own social and cultural settings. The probability that individuals will violate the criminal law depends, to a large extent, on how much power and influence their segments have in enacting and enforcing the criminal laws. In more powerful segments of society, people are able to act according to their normative standards and behavioural patterns without violating the law. But when people in less powerful segments do the same thing, their actions are legally defined and officially processed as criminal.[13] Actually, when a migrant comes to a country, he/she never becomes a part of the powerful segments of society, which in most cases pushes him/her on the edge of criminal activity.

Sutherland, himself offered an explanation stating that in times of conflict of cultures, when the cultural patterns collide there are even more cases of unpredictable behaviour by individuals. Being explained in this way, immigration crime must happen at the end, especially when all other factors are equal. Always, immigrants have higher criminal rates than natives.

11 Williams III, Frank P. Marilyn D. McShane. *Criminological theory.* (Pearson: New Jersey, 2010). p. 111.
12 Martinez Jr. Ramiro. Matthew T. Lee. "On Immigration and Crime" *Crime and Justice. Vol 1(2000):* 490.
13 Thomas J. Bernard. Jeffrey B. Snipes. Alexander L. Gerould. *Vold's Theoretical Criminology.* (Oxford University Press: New York, 2010), p. 250.

On the other hand, the explanations using the term of social disorganization, seen as *a decrease of the influence of existing social rules of behaviour upon individual members of the group.* In an organized society, there is congruence between group rules and individual attitudes. Disorganization implied a gap between rules and attitudes, such that an individual did not feel bound by the rules and was free to disobey them (for example, engage in crime). Disorganization was a neutral and individual liberation from oppressive community standards, although it has the recognition that crime not only is a function of economic (poverty) or cultural (subculture of violence) forces, but is intimately tied to the fundamental processes of social change.[14]

Also, the social disintegration theory is mostly associated with the work of Shaw and McKay on the ecological distribution of delinquency. They were using quantitative data from Chicago's neighbourhoods to specify the role of community disorganization in producing high crime rates.

Their findings were explained by reference to a theory of urban ecology which viewed the city as analogous to the natural ecological communities of plants and animals. The residential, commercial and industrial pattern of urban settlement was described as developing an ecological pattern of concentric zones that spread from the centre towards the outermost edge of the city. Directly adjacent to the city's commercial and business core of the city was a "zone in transition", which was changing from residential to commercial. It was in this area that the highest rates of delinquency were found.[15]

This transition zone was characterized by physical decay, poor housing, incomplete and broken families, high rates of illegitimate births, and an unstable, heterogeneous population. The residents were at the bottom end of the socio-economic scale with low income, education and occupations. In addition to high rates of delinquency, this area had high official rates of adult crime, drug addiction, alcoholism, prostitution and mental illness. All these forms of deviance and lawlessness were interpreted as the outcome of the social disorganization within this urban area. The Chicago sociologists emphasized that residents in this area were not biologically and psychologically abnormal. Rather, their crime and deviance were simply the normal responses of normal people to abnormal social conditions. Under these conditions, criminal and delinquent transitions developed and were culturally transmitted from one generation to the next. Industrialization, urbanization and other social changes in modern society were seen by the Chicago sociologists as causing social disorganization by undermining the social control of traditional social order and values.[16] Their most important conclusion regarding their theory is that in social areas which are from the same type, the foreign born and the natives, recent immigrant nationalities and older immigrants produce very similar rates of delinquency.

Being associated with immigration, the ecological theory might explain the lack of application of conduct norms in places, neighbourhoods and areas where immigrants live. Namely, even in times of urbanization and internal migration when people moved from rural to urban areas, they were always pushed to the margins of communities or not even socially included which, of course, could result in those people's criminal activities. Using ecology's theory findings, we might conclude that immigrants (mostly first generations) are always found moving on edges of society, not being able to include themselves in everyday routine, not being able to start a new life with a job and a proper place to live. In such conditions people always move towards other exits, among which crime is the most profitable, but also the most dangerous.

14 Martinez Jr. Ramiro. Matthew T. Lee. "On Immigration and Crime" *Crime and Justice. Vol 1(2000):* 492.
15 Akers. Ronald L. *Criminological Theories: Introduction and Evaluation.* (Roxbury Publishing Company: Los Angeles, 1997), p. 116.
16 Akers. Ronald L. *Criminological Theories: Introduction and Evaluation.* (Roxbury Publishing Company: Los Angeles, 1997), p. 116.

Close to such conclusions are Zimbardo's experiments inside the Broken Windows theory. In his experiment he arranged a car without plates to be parked in Bronx neighbourhood and one comparable car in Palo Alto, California. Of course, the first one was destroyed in hours of time, but the other was left untouched for a week. After that, Zimbardo smashed a window, after which a passer-by started to vandalize the car. Signs of destruction and disorder are starting points of criminal actions. "Broken windows" situations are more common for poor, non-developed neighbourhoods, such as those where immigrants live.

Another theoretical explanation of the connection between immigration and crime can be made using Merton's strain theory which explains such situations using anomie situation in societies. But, unlike Durkheim's definition of anomie as a situation in society in which there is lack of norms that will secure control over natural and unlimited individual's needs and aspirations, Merton uses the misbalance between legitimate means and culturally prescribed goals.

Namely, disadvantaged groups in which often immigrants are included, may be denied legitimate means to attain culturally prescribed goals, let's say a job so they can live a mid-class lifestyle. There is a tendency in the world for immigrants to settle in urban neighbourhoods which are characterized with poverty, poor schools, substandard housing, and high crime rates. Living in such conditions and being segregated may turn them to crime as a means to overcome blocked economic opportunities. Becoming Merton's innovators, they can be simply "contaminated" by the neighbourhood they live in, and possible criminal opportunities.

By analysing the above mentioned theoretical explanations of possible connections between immigration and criminal activities, one can conclude that moving through years and starting with biological and anthropological explanations regarding physical characteristics of migrants, authors have built (intentionally or not) a model of the so-called "born" immigrant (criminal). In every different migration flow, regardless of the reasons of movement, immigrants get their gender, age, ethnical background, religious beliefs, level of danger, and change in lifestyle.

CONCLUSION: IMMIGRANTS IN CRIMINAL WORLD: VICTIMS OR OFFENDERS (MACEDONIAN CASE)

Globalization as process was an inevitable "movement" of society's framework and something that was always waiting at the end of the tunnel called urbanization, industrialization, opening borders and technological progress. And it is then when the story of the new world has started. Borders were opened, but continent's fortresses were born. Building "walls" has culminated in panic, xenophobia, and fear from newly comers, those who will change it all.

Macedonia was rarely seen as a destination to immigrants, but was mostly used as a path towards their hope. Immigrants, even now in a present migration crisis in Europe, use Macedonia only as a station in the long journey to the European Union.

With the start of everyday movement of huge groups of migrants, Macedonian soil got new sources for criminal activity. The smuggling of migrants have increased, but also crimes whose victims were immigrants. The State Statistical Office does not publish statistics connected with citizenship of offenders, but only with their ethnical background. Because of such situation, some of the Ministry of Internal Affairs' statistics regarding smuggling of migrants were used, as well as those of the Helsinki Committee of Human Rights (cases which are also confirmed by the Macedonian Police). [17]

17 In 2007, 85 Macedonian citizens have been reported, 2 were Swedish and Albanian, and 1 Moldavian and Turkish citizens. They were smuggling migrants to the Macedonian-Greek border. The 2 Swedish

In the Republic of Macedonia, immigrants in the period 2015–January 2016, in most cases have been victims of violent attacks or robberies. Offenders either directly attack victims or offer them a lift to the Serbian border (for money = smuggling of migrants) and never take migrants to their destination (leave them on unknown territory and robe them).

In the last two months, the so-called "economic" migrants have been mostly victims of attacks, because they cannot move to the EU, as those coming from war zones can (because of their status as refuges).[18]

In comparison to Macedonia, the EU situation where immigrants settle and try to start a new life, as has been already mentioned above, the criminal rate and their participation rate are high in some types of crime.

By analysing the above mentioned theoretical explanations of possible connections between immigration and criminal activities, one can conclude that moving through years and starting with biological and anthropological explanations regarding physical characteristics of migrants, authors have built (intentionally or not) a model of the so-called "born" immigrant (criminal). In every different migration flow, regardless of the reasons of movement, immigrants get their gender, age, ethnical background, religious beliefs, level of danger, and change in lifestyle.

Immigration can be and is in connection to crime in some cases, but should never be analysed individually, as the only, solely factor of criminal behaviour. Even now, in the XXI Century, states and political elites are building models of immigrants from whom they should protect their states in order to successfully fulfil their political agendas.

REFERENCES

1. Akers. Ronald L. *Criminological Theories: Introduction and Evaluation.* Roxbury Publishing Company: Los Angeles, 1997.
2. Bhattacharyya, Gargi. *Traffic: The illicit movement of People and Things.* London: Pluto Press, 2005.
3. Calderoni, Francesco. *Organized Crime Legislation in the European Union: Harmonization and Approximation of Criminal Law, National Legislations and the EU Framework Decision on the Fight against Organized Crime.* Dordrecht: Springer, 2010.

smugglers were smuggling migrants from Kosovo to Greece through the territory of Macedonia. In 2008 smugglers organized smuggling of 173 migrants from Serbia (the region of Kumanovo) and Albania (Ohrid Lake or Struga region), to EU destinations (Greece or other European countries). Migrants for those services had to pay from 600 to 1500 euros. In 2009 through the KANIS action of the SECI Center, a smuggling group was reported. 12 Macedonian citizens (1 police officer) and 1 Serbian citizen for a longer period have smuggled migrants from China, through Serbia, Macedonia and Greece to the Western European countries. Also, in December 2009, Afghanistan migrants were found in a special compartment of a truck on the border crossing Bogorodica. Those migrants were taken from the Greek port of Patra. In 2010, organized crime groups were transporting migrants from Greek and Albanian border to the Western EU countries. Also, in this year for the first time migrants were originating from countries affected by the Arab Spring. Also, in 2011 and 2012, Macedonia is still a transit country for illegal migrants coming from countries of the Middle East and North Africa. 2013 and 2014 are years when migrants are originating mostly from Syria, and in many cases, especially in 2014, migrants were victims of railway accidents (in cases when they were not using the services of smugglers).

18 On 6 January 2016, two Moroccans arrived in the camp. According to their statements, they had been abused, beaten and robbed in the Demir-Kapija region. They had their money and mobile phones stolen. The case was reported, and the police took their statements in the camp. On the same day, three Moroccan citizens were attacked by a group of armed thugs who robbed them of 900 EUR. Only one day later, two citizens of Morocco were also attacked by unknown perpetrators in the vicinity of Skopje, who used a baseball bat and electro shocks to torture them and steal their money and mobile phones. Two days later, the same people were attacked in the vicinity of Kumanovo, by the two people who were transporting them by car.

4. Dauvergne, Catherine. *Making people illegal: What globalization means for Migration and Law.* Cambridge: Cambridge University Press, 2008.

5. Donev. D. S. Onceva. I. Gligorov. "Refugee Crisis in Macedonia during the Kosovo conflict in 1999" *Croat Med J 43(2):* 184–189.

6. Fijnaut, Cyrille, and Letizia Paoli. *Organized Crime in Europe: Concepts, Patterns and Control Policies in the European Union and Beyond.* Dordrecht: Springer, 2004.

7. Kelly, Robert J., Jess Maghan and Joseph D. Serio. *Illicit Trafficking.* Santa Barbara: ABC-CLIO, 2005.

8. Koser, Khalid. *International Migration: A Very Short Introduction.* New York: Oxford University Press Inc., 2007.

9. Lombroso, Cesare. *Criminal Man (translated by Mary Gibson and Nicole Hahn Rafter).* Duke University Press: Durham and London, 2006.

10. Martinez Jr. Ramiro. Matthew T. Lee. "On Immigration and Crime" *Crime and Justice. Vol 1(2000).*

11. Melossi, Dario. *Crime, Punishment and Migration.* SAGE: London, 2015.

12. Melossi, Dario. "The Borders of the European Union and the processes of criminalization of migrants" *The Routledge Handbook of European Criminology.* (2013).

13. Thomas J. Bernard. Jeffrey B. Snipes. Alexander L. Gerould. *Vold's Theoretical Criminology.* Oxford University Press: New York, 2010.

14. Williams III, Frank P. Marilyn D. McShane. *Criminological theory.* Pearson: New Jersey, 2010.

UDC: 343.851:[343.9.024:336.7

MODEL SYSTEM OPERATION IN THE FIELD OF PREVENTION OF MONEY LAUNDERING

Miroslav Radojičić, PhD
Óbuda University, Budapest
Jovanka Vukmirović, PhD
University of Belgrade, Faculty of Organizational Sciences
Aleksandra Vukmirović
Belgrade Business School College of Professional Studies
Stefan Radojičić
University of Szeged
Dragan Vukmirović, PhD
University of Belgrade, Faculty of Organizational Sciences

Abstract: Models of financial scam are part of a complex system of organized crime, which is growing more and more, so you constantly find and apply new techniques in line with the development of science and technology. Therefore, for a successful fight against financial crime, particularly money laundering and terrorist financing, an important role is preventive measures, especially those concerning the analysis and risk assessment. The system based on rules (rule-based system) was in effect from the adoption of the First Directive on the prevention of money laundering in 1991. The third directive of 2005 introduces a system based on risk analysis (risk-based system), the observance of which is contained in the FATF recommendations in 2012.

The paper is a model system for preventive action in cases of financial fraud. The assumption is that only a comprehensive, systemic solution, based on clear methodological assumptions can be effective to prevent the emergence of financial fraud. For the purpose of defining the model, based on the theoretical and practical research and analysis of case studies, the basic components and related processes are recorded in the model. The model is presented in two level indicators, including the local (state) and international dimension, which is fully in line with international recommendations and directives in the field of combating money laundering and financing of terrorism, which have undisputed international aspect.

Key words: financial fraud, money laundering, model, system, prevention.

INTRODUCTION

Pascal Fontan in its publication Europe in 12 lessons stated that European citizens have the right to live in freedom, without fear of persecution or violence, anywhere in the European Union. [1]In doing so, he emphasizes that international crime and terrorism are among the issues that today are most concerned about Europeans. It is alleged that organized crime is becoming increasingly sophisticated and regularly for their activities benefit both European and international networks.

1 Fontaine, P. (2010). Europe in 12 lessons. Publications Office of the European Union, Luxembourg, p. 80.

Financial frauds are part of a complex system of organized crime, and therefore are subject of the development trough constant inventions and application of the new methods that are in accordance with the development of science and technology. This forced the state, international institutions and organizations to improve their strategies and the establishment of new mechanisms and instruments to combat financial fraud. To effectively combat financial crime, particularly money laundering and terrorist financing, an important role is preventive measures.

This paper presents a model system for preventive action in cases of financial abuse, which is based on the most recent Directive on the prevention of money laundering from 2015[2], which stresses the importance of a coordinated operation by the supervisory authorities at both EU and national level. The assumption is that only a comprehensive, systemic solution, based on clear methodological assumptions can be effective to prevent the emergence of financial fraud.

LEGAL AND INSTITUTIONAL FRAMEWORK FOR THE FUNCTIONING OF THE MODEL

The legal basis for the operation of the model is viewed in two levels, internationally and nationally. The basic step that each country should take in order to build a sustainable system against financial abuse and fraud is harmonization of national legislation with all relevant international standards. In the field of international regulations which regulate the prevention of money laundering and terrorist financing, the model complies with the conventions, recommendations and directives relate to financial institutions. In addition to the Convention, the most important document that sets standards in this area is, 40 + 9 "recommendations of the FATF - Working Group for the Prevention of Money Laundering[3].

Directives issued at the EU level for the prevention of financial abuse are binding all Member States and candidate countries and they have been standardized national legislation against money laundering and terrorist financing. In the directives, among other things, the importance of a coordinated operation by the supervisory authorities at both EU and national level is emphasized, and it is stated that money laundering and terrorist financing often takes place at the transnational level. The latest is the fourth directive of 2015 - *Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.*[4]

At the national level, the umbrella law in this area is the Law on the prevention of money laundering and terrorist financing (hereinafter the Act). The law specifically regulates the institutional framework that determines the relevant institutions responsible for the prevention, organization and fight against all kinds of financial abuse, particularly money laundering, whose activities are based on the above-mentioned legal framework.

The goal of the legal measure is to intensify actions that will act preventively in order to combat the most common crimes fraud, such as money laundering. To achieve this goal cooperation of all relevant institutions is required, as well as improving the international legal instruments that will lead to better coordination and international cooperation, because the problem of organized crime has long transcended national boundaries.

2 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
3 http://www.fatf-gafi.org/
4 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

On the other hand, activities aimed at local operators, in order to increase the efficiency of internal control, to achieve credibility of the financial reporting of companies and the establishment of effective external controls aimed at closing the channels for the outflow of funds, money laundering and preventing direct financial crime but also one that relies on the latest technology they decorated the legal system of each country.

The international legal framework for the establishment and functioning of the Directive 2005/60 / EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on prevention of the use of the financial system for money laundering and terrorist financing[5]. In accordance with this Directive, each Member State is obliged to establish a special financial intelligence in order to effectively fight against money laundering and terrorist financing.

The main national legal framework for the establishment and functioning of the Board are the Law on the Prevention of Money Laundering and Financing of Terrorism[6] from 2014 or terrorist financing also from 2014[7]. The institutional framework to combat financial abuse in the Republic of Serbia is defined in the National Strategy for Combating Money Laundering and Financing of Terrorism, in which are listed the basic institutions involved in the above activities (Figure 1)[8]. The central among these institutions takes the Directorate for the Prevention of Money Laundering (Management) in the Ministry of Finance of the Republic of Serbia. The management is a financial - intelligence service of the Republic of Serbia - FOS (Eng. Financial Intelligence Unit - FIU) and established according to international standards that collects, analyzes and stores data and information, and when it determines that there is a suspicion of money laundering, the relevant government authorities are informed (police, justice and inspection authorities) to take measures within their jurisdiction.

Figure 1: *Graphic representation of the system for combating money laundering and terrorist financing in the Republic of Serbia*[9]

5 DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing), Official Journal of the European Union L 309/15.
6 Official Gazette of the Republic of Serbia, no. 20/09, 72/09, 91/10 and 139/14.
7 Official Gazette of the Republic of Serbia, no. 55/05, 71/05 - correction, 101/07, 65/08, 16/11, 68/12 - Constitutional Court decision, 72/12, 14/07 - decision and 44/14).
8 The national strategy for combating money laundering and terrorist financing. Official Gazette of the Republic of Serbia, no. 55/05, 71/05-correction, 101/07, 65/08, 16/11, 68/12-US, 72/12, 7/14 and 44/14-US.
9 The national strategy for combating money laundering and terrorist financing. Official Gazette of the Republic of Serbia, no. 55/05, 71/05-correction, 101/07, 65/08, 16/11, 68/12-US, 72/12, 7/14 and 44/14-US.

The establishment of the Directorate for Prevention of Money Laundering as an administrative body within the Ministry of Finance of the Republic of Serbia has clearly expressed their interest to work together with the international community in order to become an active participant in the international system to prevent financial fraud, especially money laundering and terrorist financing.

MODEL OF PREVENTIVE ACTION IN MONEY LAUNDERING

The primary goal of the Model System of preventive action with money laundering is to establish a system solution for the protection against financial abuse based prevention. To achieve this goal, it is necessary to define a unique methodological basis on which one such system is based[10]. Based on the theoretical and practical research and analysis of case studies, they are recorded in the basic components and the corresponding processes in the model.

These components are conveniently placed on two levels: international and local (national) level. Connections between them are the two-way and continuous, given the required dynamic of mutual communication, which must be permanent and continued.

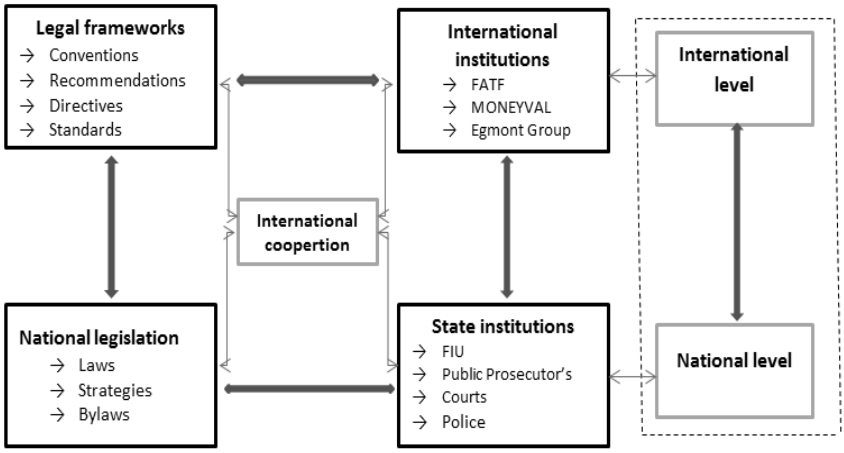


Figure 2: *The main components of the model*[11]

1. International legislation - includes international conventions, recommendations, guidelines and standards related to financial fraud, and are predominantly directed to the issue of money laundering;

2. International institutions - includes all international actors who create legal regulations in the field of financial abuse, as well as international institutions responsible for their prevention and detection;

3**. Legislation** at the level of individual countries - the national legal norms in the field of financial abuse, which should be fully and timely harmonized with the current international regulations; and

10 Radojičić, M. (2015) The interrelations between banking and insurance systems in the prevention of international financial abuse, PhD Thesis, Obuda University, Budapest.
11 Radojičić, M. (2015) The interrelations between banking and insurance systems in the prevention of international financial abuse, PhD Thesis, Obuda University, Budapest.

4. State institutions - all national institutions in charge of preventing money laundering and preventing direct financial crime, led by the competent Administration for Money Laundering Prevention (FIU).

The following must be particularly emphasized: the importance of the dynamic approach, better organization and international cooperation in order to prevent and detect abuses in the financial sector. This means that those components of the system cannot be static, but must be viewed continuously, introducing appropriate processes to raise its efficiency.

Processes are represented by model, and the complete system is shown in Figure 3. These processes are going in a circle and constantly complement the results of the previous process, making the system sustainable in the ongoing struggle with the financial crime, which continually finds and introduces new methods and techniques of financial fraud using the latest technical and te chnological achievements. The recorded processes (13) are:

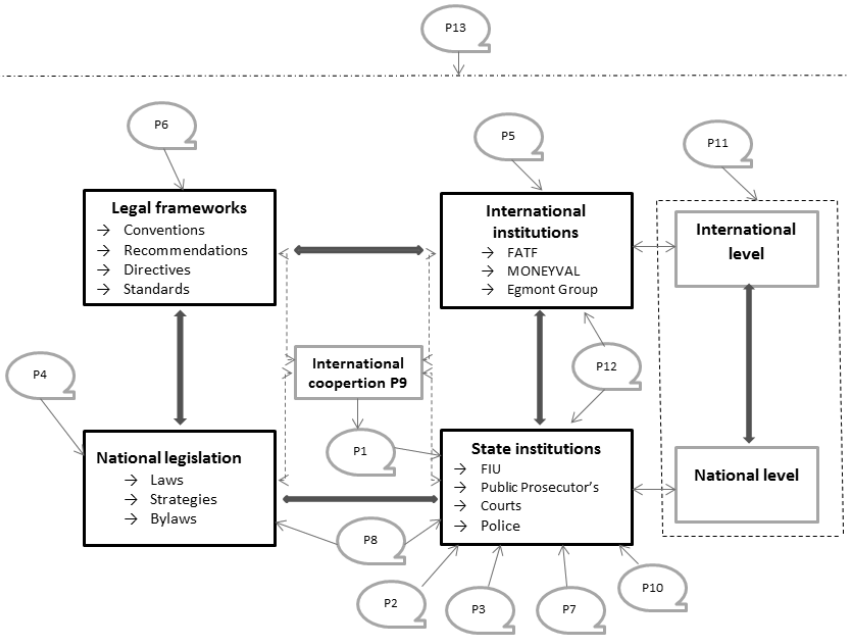


Figure 3: A model system of preventive action in cases of money laundering[12]

P1: Methodology (theoretical) research setting financial abuse

The main fight against financial crime is kept at the level of each country individually. However, it is necessary to achieve the synergy effect through interstate exchange not only data and information, but also knowledge. The States must set focus of their joint efforts on the following: comprehensive, theoretical and practical research methodologies and techniques of financial abuses, reviewing and expanding the indicators of the unfair actions, creating and updating of the fraud typology, identifying all forms of financial crime, completing legislation, amendment of criminal legislation, training of police and investigative methods, harmonization of criminal and judicial policy and other activities, such as staff training and coordination of media campaigns for educating the general population - citizens.

12 Radojičić, M. (2015) The interrelations between banking and insurance systems in the prevention of international financial abuse, PhD Thesis, Obuda University, Budapest.

All these activities also have the legal and economic dimension, given the fact that financial fraud at the same time undermines the legal system of each country and its economic stability.

The basic methodological assumption on which is based system for preventive action in cases of financial abuse is that it is based on risk assessment. Model system of preventive protection for financial abuse unless a risk assessment of exposure to financial abuse includes the classification of risk in the field of existing typologies of fraud, as well as their materialization in the form of suspicious transactions.

FATF knows the next phase in the implementation of a system based on risk assessment. These are (FATF, 2012):

- Detection of risks,
- Risk Assessment
- The development of risk management strategies and
- Minimization of risk.

In addition knows the three risk categories[13]:

- Low risk,
- High risk and
- Innovation (such as, technological innovations).

Methodology which is based on the presented model assumes and incorporates the FATF rules, which provide for mechanisms that are used to analyze the procedures applied and the decision on the level of risk. Risk assessment must be such as to refer to each customer and each product (service). The assessment based on risk is based on an analysis of all relevant facts, and obtained information that may indicate suspicious financial transactions. This is especially true to all complex or unusual parts of transactions that have no apparent economic and lawful visible logic.

The effective use of the system requires: a detailed definition of suspicious transactions, effective supervision and registration of suspicious transactions not only by banks but also other taxpayers, or all those representatives of the financial and non-financial sector, which are obliged to apply the regulations for the prevention of money laundering (banks, insurance companies, auditors ...)[14]. The goal is to get through the implementation of actions and measures prescribed by law, create an unfavorable environment for money laundering in the country. Although not directly listed among taxpayers, lawyers are also required to implement the actions and measures prescribed by the Prevention of Money Laundering and Financing of Terrorism.

P2: Identifying all forms of financial crime in banking and insurance

The process of identifying all forms of financial crime is a logical continuation of the previous process which covers the theoretical concept study of fraud in the financial sector. The main result of this process is a list of all forms (methods and techniques) fraud that occurs in international practice and typology of fraud in the financial sector, as well as a list of appropriate indicators. The typology of financial fraud is particularly important in the banking sector and the insurance sector and a starting base which is continually updated discovering new forms of financial abuse[15].

13 Cindori, S. (2013). Money laundering: correlation between risk assessment and suspicious transactions, Financial Theory and Practice, 37(2), 181–206).
14 http://www.apml.gov.rs/
15 Typologies of money laundering in the Republic of Serbia, the Organization for Security and Cooperation in Serbia, http://www.apml.gov.rs/REPOSITORY/977_tipologije-pranja-novca-u-republici-srbiji-13-09-2011.pdf

P3: implementation and evaluation of the proposed methodology through research of existing methods and techniques of financial abuses

After the establishment of the current typology of fraudulent activities in the previous process, the next step is their research that involves the study of existing methods and techniques of deception, their evaluation and proposal of measures for their detection or suppression, prevention and punishment.[16] In order to achieve this, it is necessary to identify appropriate indicators of fraud, what exactly makes the contents of the next process.

P4: Review and extension of indicators of fraudulent acts

Development of indicators for identifying suspicious transactions is significant to direct effectively, identify and prevent money laundering and terrorist financing, as well as training of staff in banks and other entities that are required to implement measures to prevent such crimes. When the previous process identifies new indicators, they must be tested and classified in the list of existing indicators. Therefore, it is necessary to conduct appropriate legal procedures and organizational support for the implementation of the new list. In Serbia, the project group, consisting of representatives of the Directorate for Prevention of Money Laundering, Tax Administration, National Bank of Serbia and the authorized persons for the prevention of money laundering and terrorist financing with commercial banks, the Post Office and agents for the transfer of money in March 2015 made the list indicators for identifying suspicious transactions related to financing of terrorism, and all taxpayers are required to be included in the list of indicators that compose yourself[17]

P5: Innovation typologies scam

It is necessary to regularly update the typology of frauds and exchange that information with other countries through the FIU units that should establish standardized inter-communication.

In this sense, the institutional networking at the international level is of great importance[18].

P6: Completion of legislation - supplementing the criminal legislation

Amendment typology fraud, the introduction of new indicator, changes international standards, requirements for harmonization of legislation, only some of the activities that require modification of the laws on the level of individual countries. Any changes that are entered in the national legislation, on the other hand, must be in accordance with international legal norms.[19]

P7: Training of police and investigative methods

Police and judicial authorities have an important role in the detection and prosecution of criminal offenses in the area of financial fraud. Therefore, it is necessary to take their knowledge and skills in the field of financial scam continuously complementing and improving. This process is of great importance to international cooperation and good organization and coordination in these services.[20]

16 Cox, D. (2011). An Introduction to Money Laundering Deterrence, John Wiley & Sons, Ltd.
17 Pray, 2001 Project against Money Laundering and Terrorist Financing in Serbia (MOLI Serbia), Preliminary report, CRIS no. 2010 / 252-978 and the Council of Europe no. JP / 2274, 2011 years, http: //www.apml.gov.rs/.
18 Rezaee, Z. & Riley, R. (2010) Financial Statement Fraud - Prevention and detection. John Wiley & Sons, New Jersey.
19 Nikolic, B. Necessary instruments for the efficient seizure of proceeds from organized crime, Guidelines for amending the domestic legislation), Justice in Transition - vol. 9, Belgrade, 2009.
20 Golobinek, R. (2007). Financial investigations and confiscation of proceeds of crime. The manual for the police and judiciary. Council of Europe Office in Belgrade.

P8: Balancing the penal and judicial policies

Repressive side of the system is reflected in the prosecution and punishment of offenders of financial fraud. The penalties for money laundering in all countries of the world are very strict (prison) and often exceed the penalties which are punishable offenses which has gotten the money that is "laundered". In addition to imprisonment, the money or assets which are the subject of a criminal offense must be taken away, as the main reason for the introduction of the crime of money laundering in legal systems preventing criminals to use the revenues gained by illegal means to legitimate uses.

In addition to the repressive hand, the model also predicts proactive, preventive action in the field of spreading awareness about the dangers and consequences of financial abuse and not only in technical, but also the general public. In this educational operation of the special role of the media and related promotional activities designed to represent an independent process that includes all components of the model.[21]

P9: International cooperation

International cooperation pervades all four components of the model and is one of the basic hypotheses underlying the entire system of preventive action in cases of financial abuse.[22]

P10: Continuing education

The importance of training and training of all involved in the chain of combating financial fraud and money laundering is particularly important when one takes into account the general assessment of the said National Strategy for Combating Organized Crime in 2009: that all state bodies in charge of fighting organized crime is characterized by insufficient staffing both in number and in quality[23]. Furthermore, in the same document from the net and the observation that there is a tendency towards outflow of quality and experienced personnel from state authorities in charge of fighting organized crime in other state bodies and the private sector, which attracts them incomparably better salaries. Finally, in the same act was noticed also that there is a system of training that would enable continuous acquisition of the necessary expertise, but it is carried out from time to time, through seminars, round tables, practical training, study visits and similar activities. For these reasons, it is stated that it is above all necessary for better enable authorized persons in entities that are required to implement measures to prevent money laundering and terrorist financing, as well as their deputies, which makes it compulsory for professional examination and licensing of a certified faces.

As for the particular money laundering, reports on the work of the Directorate for Prevention of Money Laundering of the Republic of Serbia clearly point to the importance of improving further training of employees in all the taxpayers in order to contribute to a more effective detection of suspicious transactions, and prevention of money laundering[24]. The administration for prevention of money laundering under the control of the application of existing regulations with domestic banks in respect of the prevention of money laundering in particular insists on the importance of continuous training and specialization of personnel and technical and technological equipment, which certainly affects the quality of the analysis and identification of potential risks. In this way the disposal of high-quality and accurate information on suspicious transactions is ensured, as one of the prerequisites to establish a whole system that works effectively to combat money laundering and terrorist financing.

21 FATF (2015), „Legal systems and operational issues" and anti-money laundering and counterterrorist financing measures - Belgium, Fourth Round Mutual Evaluation Report, the FATF. www.fatf-gafi.org/topics/mutualevaluations/documents/mer-belgium-2015.html.
22 Demetis, D.S. (2010) Anti-money Laundering, Edward Elgar Publishing Inc.
23 Official Gazette of the Republic of Serbia no. 23/2009.
24 http://www.apml.gov.rs/

Management seeks to, as well as in the previous period, actively monitor new trends in supplying and misusing financial instruments banks in the country and the world and share experiences with other financial intelligence services in international seminars and conferences[25]. The information about the work of the anti-money laundering highlight the importance of enhancing further training of persons employed in the taxpayers in order to contribute to a more effective detection of suspicious transactions, and prevention of money laundering. So far, banks have submitted the highest number of reports of cash transactions in the amount of EUR 15,000 or higher (over 97% of total), while the reports of suspicious transactions regardless of the amount submitted exclusively Bank.[26] In order to improve the functioning of the system of prevention of financial fraud, it is necessary that the other persons become more active in identifying suspicious transactions. This requires the continuous education and training of all taxpayers, especially in banks and insurance companies. Within the "Pray" realized in 2011 in the Republic of Serbia, significant needs were identified for education in the most important institutions in the fight against all financial scam.[27]

P11: Communication and promotion.

Communication takes place within the components of 2:03 Model (internal communication), as well as between these components (external communication). It is necessary to communicate with the public, both domestic and international. This part of the communication is done through the media, formally, through promotional activities.

The role of the media in the fight against financial fraud is overwhelming, and may be twofold: they can provide negative and positive publicity activities in the fight against financial abuse. An example of the negative publicity the media presentation of statistics that reveal huge delays in the work of government organs, ministries, agencies, police, courts, and all those who are responsible for law enforcement and trial.[28]

The slowness in dealing with proceedings initiated can create public image that most crimes of financial fraud resulted in no formal charges or not to lead to criminal proceedings, and that the culprits remain unpunished. Certainly this does not send a good message to the citizens, especially the potential perpetrators and participants in the crimes of financial fraud.

Based on the model of the system of preventive action in cases of financial abuse (Fig. 3) is clearly the importance of promotional activities, which include all the components and processes of the system. Regardless of such importance, this process will not be effective enough if not far enough, especially in terms of methodology. This in turn can be achieved by ensuring that promotional activities must follow all the rules of the profession. Within this project, "Pray" revealed the need for better visibility. In particular, the Directorate for Prevention of Money Laundering of the Republic of Serbia emphasizes the need to improve your site in order to facilitate its use by the public, but also to allow for a better flow of information from agencies with which it cooperates.[29]

25 Typologies of money laundering in the Republic of Serbia, the Organization for Security and Cooperation in Serbia, http://www.apml.gov.rs/REPOSITORY/977_tipologije-pranja-novca-u-republici-srbiji-13-09-2011.pdf

26 Vukovic, S, Mijalković, S. Bošković, G. (2011). Prevention of money laundering and terrorist financing, the basic methods and possibilities, NBP, Journal of Criminal Justice and Law, Criminalistics - Police Academy, Belgrade, ISSN 0354-8872.

27 Pray, 2001 Project against Money Laundering and Terrorist Financing in Serbia (MOLI Serbia), Preliminary report, CRIS no. 2010 / 252-978 and the Council of Europe no. JP / 2274, 2011 years, http: //www.apml.gov.rs/.

28 Radojicic, M. (2015) the interrelations between banking and insurance systems and the prevention of international financial abuse, PhD Thesis, Obuda University, Budapest.

29 Pray, 2001 Project against Money Laundering and Terrorist Financing in Serbia (MOLI Serbia), Preliminary report, CRIS no. 2010 / 252-978 and the Council of Europe no. JP / 2274, 2011 years, http: //www.apml.gov.rs/.

P12: The use of information and communication technologies (ICT)

Information and communication technologies have an increasingly important role in the whole society. In the area of financial fraud that their role is twofold - they are also a tool for the implementation of fraud and tools for their control and prevention. One of the best ways of catching criminals is to track their ill-gotten gains by using ICT. The Schengen Information System (SIS) has been set up at the level of European Union, which is composed of many interconnected databases that enable police forces and judicial authorities to exchange information on persons or objects that are being traced.

Databases of the new generation (SIS II) have a higher capacity and allow storage of new types of data, in accordance with new IT concepts: Big Data, Data Mining, etc.[30]

P13: The organization and coordination

The use of information and communication technologies (ICT) encompasses the entire fourth component models (state institutions, led by the Directorate for Prevention of Money Laundering of the Republic of Serbia), or exclusive reliance on ICT can contribute to a successful fight against the finance crime. ICT is only a tool that serves one indeed an important component of the system of preventive action in cases of financial abuse. It is necessary to develop and maintain, other system components too, and processes that link them or rely on them. So, the only integrated solution that dynamically improves, can lead to complete success in the struggle with the challenge of fraud in the financial sector, where necessary and excellent organization and perfect coordination between all components in the system.[31]

CONCLUSION

Drawing on the statement that the problem of financial crime is global and that this form of organized crime knows no borders, it seems increasingly to be the answer to this "challenge" must also look exclusively at the global level. The conclusion that I imposed the relevant factors in dealing with financial crime is that it must take a series of "solid, comprehensive and international measures" that will, by solving the problem of the drug trade, and set up a foundation to combat other illegal activities, primarily anti-money laundering.[32]

Defining unified, systematic approach to testing and detection of financial fraud and defining preventive actions aimed at combating financial crime in the form of a Model System of preventive action in cases of money laundering presented in this paper aims to increase the safety of the financial sector and reducing the threat of financial abuse to a minimum.

The analysis of the components and processes of the proposed model system of preventive action in cases of money laundering carried out a number of conclusions and recommendations based on them are aimed at achieving this end:[33]

30 Djurdjevic Z, D, & D Stevanovic, M. (2015). The problems facing the IT sector in the fight against money laundering in Serbia. (Čekerevac W., Ed.) FBIM Transactions, 3 (1), 174-187. doi: 10.12709 / fbim.03.03.01.20.

31 Radojicic, M. (2015) the interrelations between banking and insurance systems and the prevention of international financial abuse, PhD Thesis, Obuda University, Budapest.

32 Mitsilegas, V. (2003) .Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance Versus Fundamental Legal Principles (European Business Law and Practice), Kluwer Law International, The Hague, p. 42.

33 Radojicic, M. (2015) the interrelations between banking and insurance systems and the prevention of international financial abuse, PhD Thesis, Obuda University, Budapest.

Maximum load is the fourth component of the model - national institutions, particularly the competent FOS unit (Directorate for Prevention of Money Laundering RS);

- It's important to invest in national institutions responsible for combating financial crime, especially in the FOS unit, police, judiciary, and other actors;

- Investments in institutions implies investment in human resources (permanent training and training with the financial stabilization which prevents the outflow of professional staff) and equipment (ICT);

- It is necessary to further develop the component of international cooperation, too, because the system cannot survive without interaction with the environment; finally,

- It is necessary to continually build relationships with the public (public relations). Promotion is a legitimate act of preventive fight against all forms of crime, including financial. It is necessary to devise a good campaign that will be adequately supported by the media and continuously conducted in order to bid farewell to all the activities that fall within the domain of financial fraud. At the very least, through the promotional activities to the general public side effects of all forms of financial fraud must be displayed and point to the potential dangers of entering into this type of crime, that of bad faith and in ignorance

REFERENCES

1. Cindori, S. (2013). Money laundering: correlation between risk assessment and suspicious transactions, Financial Theory and Practice, 37 (2), 181-206.):
2. Cox, D. (2011). An Introduction to Money Laundering Deterrence, John Wiley & Sons, Ltd.
3. Demetis, D.S. (2010) Anti-money Laundering, Edward Elgar Publishing Inc.
4. Djurdjevic Z, D, & D Stevanovic, M. (2015). The problems facing the IT sector in the fight against money laundering in Serbia. (Čekerevac W., Ed.) FBIM Transactions, 3 (1), 174-187. doi: 10.12709 / fbim.03.03.01.20.
5. Golobinek, R. (2007). Financial investigations and confiscation of proceeds of crime. The manual for the police and judiciary. Council of Europe Office in Belgrade.
6. FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, updated October 2015, the FATF, Paris, France, www.fatf-gafi.org/recommendations.html
7. Fontaine, P. (2010). Europe in 12 lessons. Publications Office of the European Union, Luxembourg, 80 pp.
8. FATF (2015), "Legal systems and operational issues" and anti-money laundering and counterterrorist financing measures - Belgium, Fourth Round Mutual Evaluation Report, the FATF. www.fatf-gafi.org/topics/mutualevaluations/documents/mer-belgium-2015.html
9. Labudovic-Stankovic, J. (2013) Money laundering with an overview of insurance, European Insurance Law Review 3/13, http://www.erevija.org/pdf/articles/ser/JasminaLabudovic 3-2013.pdf
10. Mitsilegas, V. (2003) .Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance Versus Fundamental Legal Principles (European Business Law and Practice), Kluwer Law International, The Hague, pp. 42nd
11. Pray, 2001 Project against Money Laundering and Terrorist Financing in Serbia (MOLI Serbia), Preliminary report, CRIS no. 2010 / 252-978 and the Council of Europe no. JP / 2274, 2011 years, http: //www.apml.gov.rs/

12. Nikolic, B. Necessary instruments for the efficient seizure of proceeds from organized crime, Guidelines for amending the domestic legislation), Justice in Transition - vol. 9, Belgrade, 2009th
13. Radojicic, M. (2015) the interrelations between banking and insurance systems and the prevention of international financial abuse, PhD Thesis, Obuda University, Budapest,
14. Rezaee, Z. & Riley, R. (2010) Financial Statement Fraud - Prevention and detection. John Wiley & Sons, New Jersey,
15. The national strategy for combating money laundering and terrorist financing. Official Gazette of the Republic of Serbia, no. 55/05, 71/05-correction, 101/07, 65/08, 16/11, 68/12-US, 72/12, 7/14 and 44/14-US
16. Typologies of money laundering in the Republic of Serbia, the Organization for Security and Cooperation in Serbia, http://www.apml.gov.rs/REPOSITORY/977_tipologije-pranja-novca-u-republici-srbiji-13-09-2011. Pdf
17. Vukovic, S, Mijalković, S. Bošković, G. (2011). Prevention of money laundering and terrorist financing, the basic methods and possibilities, NBP, Journal of Criminal Justice and Law, Criminalistics - Police Academy, Belgrade, ISSN 0354-8872

UDC: 343.359.3:7.032
314.151.3

MIGRANT AND ANTIQUITIES SMUGGLING

Antonios Maniatis, LLD[1]
Police Academy, Officers' School, Athens

Abstract: In the European Union, there are two models of maritime migrant smuggling, the Western one, similar to the model of piracy in the Straits of Malacca, and the Eastern – Greek model, rather quite similar to the model of piracy off Somalia. Due to the current crisis relevant to migrants and refugees, FRONTEX is likely to be upgraded in legal and institutional terms. As far as antiquities looting and smuggling is concerned, it is about a diachronic prosperous criminal activity. Italy is the point of entrance of very important quantities of both smuggled migrants, particularly coming from North Africa, and smuggled antiquities, particularly the ones coming from the land or the bottom of the seas of Greece. In cases of smuggling (migration as well as antiquities looting), Italy receives the major part of inputs through maritime transports and remains often a country of passage to other countries. As far as antiquities "trafficking" is concerned, relatively little empirical data have been gathered and published, compared to other types of commodity trafficing, in drugs, wildlife or even human beings. The present paper proves the similarity of migrant smuggling and antiquities looting and smuggling, as for their incentives and methodology.

Keywords: smuggling, migrants, refugees, sponsors, antiquities looting, criminality in Italy and in Greece.

INTRODUCTION

The Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the UN Convention against Transnational Organized Crime defines migrant smuggling. Thus, this phenomenon consists in "…the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a state party of which the person is not a national".

Besides, since 1970, humanity has been endowed with an important legal tool against the diachronic prosperous activity of monuments trade. It is about the Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property, adopted in Paris.

We suppose that migrant smuggling is similar to the antiquities smuggling.

PIRACY AND SLAVERY: THE WAR CHARACTERISTIC IN COMMON

Piracy is an economic crime, genrally not a political one, which was classified by Aristotle among the socially acceptable jobs. Indeed, even though pirates are generally described as *hostis humanis generis*, there has been a time when piracy was not a crime as such, when

1 E-mail: maniatis@dikaio.gr.

lawful and unlawful pirates did effectively coexist[2]. Nowadays, since the creation of competent international organizations and its resurgence in the 1970s, piracy has become a major security issue[3]. It is important to remember that legal international standards can only emerge when the interests of a large number of states coincide. Piracy constitutes a perfect example, especially while the United Nations worked on the law of the sea from 1973 to 1982 and created the1982 Montego Bay Convention on the Law of the Sea (UNCLOS).

Piracy is the "forgotten" international law crime, against public opinion, which mainly Military Navy forces have to cope with. It has been put into publicity mainly since the emergence of piracy criminality in 1990s, in the Straits of Malacca and the wider region. The main region of piracy risk is located off Somalia, implicating international anti-piracy interventions, such as the European Union operation "Atalanta" and the NATO operation "Ocean Shield".

Even officials of Libya invoked the piracy risk, to avoid international intervention against their power. Following the Muammar al-Gaddafi regime's targeting of civilians in October 2011, NATO answered the UN's call to the international community to protect the Libyan people[4]. A son of the dictator declared to media that if the regime collapsed, the Mediterranean Sea would become full of pirates, reaching the Italian coasts and Crete. Anyway, migrant smuggling has produced a very serious concern since the beginning of the on-going revolutionary domino crisis, called "Arab Spring", put into practice from December 2010 and on, and exemplified by the Libyan case. In Tunisia, the point of beginning of this set of rebellions and civil wars, the authoritarian government was overthrown in January 2011.

In 2009, Libya's leader signed a deal with Italy to stop the flow of illegal immigrants from northern-Africa to its shores and warned the waters might "turn black because of illegal immigrants". Nowadays, ISIS backs up what it promised would happen if the regime fell – there would be pirates in Crete, and on the Italian shore. Libya would become another Somalia. In February 2015, Italian officials already believed that militants of ISIS were working with experienced seamen – the human traffickers shipping tens of thousands of migrants to Europe every month[5]. This seems one of the versions of the links between migrant smuggling or human trafficking and terrorist organizations and similar armed movements, like ISIS.

MIGRANT SPONSORS

Italy has seen important inward migration since the 1980s. Given its position in the centre of the Mediterranean, and with over 8,000 kilometres of coastline, it is considered the most accessible entrance to Europe by many migrants[6]. In this country, in March 1998 a new immigration law was voted, 40/98, known as the Turco-Napolitano Law. One of the objectives of that legislative text was the development of an active policy relevant to the entrance of foreigners, enabling them to enter the country legally, as long as there is an invitation from an employer or a private person[7].

2 D. Gaurier, *The Pirate's Path: Becoming the Enemy of All Mankind*, pp. 25-40, in H. Ch. Norchi, G. Proutière –Maulion, *Piracy in comparative perspectives: Problems, Strategies*, Law, Paris,-Londres, Pedone – Hart, 2012.
3 C. Leboeuf, *France's action against maritime piracy and the Contact Group on Piracy off the Coast of Somalia (CGPCS): interests, interactions and priorities*, Neptunus, e.revue, vol. 21, 2015/1, p. 2.
4 Anonymous, *NATO and Libya (archived)*, http://www.nato.int/cps/en/natolive/topics_71652.htm.
5 H. Roberts*, ISIS could become the pirates of the Mediterranean and bring havoc to European waters after taking coastal towns in Libya*, Mailonline 2015, http://www.dailymail.co.uk/news/article-2959848/Warning-ISIS-pirates-Mediterranean-bring-havoc-European-waters-taking-coastal-towns-Libya.html.
6 D. Paparelle, V. Rinofli, *New legislation regulates immigration*, European Observatory of Working Life, http://www.eurofound.europa.eu/observatories/eurwork/articles/new-legislation-regulates-immigration.
7 A. Polyzou, D. Altsitzoglou, *The case of Italy*, pp. 156–204, *in Immigration Policy The European Experience*, 2007 (in Greek).

The sponsor model was applied in the period 1998–2000 with satisfactory results, as it provided the occasion to new immigrants, endowed with some contacts in the Italian territory, to find a job and to enter the country in a legitimate way. In Italy, a sponsor could be either a natural person or an organization. The terms of sponsorship, in both alternative cases, remained the same, with the unique exception of the fact that a natural person could take over, as a sponsor, the stay of up to three foreigners, against eight as far as an organization was concerned.

However, the Bossi-Fini Law, in 2002, modified the aforementioned law and put into practice a new program of legitimization of immigrants. One of the major changes that it produced consisted in the contracts between the employers and the immigrants and the raise in expulsions[8]. Given that this model was proved to be successful, a part of the Greek doctrine has proposed it for the Greek legal order[9].

MIGRANT SMUGGLERS

In European Union there are two models of illegal maritime migration, the "Western" one, comparable with the model of piracy in the Straits of Malacca (operations made by relatively big ships), and the "Eastern – Greek" one, rather quite similar to the piracy model off Somalia (operations made by small speedboats)[10].

On the one hand, the Western model is located off Spain and Malta and has to do with big sea distances between the country of origin and the country of destination, the use of big ships and the transport of a great number of smuggled migrants "on block".

On the other hand, the Eastern model includes short sea distances, a thoroughly different *modus operandi* of the criminals' networks and a big number of incidents with the use of ships of various types, which can carry wide range numbers of smuggled migrants.

As for migration from Turkey to Greece, the first step of the process of this illegal industry is the external syndicate structure that transports migrants from other countries towards the Greek borders. The major centre of these crime groups is Turkey, though not only Turkish nationals participate. In the major cities of Turkey and in particular in Istanbul, Izmir, Bursa, Edirne and Mersin, as well as all the ones close to the tri-border corridor with Iran, Iraq and Syria, well-formed smuggling networks quickly assemble prospective "clients" and arrange transfers. Depending on the economic situation of each immigrant, his/her time schedule and the number of groups assembled, a long march via trucks, vehicles and trains takes form onwards to the Aegean shores. Nevertheless, this land route is still active to an extent. The sophistication and influence of the smugglers can be shown by the fact that they tend to be always equipped with the necessary means of transportation and have ample human resources. Besides, yachts from Turkey have been noticed traveling the entire Aegean and Ionian seas to reach groups of immigrants massed at specific points, and then take them across to Italy. The same can be said for speedboats, included luxurious, "unsuspicious" ones. Back on land, an unknown number of warehouses in both Turkey and Greece are rented for the purposes of hiding people, while thousands of vehicles are used for transport[11].

8 Hellenic Migration Policy Institute, *Policies of Immigrants' Inclusion: The European Experience*, 2006, p. 131 (in Greek).
9 A. Triantafyllidou, *Chapter 11 The Greek immigration policy in the 21st century: problems and challenges*, pp. 441–454, in A. Triantafyllidou, Th. Maroukis (Eds), Immigration in Greece of the 21st century, Kritiki Publishers 2010 (in Greek).
10 Ministry of the Merchant Navigation, Aegean and Insular Policy, *A synoptic presentation of the phenomenon*, http://www.yen.gr/wide/yen.chtm?prnbr=32021 (in Greek).
11 I. Michaletos, Ch. Deliso, *The Illegal Immigration Industry in Greece in 2015: a Strategic Overview*, Balkananalysis.com, http://www.balkanalysis.com/greece/2015/03/25/the-illegal-immigration-

It is to pay special attention to the fact that an alternative route to the Thracian land border along the River Evros has been greatly reduced due to fences constructed by the Greek and Bulgarian authorities. It is about an important innovation, of technical nature, which initially raised severe criticism in Greece, as for the protection of the human rights of the persons involved, such as migrants and refugees. This development led the smugglers' networks to make use almost uniquely of the maritime transports instead of the safer route of Evros. In 2015, the migration movement from Eastern countries, especially from Syria due to the civil war and to the barbarism of the ISIS involvement, via Turkey to Greece raised drastically. Smuggling, at least with the tolerance, if not with the encouragement, of the Turkish authorities has provoked the loss of many human lives in the Aegean Sea and, as a result, great emotion on international scale. In spite of this fact, the Greek government has no political will to create a passing point in the land of Evros, with the pretext that in this region, migrants would run the risk of passing through mine fields.

Anyway, once arriving in Greece, the vast majority of migrants and refugees want to leave the country, mainly for Central Europe. So, another type of smuggling network is activated, to transport people from Greece, particularly from Athens, further into Europe, by making use of forged papers, such as identity cards and passports.

THE MIGRANT INTERCEPTION

Amongst the extraterritorial immigration control techniques, a primary role is attributed to interception, a term which aptly describes "measures applied by States outside their national boundaries which prevent interrupt or stop the movement of people without the necessary immigration documentation from crossing the borders by land, sea or air". In the maritime context, interception of this kind has attained even more vigour the last years in the light of the adoption of the aforementioned Protocol against the Smuggling of Migrants by Land, Sea and Air, as well as of the relevant practice of states, like Australia (laws commonly referred to as "Pacific Strategy"), United States and various European States. This has also been the recent activity of the European Union and more specifically of the European Agency for the Management of External Borders (FRONTEX), which was established in 2004 to help Member States in implementing community legislation on the surveillance of EU borders. After the establishment of FRONTEX, interception operations are still executed by EU Member States, which have the relevant authority and responsibility, yet are principally planned and coordinated by FRONTEX. Anyway, extraterritorial rescue operations concerning migrants at sea cannot be disconnected from the duty of safeguarding the human rights of the persons subject to these measures[12].

ANTIQUITIES SMUGGLING

Cultural law is a specific branch of law, having as its main subcategory the cultural goods law. Some countries not enough familiarized with sponsorship, such as France and Greece, have recently adopted specialized legislation on contracts of cultural sponsorship. In opposition to the Greek empirical data, the French state has made use of this mechanism to back up its fight to the cultural goods looting. Sponsors have financially supported the authorities to

industry-in-greece-in-2015-a-strategic-overview/.

12 Ef. Papastavridis, *Extraterritorial Immigration Control. The Responsibility of States for Human Rights Violations*, Annuaire International Des Droits de l'Homme VI/2011, pp. 315–344.

outlaw the perpetrators against large monetary compensation. Anyway, looting and illicit export of cultural goods are considered as a rather "fine" kind of sophisticated activity. Indeed, it is not about a commerce implicating dangers for human life and health, in contradiction with the weapons market and the drugs one.

Italy is the point of entrance of very important quantities of both smuggled migrants, particularly coming from North Africa, and antiquities, particularly the ones coming from the land or the bottom of the seas of Greece[13]. Of course, the illegal trafficking of monuments is eventually related to the phenomenon of piracy in a metaphorical sense, having to do with the violation of intellectual property rights, and the problem of alteration or lack of the scientific knowledge on matters of history and archaeology[14]. In cases of smuggling (migration as well as antiquities looting), Italy receives the major part of inputs through maritime transports and remains often a country of passage to other countries.

Anyway, antiquities smuggling seems to adopt a more inventive methodology than migrant smuggling, as implied by the so-called "Chippindale's Law", which is the following: "However bad you feared it would be [so far as antiquities looting and smuggling are concerned], it always turns out worse".

As far as antiquities "trafficking" is concerned, relatively little empirical data have been gathered and published, compared to other types of commodity trafficking, in drugs, wildlife or even human beings, till a recent empirical study conducted in Cambodia and Thailand[15]. This research, supported by the European Research Council under the European Union's Seventh Framework Program, has ended up with the following important findings:

- organized crime is involved in antiquities looting and trafficking,
- the traffic in looted artefacts overlaps with the insertion of fakes into the market, so the fake monuments have proved to be a serious danger for culture and science,
- surprisingly few stages there are between looting at source and the placing of objects for public sale in internationally respected venues.

ANTIQUITIES, CRIMINAL ORGANIZATIONS AND TERRORISM

A few years before the adoption of the aforementioned legislation on cultural sponsorship, from about 2000 and on, antiquities looting and smuggling have been incorporated into a new globalized set of regulations, the organized crime criminal law, like human trafficking. For instance, according to the constitutional law 5/99, the organized crime group is an association of three or more persons, united with the goal to commit, constantly or repeatedly, one or more of the following crimes:

1. kidnapping,
2. crimes related to prostitution,
3. crimes against property and socioeconomic order,
4. crimes related to intellectual or industrial property,
5. crimes against the rights of workers,

13 A. Maniatis, *Les mesures de protection des biens culturels*, RSC 2010 Janvier/Mars, pp. 303–306.
14 A. Maniatis, *Sea and see piracy*, pp. 1385–1394, in D. Vrontis, Y. Weber, E. Tsoukatos (Eds.), 8th Annual Conference of the EuroMed Academy of Business Innovation, Entrepreneurship and Sustainable Value Chain in a Dynamic Environment, 2015.
15 S. Mackenzie, T. Davis, *Temple looting in Cambodia. Anatomy of a Statue Trafficking Network*, Brit. J. Criminol. 2014, 54, pp. 722–740, mainly p. 722.

6. crimes of endangered species trafficking,
7. crimes of nuclear and radioactive material trafficking,
8. crimes against public health,
9. crimes of money forgery,
10. trafficking and deposit of fire arms and ammunition,
11. terrorism,
12. crimes against historic heritage[16].

In many national legal orders in the last years specialized regulations have been introduced not only against organized crime but also against acts of terrorism, as it is the case of Greece. Anyway, antiquities smuggling has proved to be potentially relevant even to terrorism. One example of how the global trade in stolen art and antiquities funds terrorism comes from Iraq[17]. US Colonel Matthew Bogdanos, who served in counter-terrorism operations in 2003, investigated the looting of the Iraq National Museum, from which thousands of valuable antiquities were stolen. For over five years the famous officer, who is one of a set of twins born and raised in New York to parents who had immigrated from Greece, led a team to recover the artefacts. Up to 2006 circa 10.000 artefacts were recovered through his efforts. He later recalled in an interview with CNN:

"From my experience, I can say that the illegal antiquities trade has become a revenue stream for terrorist activity in the region. In 2005, every single weapons shipment that we seized, whether from terrorists or insurgents, also contained antiquities. These trucks, but also caves, buildings and other hiding places, would contain boxes of rocket propelled grenades alongside boxes containing ancient tablets and figurines".

CONCLUSION

Migrant smuggling is a form of criminality with particular characteristics, given that it is about a transnational organized crime with a different *modus operandi* within the Eastern – Greek model from the Western model one. Like the antiquities traffickers, smugglers tend to adopt sophisticated and frequently innovative techniques to accomplish their mission. The last years there have been important developments in both cases of legal migration and smuggling (institutionalization of the role of sponsors, Frontex, state fences in the land of Evros, etc.).

Anyway, the hypothesis of the current study has been confirmed, as migrant smuggling is quite similar to the antiquities looting and smuggling phenomenon, particularly to its juridical modern version of crimes of the so-called "criminal organizations".

Besides, in spite of the fact that the objects of these two different types of crimes may appear similar from a morphological point of view (human victims as for migrant smuggling against statues, figurines and icons of human beings, as for monuments smuggling), these types have a lot of essential features in common, such as:

a) financial incentives, although antiquities smuggling has the particularity that it is basically a "white collar crime",

b) transnational character, with Italy as a country of strategic location,

16 M. J. Hurtado, *The fight against transnational organized crime*, pp. 7–15, mainly p. 11, in International Scientific Conference, "Archibald Reiss Days" Thematic Conference Proceedings of International Significance Volume I, Beograd, 2015, Academy of Criminalistic and Police Studies, Belgrade, 2015.
17 Interpol, *Against Organized Crime. Interpol trafficking and counterfeiting casebook 2014*, www.interpol.int, p. 118.

c) Incorporation into the notion and the modern legislation on "criminal organizations", as for antiquities looting and smuggling and as for human trafficking, even if there is also the case of migrant smuggling, which deserves to be incorporated into,

d) unlawful variations, namely human trafficking against migrant smuggling as well as monuments counterfeiting against antiquities looting and smuggling,

e) potential bonds with cases of terrorism or other similar armed movements (refugee and migrant smuggling may facilitate the entrance of prospective perpetrators of acts of terrorism to the countries they want to offend, terrorist organizations or rebels are funded through antiquities looting and trade).

Last but not least, the current analysis has highlighted the existence of various legitimate tools, under the common label of sponsors, relevant to these two types of criminality or the correspondent legitimate social activity. Indeed, the role of sponsors has been institutionalized for the legal immigration whilst companies may help the authorities outlaw perpetrators of crimes against the property of cultural goods.

Migrant smuggling is based on the real will of people to leave their homeland to the developed countries for financial reasons, antiquities smuggling is based on the real will of the perpetrators to export looted antiquities, mainly from the "archaeological countries" like Greece and Italy to the Western developed countries, equally for financial reasons. So, migrant and antiquities smuggling in a way constitute "the two sides of the same coin".

REFERENCES

1. Anonymous, *NATO and Libya (archived)*, http://www.nato.int/cps/en/natolive/topics_71652.htm.
2. D. Gaurier, *The Pirate's Path: Becoming the Enemy of All Mankind*, pp. 25-40, in H. Ch. Norchi, G. Proutière –Maulion, *Piracy in comparative perspectives: Problems, Strategies*, Law, Paris,-Londres, Pedone – Hart, 2012.
3. Hellenic Migration Policy Institute, *Policies of Immigrants' Inclusion: The European Experience*, 2006, p. 131 (in Greek).
4. Interpol, *Against Organized Crime. Interpol trafficking and counterfeiting casebook 2014*, www.interpol.int.
5. C. Leboeuf, *France's action against maritime piracy and the Contact Group on Piracy off the Coast of Somalia (CGPCS): interests, interactions and priorities*, Neptunus, e.revue, vol. 21, 2015/1.
6. S. Mackenzie, T. Davis, *Temple looting in Cambodia. Anatomy of a Statue Trafficking Network*, Brit. J. Criminol. 2014, 54, pp. 722-740, mainly p. 722. M. J. Hurtado, *The fight against transnational organized crime*, pp. 7-15, mainly p. 11, in International Scientific Conference, "Archibald Reiss Days" Thematic Conference Proceedings of International Significance Volume I, Beograd, 2015, Academy of Criminalistic and Police Studies, Belgrade, 2015.
7. A. Maniatis, *Les mesures de protection des biens culturels*, RSC 2010 Janvier / Mars, pp. 303-306.
8. A. Maniatis, *Sea and see piracy*, pp. 1385-1394, in D. Vrontis, Y. Weber, E. Tsoukatos (Eds.), 8th Annual Conference of the EuroMed Academy of Business Innovation, Entrepreneurship and Sustainable Value Chain in a Dynamic Environment, 2015.
9. I. Michaletos, Ch. Deliso, *The Illegal Immigration Industry in Greece in 2015: a Strategic Overview*, Balkananalysis.com, http://www.balkanalysis.com/greece/2015/03/25/the-illegal-immigration-industry-in-greece-in-2015-a-strategic-overview/.

10. Ministry of the Merchant Navigation, Aegean and Insular Policy, *A synoptic presentation of the phenomenon*, http://www.yen.gr/wide/yen.chtm?prnbr=32021 (in Greek).
11. D. Paparelle, V. Rinofli, *New legislation regulates immigration*, European Observatory of Working Life, http://www.eurofound.europa.eu/observatories/eurwork/articles/new-legislation-regulates-immigration.
12. Ef. Papastavridis, *Extraterritorial Immigration Control. The responsibility of States for Human Rights Violations*, Annuaire International Des Droits de l'Homme VI/2011, pp. 315-344.
13. A. Polyzou, D. Altsitzoglou, *The case of Italy*, pp. 156–204, *in Immigration Policy The European Experience*, 2007 (in Greek).
14. H. Roberts, *ISIS could become the pirates of the Mediterranean and bring havoc to European waters after taking coastal towns in Libya*, Mailonline 2015, http://www.dailymail.co.uk/news/article-2959848/Warning-ISIS-pirates-Mediterranean-bring-havoc-European-waters-taking-coastal-towns-Libya.html.
15. A. Triantafyllidou, *Chapter 11 The Greek immigration policy in the 21st century: problems and challenges*, pp. 441-454, in A. Triantafyllidou, Th. Maroukis (Eds), Immigration in Greece of the 21st century, Kritiki Publishers 2010 (in Greek).

UDC: 343.85:343.352

CORRUPTION: INDIVIDUAL OR/AND ORGANISATION RELATED PHENOMENON

Gyöngyi Major, PhD[1]
Institute for Strategic Research, Budapest

Abstract: This study focuses on the methods of corruption measurement that estimate the rate of corruption based not on subjective perception. Instead, it tries to track down disappearing funds by monitoring economic processes. The present document will also analyse the practice introduced into professional literature by Olken (2009), which tries to find and apply an intendedly objective corruption identification method, to replace reports on cases of corruption.

Our starting point is the set of results of research into interconnections between corruption and economic growth. With reference to the Multiple Indicators/Multiple Causes model, attention will be paid to the negative correlation between control over corruption and the volatility of inflation and growth.

Besides the economic aspects of corruption, we will also shed light on the social and cultural causes since, with an evolutionist approach, evidence is available to prove that corrupt individual behaviour can become a norm in the long term. We will emphasise that, if we are to prevent that from happening, efforts must be made against corruption – but these efforts can only be successful if a strategic approach is taken.

Keywords: corruption, economic growth, monitoring, MIMIC, prevention

INTRODUCTION

„Many lower-class male adolescents experience a sense of desperation surrounding the belief that their position in the economic structure is relatively fixed and immutable. As a result of failing to meet cultural expectations of achieving upward mobility, conditions become ideal for socialization functions such as recruitment, screening, and training for organized crime to occur at the community level."

(Lyman –Potter, 2007, p. 69)

Despite the fact that it can be described as a concept, corruption, due to its dynamic nature, cannot be interpreted as a transparent phenomenon – on the contrary: because of the internal essence of corruption, it is its obscure intertwining network that we can consider as its determining feature.[2] Corruption crimes are characterised by a strong relationship of trust between the actors, each participant has an interest in keeping the act in secret and the crime itself can usually qualify as a negative externality. The frequent time difference between the commitment and the achievement of the desired aim makes it even more difficult to track

1 *E-mail: major.gyongyi@gmail.com* Tel:+36 307605970

2 The term is used in the broadest sense in the definition of Transparency International: abuse of entrusted power for private gain. http://www.transparency.org/whatwedo?gclid=CO6T_5u3ir0CFaQfwwoda7oAzg This is a rather broad definition and mostly covers what is called "grand" or "large-scale" corruption, yet not even the contents of the two are entirely the same. Corruption is a phenomenon that exists in many forms and at numerous levels, which is defined through the pronounced separation of two levels: one is the so-called "petty corruption", the other is "grand / large-scale corruption". For more, see: Bunt, H.G. van de – Nelen, H. (2012): Corruption in various shapes and sizes – some criminological reflections", in. International Law and Fight against Corruption. The Hague, Asser Press, p. 13

down the process. Corrupt transactions and the giving of gifts do not always require immediate compensation (Jancsics, 2014). If corrupt exchanges take place at different times, it is easier for the actors to hide the corrupt nature of their transactions.[3]

Using as its starting point the premise that a fundamental precondition of successfully fighting against corruption is to understand its nature (Blackburn – Forgues-P., 2009), this study focuses on interpreting corruption in the framework of a universal – interdisciplinary model, which could solve the problem of organisation researchers generally known as the „Rotten Apples versus Rotten Barrels" dilemma (Trevino - Youngblood 1990, Kish-Gephart et al. 2010, Gottschalk, 2012); i.e. whether corruption is actually an individual or an organisation related phenomenon (Coleman 1987; Sherman 1980; Wheeler - Rothman 1982).

This study approaches the problem of getting to know the nature of corruption from two aspects. On the one hand, we will discuss the controversial nature of the system of relations between the competition/market and corruption and, on the other hand, we will seek an efficient screening methodology for the identification of actual cases.

MARKET, INSTITUTIONS AND CORRUPTION

„Quando crumena sonat litem bene iura coronat"[4]

This study identifies the lack of a universal frame of interpretation as the fundamental problem: the theoretical model that can describe the nature of the process of becoming corrupt at the level of the individual is incapable of identifying the „corruption mechanism" at a system level, and the principles of fighting against corruption that prove efficient at the level of the individual become totally inefficient at a macro level. In this respect, integrated operation based upon following commonly approved values, i.e. „integrity", can counterbalance or, at least, reduce the „corruption pressure" and the development of professional and leadership competencies can be seen as a real act of defence. It should be emphasised, however, that the same level of attention should continue to be paid to transparency. This is a valid priority also because

„(…) education also opens up the way to new and colossal kinds of crime, as debauching of conventions, councils, legislatures, and bribery of the press and of public officials." (Henderson, 1901, p. 250)

There is agreement among corruption researchers that the social models which do not aim at creating and maintaining a well-balanced system of relations will sooner or later be torn apart by internal tensions. (Takács et al, 2011) The fundamental problem, however, is the traceability and comprehensibility of corruption that gets embedded in the social structure and becomes institutionalised[5] (Anders – Nuijten 2008): the essence of these problems is the fact that corruption becomes a social norm and, consequently, social factors, which reach beyond the level of the individual, become motivational factors.[6] (Jancsics, 2014)

3 Jancsics (2014) quotes: Hipp, L. – Lawler., E. (2010): Corruption as Social Exchange. Paper presented at the 105th Annual Meeting of the American Sociological Association, Atlanta, USA, August 2010

4 Is your money a good orator? You will achieve your aim with the judge! (Juvenal: The Satires X, 146)

5 „While traditional societies are transparent and the breaking of norms easily gets unveiled, modernity is characterised by an increasing complexity of relations, as a result of which transparency decreases and exchange transactions are realised more and more along self-interest. In the game theory context, corruption is a behavioural system that carries the elements of competition and cooperation at the same time. According to co-authors Bereczkei-Tóth, this is exactly where one of the problem's roots is found." (Major-Čudan, 2015)

6 Inzelt (2015) emphasises that the concept of corruption and its condemnation by society depend on society's approved norms of operation, ethics and laws. In certain societies, corruption is part of the social-cultural tradition, which gets passed down over different regimes.

According to the representatives of the evolutionist school, corrupt behaviour enables individuals to survive and, in an evolutional process, even becomes self-evident in a special way, through adapting. (See: Mishra, 2005).

Professor Sutherland discussed, as early as in the 1930s, what a serious danger the spreading of corrupt practices poses on society: despite the fact that corrupt companies must pay fines for and get banned from unlawful practices, they do not suffer a major loss of prestige and no personal judgements are passed. As a consequence, corrupt behaviour becomes a competitiveness increasing factor, and the same is accepted as general practice.[7]

Table 1: *Breaches of law by American companies in the first half of the 20th century, based on the collection of Sutherland*[8]

Name of company	Influencing trade	Misleading advertising	Breaches of law	Breaches of labour regulations	Misuse of commissions	Other
General Electric	13 convictions	2	9	0	0	1
General Motors	6	2	22	9	0	1
Goodyear	1	1	4	3	0	5
Procter & Gamble	1	8	1	1	0	2
Sears Roebuck	0	18	20	1	0	0
U.S. Steel	9	2	5	2	5	3

(Inzelt, 2015, p. 35)

Today, research results clearly evidence that one of the most pronounced features of large-scale corruption is the fact that actors can artificially intervene in economic processes and influence state institutions to enforce their own interests. In essence, following the logic of Sutherland, this is what we call white-collar crimes[9], whose essence is that they are not only deliberate but are also organised. (Sutherland, 1983, p. 229)

Recently, the school known as New Institutional Economics (NIE) has started to investigate how corrupt actors create the institutions that reduce the risk of being caught (e.g. through betrayal) (Della Porta – Vannucci 2012). The authors mentioned pointed out in an earlier study that the recurrence of corrupt transactions between the agent and the recipient automatically leads to the strengthening of trust, which structures and institutionalises the corrupt situation in society, stabilises the price of the given act and decreases the transaction cost of corruption (Della Porta – Vannucci 2004). „At this point, players assume that everyone else also breaches the rules. Under such conditions, rules cannot achieve their aims and an atmosphere of uncertainty prevails. Since long-term plans are totally unpredictable in such a scenario, players are likely to make plans that will bring a relatively certain profit in the short run. If these plans are

7 Nowadays, game theory models can be excellently used to resolve the dilemma of whether the profit and benefits expected from corrupt behaviour exceed the amount of fine imposed for corruption.
8 Sutherland (1983) summarised the most important data in 18 tables, which Inzelt congested into one single table.
9 Edwin H. Sutherland used the term „white-collar crime" at a conference of the American Sociological Society held on 27 December 1939.

not successful, players' distrust in institutions increases and players are prompted to reach success through other dishonest methods. And success achieved through corruption or personal relations will not strengthen trust in institutions but will make people interested in maintaining the corrupt system." (Győrffy, 2012)

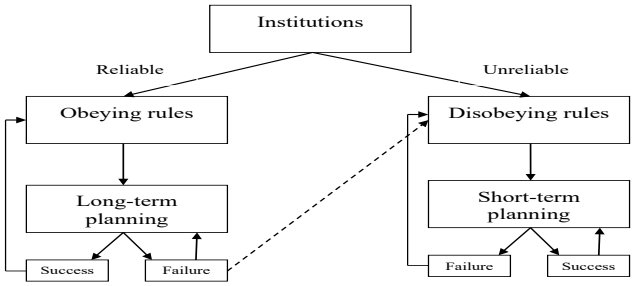


Chart 1: *Institutions and individual decision making (Győrffy, 2012)*

Consequently, the intellectual challenge is how to discover corrupt behaviour[10] and to identify the reasons; more precisely, to decide whether corruption is a system element of competition[11]. An essential question is whether a competitive environment actually prompts actors to disobey rules[12] and, consequently, whether control by institutions is inevitable or on the contrary, the competitive environment becomes a corrupt environment through institutionalisation and the increase of bureaucracy. The most essential aspect of the problem culminates when those protecting the common good also become corruption actors themselves. (Persson et al., 2010, p. 19, Rothstein 2011, pp. 99–104). Once this happens, there is no chance to find any actor in the system who could monitor and sanction corrupt behaviour.[13] (Jancsics, 2014)

In most cases, empirical research proves that there is a reverse correlation between economic competition and corruption[14] (Treisman 2000), as well as the fact that – like in the case of Scandinavian countries – corruption may stay at a low level even with a major level of state intervention in place. (Della Porta - Vannucci 2012; Hopkin - Rodriguez-Pose 2007)

Therefore, our attention should be focused not only on the relations between state

10 At this point, reference should be made to a study of Boehm (1999). From the analysis of hunting and gathering societies, the author arrives at the conclusion that corruption, in the meaning we use it, does not exist in these societies.

11 Jancsics (2014) points out that in certain branches of the economy, where competition is fierce, the level of corruption may be high – but if we look at the country as a whole, for which corruption is shown in an aggregated way, such peaks actually point out that the general level of corruption is low. For this reason, data collected from the organisation level may provide more accurate information about the given organisations' competitive and institutional environment (Alexeev – Song 2013). National data does not reflect company-level variations. Corruption may be very high in certain economic sectors with fierce competition but low at the general national level. „Some scholars found other organizational structural features responsible for illegal activities. For example, large firm size, plentiful slack resources, firms with more complex organizational structures, activity remote from supervision, frequent interaction with costumers, lower dividend payments and higher executive compensation in the form of salary and bonuses provide opportunity structures to conduct corrupt practices." (Jancsics, 2014)

12 One example: Baucus (1994).

13 It has become common practice for companies to invest major amounts of money in influencing journalists and, in general, in making a good impression on public opinion. (For more details, see: Sutherland, 1983, p. 227)

14 When examining the intertwining between corruption and competition, we ought not to forget the fact the social embeddedness of corruption is conspicuous in former socialist countries. Moreover, giving an official some gift was not even seen as bribery. World Bank (2000) Anticorruption in Transition. A Contribution to the Policy Debate, 1-101, Washington, D.C

intervention and corruption but far more on the process of and the system of relations in macrostructural embedding.[15]

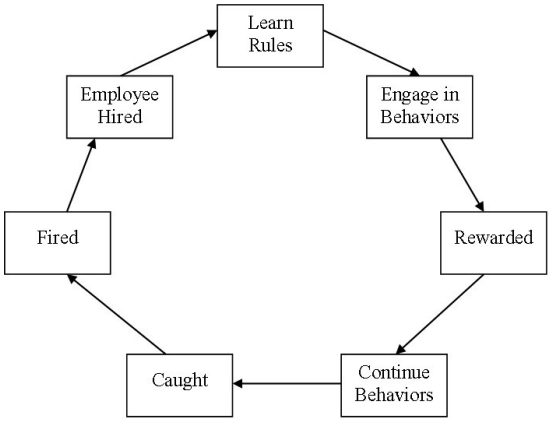


Figure 1: *The Cycle of Corporate Crime*

(Payne, 2013 p. 285)

MEASUREMENT, OBJECTIVITY AND REGULATION

„For participants, corruption is a cooperative „game", in which unselfishness between players has a significant role but, on the level of the entire society, it is an expressly selfish strategy."

(Major- Čudan, 2015)

A precondition of the proper handling of corruption is the creation of a proper definition with an interdisciplinary approach, as reasons are also diversified and increasingly interrelated. Professional literature now deeply analyses the impacts of political, historical, socio-cultural and economic factors and attention is more and more focused on latent aspects. Applying the MIMIC (Multiple Indicators/Multiple Causes)[16] model, Dreher et al. (2007) identified a negative correlation between control over corruption and the volatility of growth, inflation and bank restrictions. It follows from these findings that the security of growth is enhanced by the efficiency of the fight against corruption and of the regulations in force.

Encouraging the no-breach-of-rules behaviour, the efficiency of corruption discovery and the judicial system become the key pillars of the fight against corruption. Consequently, the

15 Jancsics (2014) points out that the extension of the jurisdiction of the government into the economy may lead to the distortion of the operation of the market: it may create new motivating factors for corrupt officials and opportunities for private companies hunting for commissions. At the same time, Jancsics emphasises that „such results suggest that variables other than the level of government intervention might also have a significant influence on the level of corruption."

16 The development of models that represent an indirect methodology was motivated by the fact that the hidden economy has many features that would be important to analyse but cannot be measured. These factors are closely interrelated, and their causes are factors that are measurable. Between the MIMC (Multiple Indicators/Multiple Causes) and DYMIMIC (Dynamic Multiple Indicators/Multiple Causes) models identify relations between the indicators that trigger hidden economic activity and that are consequences of this hidden activity – so that, as a first step, the level of hidden activities are estimated using their causes and then, as a second step, the consequences are estimated using the latent variable of the hidden activity. By amalgamating the two correlations, the structural relations between the different causes and consequences can be analysed. (Murai – Ritzlné Kazimir, 2011)

importance of the role of the state should be reconsidered. Paradoxically, this means that the "3E" set of principles of New Public Management proved neither cheap ("Economy"), nor efficient ("Efficiency"), nor effective ("Effectiveness"). We can thus say that it is becoming ever clearer that it would not really be purposeful to do away with the approach that places the "common good" – a value aspect – over the aspect of economic efficiency.

New Public Management is an approach that wishes to implement the business spirit in the public sector. However, as it has turned out in recent years, the removal of welfare functions will not solve corruption related problems and the diminishing of the role of the state will not in itself result in the decrease of corruption – on the contrary: it entails the possibility that „it is actually certain, privileged players of the *market* that will finally be involved in governance". (Stump – G. Fodor 2008) Based on these findings, the authors of this study expect that the key to forcing back corruption would be a shift towards good governance.

We wish to emphasise that, with regard to its actual contents, good governance can be realised in a model in which public policy making is a multi-level activity (*"multi-level governance"*), and in which „citizens are not merely the addressees of legislative and governance acts, i.e. the subjects of these as subjects of the state, but the *actors* of governance activities and, as such, together with public authority governance actors, will identify the common good by special policy fields and implement it in public policy cycles." (Frivaldszky, 2010)

If we want the fight against corruption to be efficient, we must revaluate the role of the state and modify its public administration system and approach. Without the accurate identification of problems, however, it seems ridiculous to call anyone to account for actual results – which means that the measurement of corruption becomes crucial. As one of the features of corruption is that it is latent, the chance to objectively measure it is, logically, minimal.[17]

Consequently, we consider the tracking of public expenditure a key issue.[18] For the tracking of corruption, however, besides the well-known and already applied methods, which are based on (subjective) perception, we wish to highlight the importance of methods that rely on the tracking of economic processes, which identify and estimate the amount of disappearing funds using actually known money movements as a starting point.

At this point, we should first make mention of the methodology developed for the estimation of corruption in the field of service delivery, QSDS ("quantitative service delivery survey"), which is a type of „frontline provider survey". Despite the fact that interviewees are not necessarily willing to talk about corruption, co-authors Reinikka – Svensson (2005) came to the conclusion that PETS ("public expenditure tracking survey")/QSDS are new microeconomic diagnostic tools for the diagnosis of corruption and other problems in developing countries.[19]

17 Olken's (2009) innovative method, which he applied in road construction projects in Indonesia, was an experiment to objectively measure corruption. In the survey, the declared costs of construction materials were compared with the estimated values of actually used materials, which were determined by drilling holes into the roads and surveying the quality and quantity of the materials actually used according to what was found. Although the study could not offer a reliable estimate about the level of corruption – as significant measurement errors resulted from the fact that there had been sand and pebbles in the ground before the road construction project was launched, i.e. the quality and quantity of the raw materials used could not be accurately assessed –, it still proved successful: it was suitable to find out that corruption was present in the project and to identify the relatively realistic values involved.
18 The so-called PETS (public expenditure tracking survey) method was first applied in Uganda, in 1996. In essence, PETS is a survey that covers service providers (schools, hospitals) and regional governments (politicians and public officials) and uses state budget and other related data. (Reinikka – Svensson, 2005)
19 We should mention the fact that Olken (2009), with his "more objective" method, which he tested in Indonesia on the road construction programme project, he examined the perception of corruption among villagers by interviewing and made estimates regarding missing expenditures and performance. According to Olken, villagers could differentiate between the possibility of corruption in the village and corruption in the road construction project – but had difficulty accurately identifying this difference due to the hiding nature of corruption.

In summary, we wish to emphasise that while corruption is a hidden phenomenon, whose "quantity" can be estimated primarily in indirect ways, the generally applied methods (Transparency International's Corruption Perception Index, the Control of Corruption as part of the World Bank's Institute Governance Indicators) are based upon expert estimates, which entail the possibility of some artificial „inertia". (Takács at al, 2011This means that once a country is identified as "corrupt", false estimates will be made about it based on prejudices, independently of the actual movements taking place in it, and it will continue to be stigmatised as corrupt, which, in essence, means the continuous overestimation of corruption. (Dreher et al., 2007)

CONCLUSION

One of the key preconditions of the success of the fight against corruption is the proper handling of trust. The decline of trust in the system of institutions may increase (or even force) trust between the players of the corruption net, which, by minimising the willingness to follow conventional rules, helps to build out the system of norms of the special „playground" of the corruption space. At the same time, the success achieved through means of corruption will, logically, not increase trust in institutions – on the contrary, actors will become interested in maintaining the corrupt system.

Multi-level, good governance seems to be the suitable tool to force back the alternative system of trust, through the involvement of the civil society, which carries community values and interests, in public policy processes, in both decision making and control functions.

By offering opportunities to the business sector to be involved in projects, New Public Management encapsulates corruption in business rationality, and business players – exactly because of their economic potential – can utilise these opportunities primarily for the enforcement of their internal interests. Along economic rationality, the principle of maximising economic profit will override all other values. As a result, it becomes mission impossible to get out of the magic but vicious circle of corruption along the logic of NPM if it lacks a normative context. Actual achievements can be expected more of the practice of good governance of a subsidiary nature, which relies on the civil society.

And the economic crises of recent years have made it even clearer that regulations and governance are a must – all the way up to the global level.

REFERENCES

1. Alexeev, M. – Song, Y. (2013): Corruption and Product Market Competition: An Empirical Investigation. Journal of Development Economics 103 pp. 154–66.
2. Anders, G. – Nuijten, M (2008): Corruption and the Secret of Law: An Introduction. In: Corruption and the Secret of Law: A Legal Anthropological Perspective. (Nuijten – Anders) Abingdon: Ashgate Publishing Group pp. 1-26.
3. Baucus, M. S. (1994): Pressure, Opportunity and Predisposition: A Multivariate Model of Corporate Illegality. Journal of Management 20 pp. 699–721.
4. Blackburn, K. – Forgues-Puccio, G. F. (2009): Why is corruption less harmful in some countries than in others. Journal of Economic Behavior & Organization. 72. pp. 797–810
5. Boehm, C. (1999): Hierarchy in the Forest. The Evolution of Egalitarian Behavior. Cambridge: Harvard University Press.
6. Coleman, J. W. (1987): Toward an Integrated Theory of White-Collar Crime. The American Journal of Sociology 93 pp. 406–439.

7. Della Porta, D. – Vannucci, A. (2012): The Hidden Order of Corruption - An Institutional Approach. Ashgate.
8. Della Porta, D. – Vannucci, A. (2004): Governance Mechanisms of Corrupt Transactions. In: The New Institutional Economics of corruption. (Ed.: Lambsdorff – Schramm) New York: Routlege. pp. 152–180.
9. Dreher, A. – Kotsogiannis, C. – Mccorriston, S. (2007): Corruption around the world: Evidence from a structural model. Journal of Comparative Economics. 35. pp. 443–466.
10. Frivaldszky, J.(2010): Jó kormányzás és helyes közpolitikaalkotás. Jogelméleti Szemle 4.
11. http://jesz.ajk.elte.hu/frivaldszky44.html#_ftnref5
12. Gottschalk, P. (2012): Rotten Apples versus Rotten Barrels in White Collar Crime: A Qualitative Analysis of White Collar Offenders in Norway. International Journal of Criminal Justice. 7 (2) pp. 575–590.
13. Győrffy, D. (2012): Intézményi bizalom és a döntések időhorizontja. Közgazdasági Szemle 59 (4) pp. 412–425.
14. Henderson, C. R. (1901): Introduction to the Study of Dependent, Defective, and Deliquent Classes. D. C. Heath, Boston
15. Hopkin, J. – Rodriguez-Pose, A. (2007): "Grabbing Hand" or "Helping Hand"?: Corruption and the Economic Role of the State. Governance 20 pp. 187–208.
16. Inzelt, É. (2015): Korrupció: fehérgallérral vagy anélkül. A fehérgalléros bűnözés változó tartalma és formái. Eötvös Loránd Tudományegyetem, Budapest Állam- és Jogtudományi Kar Kriminológiai Tanszék, Ph.D. Disszertáció
17. Jancsics, D. (2014): Interdisciplinary Perspectives on Corruption. Sociology Compass 8/4 pp. 358–372.
18. Kish-Gephart, J., Harrison, D. A. – Trevino, L.K. (2010): Bad Apples, Bad Cases, and bad Barrels: Meta-Analytic Evidence About Sources of Unethical Decisions at Work. Journal of Applied Psychology 95 pp. 1–31.
19. Lyman, M. D. – Potter, G. W. (2007). Organized crime, 4th edition, Pearson Prentice Hall, Upper Saddle River, New Jersey.
20. Major Gy. – Čudan A. (2015): Corruption, Trust and Integrity. In: Thematic proceedings of international significance „Archibald Reiss Days" Belgrade, 3-4 March 2015. (Ed. Bajagić). Academy of Criminalistic and Police Studies, Belgrade, III, pp. 91-99.
21. Mishra, A. (2005): Persistence of corruption: Some theoretical perspectives. World Development. 34(2) pp. 349–358.
22. Murai, B. – Ritzlné Kazimir, I. (2011): A nem megfigyelt gazdaság mérésének lehetőségei. Statisztikai Szemle, 89 (5) pp. 501-522.
23. Olken, B. A. (2009): Corruption perceptions vs. corruption reality. Journal of Public Economics. 93. pp. 950-964.
24. Payne, B. K. (2013): White-collar Crime. The Essentials. SAGE Publications
25. Persson, A. – Rothstein, B. – Teorell, J. (2010): The Failure of Anti-Corruption Policies: A Theoretical Mischaracterization of the Problem. QoG Working Paper Series, Gothenburg University of Gothenburg
26. Reinikka, R. – Svensson, J. (2005): Using microsurveys to measure and explain corruption. World Development. 34 (2) pp. 359–370.
27. Rothstein, B. (2011): The Quality of Government: Corruption, Social Trust, and Inequality in International Perspective. Chicago & London: The University of Chicago Press
28. Sherman, L. W. (1980): Three Models of Organizational Corruption in Agencies of Social Control. Social Problems 27 pp. 478–91.
29. Stump, I. – G. Fodor, G.(2008):Jó kormányzás és az állam 2008. A Századvég Alapítvány Politikai Barométere az ország állapotáról. Századvég, http://www.szazadveg.hu/files/kutatas/Jo-kormanyzas-es-az-allam-2008.pdf

30. Sutherland, E. H. (1983): The White Collar Crime. The uncut version. Yale University Press, New Haven (Firs ed: Chicago: University of Chicago Press, 1924)
31. Takács, I. – Csapodi, P. – Takács-György K. (2011): A korrupció, mint deviáns társadalmi attitűd. Pénzügyi Szemle 56 (1) pp. 26-42.
32. Treisman, D. (2000): The Causes of Corruption: A Cross-National Study. Journal of Public Economics 76 pp. 399–457.
33. Trevino, L. K. – Youngblood, S. A. (1990): Bad Apples in bad Barrels: A Causal Analysis of Ethical Decision-Making Behavior. Journal of Applied Psychology 75 pp. 378–85.
34. Wheeler, S. – Rothman, M. L. (1982): The Organization as Weapon in White-Collar Crime. Michigan Law Review 80 pp. 1403–1426.
35. World Bank (2000) Anticorruption in Transition. A Contribution to the Policy Debate, 1-101, Washington, D.C.

UDC: 343.352(4-664)

FORMS OF CORRUPTION IN TRANSITION STATES

Savo Milašinović, PhD
Ministry of Defense of Montenegro,
Department for Finance and Procurement
Vladan Martić, MA[1]
Mediteran University, Podgorica,
Faculty of Business and Tourism, Budva

Abstract: This paper will address the various forms of corruption in countries in transition, with an emphasis on the analysis of corruption in Montenegro. The aim is to distil the specific fund of knowledge on corruption, which, in addition to scientific, has a practical value because it can contribute to enhancing the fight against corruption. This practical aim of the paper stems from the fact that the widespread corruption in transition countries is large, that its manifestations are different and it is necessary to come to knowledge of the existing and new forms of corruption in Montenegro and the countries in transition - taking into account all previous scientific and theoretical knowledge, as well as that at the national and international level the most appropriate solutions are devised in order to effectively prevent and combat corruption in these countries. The observed specificity of corruption and forms of corruption are analyzed by means of an objective analysis of the existing data from various available sources that have been obtained from the empirical studies of corruption in the countries in transition and in Montenegro.

Keywords: corruption, transition, crime, anti-corruption measures, Montenegro.

INTRODUCTION

Corruption is rightly regarded as the companion of social development, which means that it has existed since the ancient period and it has manifested in various forms. Over time, it penetrated ever deeper into all the pores of the economy and the state apparatus, so in modern conditions it is one of the most serious obstacles to the realization of the rule of law and economic law. Corruption is seen as an evil that affects public administration and the functioning of the economic system, the foundations of free enterprise, the bad influence of democratic institutions and the society in general, the rule of law. Recent years underline the economic importance of the phenomenon of corruption, but it is defined as an attempt to extend for personal gain income from services, causing disruptive competition and increases inequality and insecurity actors in economic transactions.

In theory and practice, there are different definitions of corruption. According to one view, corruption is behavior that is a deviation from the normal discharge of public office for personal (or other: family, familial, private interest groups or cliques) and is a violation of norms to achieve personal interests. This includes activities such as bribery (accepting money or other benefits which affect the decision of a public authority), nepotism (patronage and

1 E-mail: vladan.martic@unimediteran.net.

applying ascribing or family criteria in deciding in the public sphere), and abuse of office for personal gain (the illegal use of public goods, services, or gratification). This is just one of the many definitions of corruption that are available in the literature.[2]

The diversity in defining the concept of corruption makes it difficult to identify the problem and prevents an adequate legislative approach to this phenomenon, and therefore appropriate measures for the detection, prevention and suppression. It is therefore justified to insist on the adoption of a unique and universal definition, which would also represent a means of communication and communication between the different entities that deal with this problem.

In this regard it should be noted that in defining corruption different approaches may apply. The first approach is the social, sociological aspect (broadly), the other with crime and criminal justice (more specific). There is a third approach to defining corruption, economic approach. In economic terms, corruption is irregular behaviour of public officials using their official position and authority in trying to gain undue advantage. Definitions belonging to a group of legalistic indicate certain corrupt behavior if it violates a formal standard or rule of conduct established by the political authorities, which is aimed at regulating the actions of public officials. On the other hand, the sociological definition of a group based on the public interest assumes that corruption is considered to include actions which ignore accountability to the public (civil) order and that are essentially incompatible with that order. The second subgroup of sociological definitions (definitions that are based on public opinion) is marked by the suggestion that "a certain procedure can be regarded as corruption when it is in accordance with that public opinion".[3]

The work will cover legal and economic approach to corruption. Most legal experts now agree that the term corruption implies systemic disorder that threatens the basis for the development of a democratic society, and the rule of law, which is why the concept of corruption should be understood in a broad sense and applied to all areas of human activity, both in the public and private sectors, as well as to all persons in the exercise of public functions or private gain of undue advantage associated with performing these functions. After defining corruption, in the second part of the paper we will discuss the prevalence of corruption in the world, especially in the countries in transition. In the third part of the article we will list and explain the forms of corruption in the developing countries. In the fourth part of this paper we will discuss corruption in Montenegro. The conclusion will summarize the forms of corruption in the countries in transition and the need to define adequate anti-corruption measures for their control, with special emphasis on combating corruption in Montenegro.

CORRUPTION IN TRANSITION STATES

Corruption exists in all countries in transition, but also in those that are in the post-transition period. It is well known that the countries of Central and Eastern Europe are very vulnerable to corruption. Numerous regional research in the countries of South Eastern and Eastern Europe show that their problems are similar, and that corruption is among the main problems in the region. This situation is not surprising, since corrupt practices as a rule, appear parallel to the impoverishment of public servants, the decomposition and transformation of political and economic systems, as well as during separation and decomposition of some socialist countries (Yugoslavia, Czechoslovakia, the Soviet Union), and then during the war and post-war period when changing political and government officials, etc. Similarly, globalization and global transition create favourable conditions for corruption around the world, especially in the developing countries.

2 Sačić Ž., Organizovani kriminal : metode suzbijanja, Informator, Zagreb, 2001, str.23.
3 Derenčinović D., Mit o korupciji, Nocci, Zagreb, 2001, str.41

The emergence and spread of corruption in these countries is the result of the accumulated economic problems, low incomes, falling living standards of a large part of the population and the like. In addition, as special factors contributing to the growth of corruption in the developing countries are usually the following: weak public administration, the absence of the rule of law, political institutions and poverty. These countries have inherited bureaucracy and lack many of the regulatory institutions necessary for the functioning of a modern state and economy, as well as many conditions necessary for accountability mechanisms function. On the other hand, the political and economic liberalization results in politicians exhibiting a wide range of pressures, many of which are corruption. This led to the distrust of citizens in the state, its institutions and the system as a whole.

In the Western Balkans, corruption is conditioned by the following general reasons that are universal (e.g., a high degree of regulations and administration in many segments of the society), or common to all developing countries (e.g., the dissolution of the previous system and its basic control mechanisms, transformation of ownership majorization relationships and individual and group interests, etc.). In addition, corruption in the region has contributed to the following conditions: inter-ethnic and inter-religious conflicts, various types of sanctions, erosion of individual, collective and socio-economic forces and capabilities, the inconsistency of behaviour and decision-making state organs at all levels, on the basis of party affiliation and other erosion of work, moral and other generally recognized social values.

It is known that in the countries in transition, insufficiently developed economic and legal systems directly affect the "overgrowth" of the traditional and the creation of new, previously unknown forms of corruption. It is believed that the lack of scientifically based and insufficiently developed practical economic system, that is harmonized with the laws governing economic, political and other conditions of social life, disregard for the situation in the domestic and global economy and individual industries and various forms of bureaucratic abuse legal (mostly discretionary) powers of managers and other organs of the state and other enterprises, in addition to other conditions indirectly affect the form and content of the forms of corruption in their formation or disappearance of the social scene.

Corruption in the countries in transition is present in all industries. It erodes the economic basis of society and causes distortions in the economic system, which is particularly evident in the countries in transition. The emergence of corruption and its various forms threaten almost all branches of economic and social life of a country. The complexity of the phenomenon of corruption stipulates that it occurs in both domestic and foreign trade, banking and insurance and in other economic branches. Corruption has not spared any economic activity and is especially noticeable in industry and construction.

CORRUPTION IN INDUSTRY AND CONSTRUCTION

Corruption phenomenon in industry appears in situations where it is difficult to get to the raw materials the consumption of which is a big. In addition, the conditions for corruption occur in the accumulated sales of goods, especially goods of poor quality. The production comes to get benefit without a legal basis, the most common abuse of the position of the person responsible and the appropriation of raw materials and finished products, which enables savings of material and higher production or inferior quality products. Here corruption activity follows the falsification of documents, which is often done in conjunction with the merchants.[4]

4 Bošković M., Aktuelni problemi suzbijanja korupcije : Prilog za izradu strategije suprostavljanja korupciji, Policijska akademija, Beograd, 2000, str.44

Various forms of corruption arise in the construction industry as well, starting with the irregular purchase of building land to contract higher prices than the market ones, which means the owner is in complicity with the responsible person, which leads to the division of unlawful profit which is the difference in price. Finally, various forms of corruption occur also in obtaining land for housing construction in expropriation of land, buildings, while adding onto the apartment buildings, and the like. It is well known that the permit for the construction and erection of temporary facilities is usually provided with a bribe or the party eligibility.

It is also known that in construction jobs it is often carried out as a part of major investment and other projects of very high values expressed in millions of euros. Regardless of the fact that this area is regulated by special rules of economy, economic, technical and technological standards (laws, standards, etc.), it is possible in this branch of economy to do various forms of corruption. When, on the basis of invitation for bids, terms of reference and other conditions, the realization of the investment program are carried out, then in order to obtain that job under the most favourable conditions, some people are recruited who are either employed by investors or have an impact on it. Namely, one that has helped a certain contractor to get the job receives a "meritorious award" as an adviser (consultant, external collaborator, etc.) or otherwise.

Some authors point to the fact that sometimes well-intentioned incentives for higher productivity are caused by abuse, especially in transport. In fact, it happens that persons transporting goods with separations such as concrete, stone and the like give the prize to the load and the number of tour operator to do during the day, but with the records does not conform records on the number and quantity of goods taken in separating what is actually delivered to the place where the material is to be installed. The situation is similar when the logs enter the building that incorporated the amount of material that does not match the real situation, but it seems in order to realize the difference through profit or acquiring illegal material benefit.

In the business of design organization, which is closely related to industry, construction and housing development, corruption is carried out usually in the form of so-called external cooperation. Specifically, the design company hired an external employee or an associate, who was able to override their "relationship" getting new business under the best conditions. It is normal that such an associate receives his part and a part of that or those persons who have helped in getting a job. Most often this provision is expressed in money, precious goods or services, conceals fictitious legal affairs and forgery of travel orders or other documents.

Corruption in the business of design and organization is manifested by individual engineers and technicians, self-made main projects. To make such projects "legitimate" it is resorted to acquaintances system and other connections in authorized designing companies that carry out verification of such projects. These services and activities are provided and a large fee in cash is received. People employed in the engineering firm, and prone to corruption, often deliberately refuse a job offered under various pretexts, and then offer the same job, or through a broker for the appropriate fee to another company. This behaviour conceals fictitious contract or work in a similar way.

CORRUPTION IN INTERNAL AND EXTERNAL TRADE

The sector of transport of goods and services, one might say, is the most vulnerable sector of economy and includes a number of very diverse forms of corruption. Internal trade (as well as external) is the focal point of carriers and corruption in the system of economic operations. Specifically, the Internal Trade manifestations of corruption occur in different conditions of

economy, such as temporary or permanent shortages of certain commodities, inflation, lack of financial resources, a fall or increase in production of certain products, disturbed payment transactions, a decline in demand or increase of supply of certain goods, interest rates, production or sale of outmoded or other types of slow moving and obsolete goods, inventory and similar circumstances.

In foreign trade, and in economic relations with foreign countries, there are different forms of corruption, malpractice and other socially-harmful behaviour of groups and individuals. Manifestations of corruption in this area are usually made in the export or import of goods and services, in the execution of capital projects abroad, in the exercise of special foreign trade activities in brokerage and representation of foreign companies, for joint ventures, long-term production, trade and scientific cooperation, foreign exchange operations, credit relations with foreign countries, transfer of technology and equipment in other areas of economic cooperation with foreign undertakings.

During the commission of criminal offenses in this area false documentation is made on the origin of goods, to provide benefits in time and manner of payment of the foreign partner, and thus outflow is performed of foreign exchange reserves of the country, bribing of responsible people in certain organizations and banks, as well as abuses by these persons. Characteristically, however, the various forms of corruption are hardest to discover and prove precisely in this area of economy. They are most often manifest in false reporting and declaration of quality, quality, type, value, origin and quantity of goods or services, import of outdated technology, environmentally harmful substances, poor quality of food and the like; export or import of goods without checking the creditworthiness of foreign companies which would allow, in the conception of a certain foreign trade activity, to the payment of foreign currency receivables and goods delivery by local companies; import, profitable export of goods or services by concluding harmful contracts (incomplete or imprecise objections) that allow a foreign company to fail in whole or in part its contractual obligations; unfair competition in all fields of economic relations with foreign countries; unauthorized agency and representation of foreign companies, etc.

These and similar manifestations are carried out, usually by means of corruption of certain officials. These are mainly persons employed in state bodies at the border or in other places where water is controlled or administrative procedures for import or export of goods and services (Customs, National Bank, the company control of goods, inspection, etc.). Signing damaging contracts is also one of the forms of criminal behavior in the area of business in the background of hiding corruption. This applies primarily to state-owned enterprises, where the broad powers of the management provide fertile ground for personal gain at the expense of the interests of companies and employees. The suspicion of the existence of practice corrupting the business of a company occurs when important decisions are made for the future, in a narrow circle of management behind closed doors. Doubt arises when contracts for the supply of goods or provision of services choose the offer of the same or lower quality and higher prices and so on.

CORRUPTION IN BANKS AND OTHER FINANCIAL INSTITUTIONS

It is known that certain forms of corruption affect business and the insurance companies, banks and other financial institutions. Various forms of abuse and corruption in the field of insurance manifest through the interface that is official. Responsible persons are employed in insurance companies with legal or physical entities that appear as users of the insurance

contract. Concealment of these abuses is done by falsifying documents such as records of insurance companies on the assessment of the damage, the official notes, bills of purchase or possession of certain things (car parts, etc.), accounts, specifications and other documents concerning the type, number and value of certain services, certificates about the report to the police and others.

The most common occurrence of abuses in the insurance organizations according to insurance companies is related to insurance of property without previously checking what is ensured. Such abuses, in particular contribute to the fact that these persons are awarded with the percentage of the value of insured property. It is often the case to ensure the assets prior to the date the insurance was destroyed or damaged, in which case the fee is based on insurance later shared between representatives of insurance companies and those provided by the property.

Corruption in banks is expressed mainly through the execution of the following criminal offenses: abuse of power, bribery, service, falsification of official documents and dereliction of duty. The crime of falsification of official documents accompanies almost all the enumerated offenses. Without falsifying financial documents, savings books, checks, bills of exchange, forms necessary for obtaining a loan for the payment and the payment of money, to switch from one account to another, and other prescribed documents, it is difficult to perform any of these offenses.

The literature rightly points only to the types of corruption that have special characteristics or are new forms of crime, uncovered in recent years: the abuse and illegality by issuing bills, abuses and illegalities in the credit relations with foreign countries, the appropriation of funds on the basis of citizens' savings, fraud and unlawfully appropriating while receiving their salaries through a savings or checking accounts, frauds with the forms of checks and misuse and misappropriation in exchange operations. Otherwise, it is certain that the area of banking business in the last two decades in particular favours a variety of abuses of the exercise of various illegal actions.[5] Such is the case with taking loans at below market rates. Many banks on various grounds provide loans at lower interest rates than the market. Those who receive such a loan generate great benefit, whereby the criteria for awarding loans is most commonly political criterion.

In terms of other financial institutions, the literature points to the fact that a large number of licensed exchange in banks, tourist organizations and other institutions established illegal business which has all the characteristics of crimes of abuse and other forms of corruption.[6]

CORRUPTION IN MONTENEGRO

As in most other transition countries, as well as in Montenegro, the beginning of transition to a market economy fundamentals could not be painless, because the transition further produces a number of problems in economy and, finally, a deep economic crisis. The economic crisis has had the effect of multiple and complex problems and opened up space for corruption in most industrial branches. Unavoidable consequences of transition processes and phenomena of corruption manifested in the form of disturbance in the functioning of state institutions and the worsening of social situation, falling living standards, a growing number of the poor, high unemployment rate, rising crime and especially corruption.

5 Antonić D. i dr.: *Korupcija u Srbiji,* Centar za liberalno-demokratske studije, Beograd, 2001.
6 Cotić D.: „Međunarodne preporuke i nacionalna iskustva u borbi protiv korupcije : aktivnosti UN, Saveta Evrope i iskustva pojedinih zemalja", *Privredni kriminal i korupcija* (zbornik radova), IKSI, Beograd, 2001, str.294-317.

There are many causes of corruption in Montenegro, which are the same as in other transition countries: the legacy of large, non-competitive bureaucracies, underdeveloped market economy, insufficient resources and a lack of democratic governance. However, there are also factors that are typical only for Montenegro and that we do not only speak about the causes and forms of corruption in the country, but also restricting other reforms such as the relatively brief experience of Montenegro as an independent state that is able to exercise its administrative authority over the entire society; small population which is statistically almost certain that the persons in key positions to be in each other's family or other connections; influence of tradition on social relations and the like. A series of these conditions has a direct impact on the political and economic corruption, which in many of its facets, presents the biggest challenge for Montenegro.

In Montenegro various forms of corruption appear in various economic sectors, where there is perceived good organization of the persons performing corruption offenses, and a number of difficulties in their detection and especially evidence. Corruption is particularly vulnerable area of foreign trade (exports and imports of goods, incorrect declaration of properties of the goods), domestic trade, particularly with the acquisition of various types of goods, construction (giving location and construction permits, land acquisition, demolition, etc.), the transformation of social ownership and the state capital and the economic and financial operations. Also, to some extent, corruption is present in the work of many agencies and institutions, such as inspection and customs authorities, the judiciary, police, administration, health, education and employment. In these bodies corruption is most often manifested in the form of commission of offenses giving and receiving bribes.[7]

Effective combat against all these forms of corruption is a very difficult task. There is not, or has never been a country that has completely curbed corruption. On the other hand, there is no doubt that this negative social phenomenon in Montenegro and most other countries has a far greater extent than official records show. In other words, corruption has become systemic and, in a sense, a constant for which, due to its resilience and adaptability to new social conditions, it must count on for a longer period of time.

CONCLUSION

In transition countries, corruption is present in all industries. It erodes the economic basis of society and causes distortions in the economic system, which is particularly evident in countries in transition.

In countries with developed democracy there is "small" administrative corruption, which some state officials work for their own account, or in which, possibly small groups work together, hiding from the law, colleagues and the investigative authorities. Type of corruption is the same, regardless of whether the corruption deals with the lowest government official or minister. It is important that this is a situation where individuals are placed outside the law in their own interest, and that the state is not inclined to their activities. This is common, so-called decentralized corruption. However, in the countries in transition corruption is taking place at a much higher level and is widespread in all economic activities. The most vulnerable in this respect are industry, construction, trade and financial sectors. It is similar in Montenegro, where corruption is also manifested in all economic activities. There are many causes of corruption in Montenegro, which are the same as in other transition countries: the legacy of large, non-competitive bureaucracies, underdeveloped market economy, insufficient resources and a lack of democratic governance.

7 Milašinović S.:"Implikacije korupcije na bezbjednost Crne Gore", Zadužbina Andrejević Beograd, 2013.

The fight against corruption is complex and requires the use of special means and methods, as well as finding the new ones. Therefore, it is necessary in the fight against corruption, principally in taking preventive measures, to rely on scientific experience in this area, and use the experience of those countries that have a lot of success in resolving the problem of corruption. In this sense, one of the most important tasks of all social forces in the fight against corruption is to strengthen social morality and public awareness of the harmfulness of corruption and the need to get involved in its prevention and suppression. In this sense, it is necessary to introduce education programs in educational institutions, and the media and professional associations have a significant role in this direction. This is because the fight against corruption at the same time is the fight for a system of moral values of a democratic society and the affirmation of honesty (integrity).

Finally, it is certain that civil society occupies the most important place in the prevention of corruption. Corruption cannot be fought only by state authorities because the suppression and prevention of corruption are subject to wider social agreement. Discussions in the media, at scientific conferences, public discussions and debates about this problem can greatly affect the public awareness about the problem of corruption and possible measures for its suppression. Political and economic reforms, legitimate authority, reform of state institutions, transparency and professionalism are prerequisites for creating an environment that does not tolerate corrupt practices.

REFERENCES

1. Antonić D. i dr.: *Korupcija u Srbiji,* Centar za liberalno-demokratske studije, Beograd, 2001.
2. Bošković M.: *Aktuelni problemi suzbijanja korupcije : prilog za izradu strategije suprotstavljanja korupcije*, Policijska akademija, Beograd, 2000.
3. Bošković M.: *Kriminološki leksikon*, Matica Srpska; Univerzitet u Novom Sadu, Novi Sad,1999.
4. Cotić D.: „Međunarodne preporuke i nacionalna iskustva u borbi protiv korupcije : aktivnosti UN, Saveta Evrope i iskustva pojedinih zemalja", *Privredni kriminal i korupcija* (zbornik radova), IKSI, Beograd, 2001, str.294-317.
5. Derečinović D.: *Mit o korupciji*, Nocci, Zagreb, 2001.
6. Milašinović S.:"Implikacije korupcije na bezbjednost Crne Gore", Zadužbina Andrejević Beograd, 2013.
7. Sačić Ž.: *Organizirani kriminal : metode suzbijanja*, Informator, Zagreb, 2001.
8. Šoškić N.: *Oblici i načini suzbijanja korupcije,* Akademska štampa, Zemun, 2004.
9. Tomanović M.: *Krivična dela korupcije* Kultura, Beograd, 1990.
10. Teofilović N.: „Politička korupcija i pranje novca", *Srpska politička misao*,br.1-4/2004, str.195-216.
11. Vukotić V. i dr.: *Sistem i korupcija,* Centar za ekonomska istraživanja Instituta društvenih nauka, Beograd, 2000.

UDC: 343.341(497.16)
323.285(497.6)

CONTEMPORARY ASPECTS OF TERRORISM IN MONTENEGRO

Damir Zejnilović, PhD[1]
Police Academy, Danilovgrad

Abstract: It is believed that there is a new kind of sickness ravening the world, the sickness which cannot be controlled. This combat against terrorism requires significant changes in startegy and tactics. Noone can predict the future development of terrorism with absolute certanity, because its explosion sets the foundation of modern civilisation, causing big concussions and conflicts in international relations.

In this paper the focus is on the most significant factors with a glimps on the state of terrorism in Montenegro, as well as the best ways to deal with it. We will analyse and explain social and historical development of terrorism, as well as psychological profile of terrorists. The paper presents a modest scientific and comprehensive framework which gives insight into the issue from which we can see the problems terrorism presents in today's society.

Keywords: terrorism, victims, profile, confront, analysis, strategy.

INTRODUCTION

When studying terrorism, its history, essence and content of important elements, one should bear in mind important elements that this negative activity has been present since the earliest times and will be present in the future. It is difficult to acquire precise data about terrorism in the world, because it is possible to statistically process and present only those phenomena which have already happened and took its tool, while terrorism prevention in practice has been difficult and it is difficult to acquire data on terrorist activities in the planning and preparation phase.

When researching terrorism-like phenomena one should start from general rules in theories of many scientific disciplines where a subject and method are positioned in mutual dependence. Terrorism as a negative social phenomenon which can be interpreted in many aspects, thanks to its multidimensionality, complexity and specificity.

New marks of terrorism are the following:

- Terrorism is a global phenomenon, because borders do not present a barrier;
- Terrorism is deadly, beacuse terrorists have changed their tactics towards theatrical violence aiming to alarm the public targeting places populated with civilians, trying hard to cause as many victims as possible;
- Destruction and professionalism in the coordination of actions;
- It is performed by civilians;
- It relies on the most up-to-date technology of contemporary civilisation;

1 E-mail: sefket56@t-com.me

- It is led by fanatical extremists who want to accomplish a goal completely destroying material resources and carnage;

- It is been led by hatred which determines the actions undertaken to achieve the goal.

It is doubtless that these changes require changes in a strategy and tactics of terrorism combat. No one can predict future development of terrorism with absolute certanity, because of its explosion in recent years, enormous increase in number of victims, material damage and chatastrophic consewuiences, it leaves behind, mine the foundations of modern civilisation, causing huge concussions and chatastrophical consequences in international relations.

IDEA AND DEFINITION OF TERRORISM

No one has managed to give a precise definition of terrorism the reason for that being its meaning changes along with social and historical context. The name terrorism is derived from a latin word terror – fear or horror. Terrorism means strategy of violence meant to cause fear in a particular segment of one society.[2] Terrorism represents use of violence against smaller number of people in order to intimidate larger group of people.[3] Terrorism represents a language used when we want people to pay attention to us.[4] Spceific teror which is linked to terrorism is what people remember.[5] Terrorism represents violence spread to cause fear, but also with the aim to direct other people in the direction wanted.[6] Terrorism comprises a series of preplanned activities of direct physical violence with aim to systematically cause panic and chaos, and which are performed within some political strategy.

All definitions of terrorism agree on the following:

- Terrorism is a strategy of violence aimed at achieving desired results by spreading fear and insecurity;

- It is based on illegal use of force or threat through continuous campaign or sporadic incidets;

- It represents planned use of violence to civilians and nonmilitary aims;

- Revolutionary terrorism is aimed to cause complete change in a country;

- It is characterised as undertaking concealed activities carefully planned in terms of goals, assets for their achievement, targets, attack and approach to the actions;

- Goal can be political, social, ideological or religious – without them terrorists would be considered deliquents and criminals;

- Terrorist actions are usually done by subnational groups, and sometimes even isolated individuals devoted to some goal;

- Important goal of these actions is to achieve as much publicity as possible.

Terrorism is different from many various forms and aims today. Not one aim, no matter how noble it is, cannot justify actions like these. Understanding cannot diminish horror of violence done to innocent people. Any right achived by murders and crippling of the innocent is not worth the price.

2 Bassiouni, M.Ch.: „Terrorism, Law Enforcement and the Mass media Problems. New York 1981.
3 Clutterbuck, R.: The Future of Political Violence, London: Memillan, Rusi, 1986.
4 De lillo, Don.: Mao II, New York: Penguin 1992.
5 Fairburn, G.: Revolutionary Guerrilla Warfare: London; Penguin 1974.
6 Fromcin, D.: The Strategy of Terrorism, Foreign Affairs vol. 53, no 4 D.C. 1975.

TERRORISM VICTIMS

Terrorism uses fear as a way to achieve special aims on purpose, in order to manipulate its victims, and thus wider population. Concern for personal safety affects more and more people. Airports, banks, industrial complexes, private and public institutions, even prisons, are endagered by terrorist activities.

Fears caused by terrorism and possibility to become its victim, are on the increase, apart from economic and social uncertanity.

There are different circumstances in which regular citizens can become victims of terrorist attacks and these are as various as the very causes of terrorism. Victims can be selective or random. Selective terrorism targets specific groups: police, judiciary, military or prison personnel etc. A "Random" terrorism does not chose victims, so anyone could become a victim – that is a method which causes the utmost fear in public.

Regardles of the aims and forms of terrorism, it comprises unpredictable, big force threatening to destroy victims. This experience is extremelly stressful and it causes the sense of utter helplessness.Terrorism affects victims in a way they cannot control their behaviour. Every difficult trauma causes physical and psychological consequences of a suffered shock. Most of the victims of terrorist attacks are random, and they can neither prevent nor control the events.[7]

The first phase of a victim's reaction to a terrorist act referrs to a current situation and experience suffered. The reaction is shock, disbelief, rejecting truth and hallucinating events. It is characterised by paralysis, icapability to move and rejecting sensual impressions. Then effects paralysis follows, so called „frozen fear" and unrealistic expectations of a victim to be rescued immediatelly. If rescue teams don't save a victim in the period of „initial adaptation", situation pressure and fear join and conquer majority of victims who fall into state of trauma psychological infantilism An individual loses the ability to function as an adult and starts the "adapted behavior" learnt in the early childhood. Victim identification with agressors becomes central topic named: "Stocholm syndrom".

Terrorists claim that innocent victims are not killed in their attacks. However, every human life is valuable – link to this value connects a terrorist, a victim and public in a triangle, which represents a characteristic of modern terrorism and makes negotiations possible. Terrorism can egsist only in places where and when there is vigilante violence of restricted form and space. If revenge is restricted, it is limitless in time. Perseverance of terrorists in vigilante intents are the hardest obstacle to those who have to plan defence from terrorism. People who were maltreated and who were unjustly punished seek for revenge.

When a terrorist attack happens, efforts to help have to be directed to softening its consequences. Care for victims is the basic principle when planning these interventions, but other factors which are political in nature and which depend on the situation itself, also influence decision making.[8] All the victims of violence and terrorism occupy special position. He or she usually represent a goverment attacked by terrorists and that's why they take hostage persons who represent these goverments. While defining strategies to defend from terrorist cruelty, one should consider that that value of human life is the most important postulate.

7 Thackrah, J.R.: op. cit. str. 293.
8 Dimitrijević, Vojin.: Savremeni oblici terorizma, časopis „Arhiva za pravne i društvene nauke", br. 4, Beograd, 1980., str. 21-25.

PSYCHOLOGY OF TERRORISM – TERRORISTS' BELIEFS

Activities of terrorist organisations are based upon subjective interpretation of reality which differs from the perception of goverments and societies they confront. Convincing systems can be drawn from numerous sources. Political and social enviroment in which it operates represents a set of resources. Both general and cultural factors are included in this category, and every member of the society adopts them sensibly in the age of maturity through socialization scheme and formal ideology. The origin of belief, can also be internal. Circumstances in which terrorists act are filled with stress and uncertanity, making individual beliefs relevant and adequate and terrorists are reluctant to change them so they persist upon them. Terrorists devote a lot of thinking to dehumanization and deification of their enemies.

Most left oriented revolutionary terrorists do not see themselves as agressors, but as victims. They perceive themselves as molested classes, workers and peasants, who are not able to help themselves. They think that they have a mission, that they are the ones devoted to the masses of unenlightened, who were chosen by the God and who, unlike a mass of people, recognize and accept a danger. Fight is their responsibility and obligation, and not a voluntary choice. The have high self-esteem, thinking of themselves as morally superior, emotional and dignified. They do not see themselves as terrorists, and consider this label is attributed to them by their enemies.[9]

The next two aspects of terrorist beliefs about the nature of conflict, are intriguing. The first represents a tendency to define combat in legalist sense. They don't see their acts as "murders" but as an execution after a trial. Their victims are perceived as "traitors". Other aspect of terrorist view about combat is their military presentation and symbolism. For terrorists, victims among "enemies" do not represent individuals, but enemy groups. Almost in all cases, they refuse to accept responsibility for violence they have done. Every activity in service of the goal can be interpreted as success. We cannot speak about failure if violence leads a terrorist closer to their goal.[10]

Social and political enviroment represents significant source of terrorist beliefs. Historical context plays a very important role. Ideology is a powerful weapon when it comes to influence – international factor which overcomes national boundaries, although it can be differently interpreted depending on the circumstances. Regarding ideologies, they were not made up by terrorists. Terrorists are oriented towards action itself rather than philosophy. Some analysts claim that many terrorists, are actually ambivalent, when it comes to violence. Internal conflict can explain why it is necessary that terrorists believe they have no choice and that the responsibility for the violence is of their enemyFor many terrorists denial of guilt is very important.

Once estabilished, convincing systems are resistant to changes. Terrorists rely exclusively on confidential intelligence. Certain types of image can help them avoid confronting complex value system present in political decisions. Model of "bad conviction" or "malicious intent" characteristic for their enemy, points to the fact that they will never have good intentions.[11] The importance of team work in terrorism has been known and accepted since the very begining. Tendency towards grouping and solidarity, present in primary groupations, lead towards rejecting differences in stances and internacionalization of standards and norms of the group. Organisation members must be completely devoted to group standards and must accept political belifs and system of social and psychological principles. However, fractions of terrorist organisations do not agree on the issue of what are the best ways to achieve common goals.

9 Kovačević, Sreten.: Terorizam i Jugoslavija, Arkade print, Beograd, 1992., str. 26.
10 D. Held, op. cit. str. 265.
11 Stajić, Ljubomir.: Osnovi bezbjednosti, Policijska akademija Beograd, 1994., str. 32.

TERRORISTS' CHARACTERISTICS

A terrorist is basically a sociopat, i.e. they do not feel guilt for killing or hurting innocent civilians who belong to security troups. It is hard to define the profile of a terrorist, because they differ in their values in terms of their goals and cultures they come from. Many theories define terrorists as individuals with clear and characteristic traits. Analysis of rural and urban terrorist gerilla groups shows that they are mostly unmarried men aged between 22 and 24, with a univeristy degree. Women terrorists are more likely to offer support than to be operative. They all mostly originate from rich, urban families from middle class, and many of them have a high social rank. Like their ancestors, many older terrorists have been educated for certain professions and did them before they have become terrorists.

Terrorists live in the world of phantasis and in the initial phases it can be said that they lead the war out of phantasy, and in the end they start beliving in their own propaganda. They want to promote changes by threat or spreading vilence which is the result of frustration – they feel that there is no other way to achieve the goal (weapon symbolises force and terrorists "cherish" it like a pet). The goal of terrorists is to draw the attention of the public so they can see their goals, to provoke Goverment's reaction in order to undermine their trust in public, as well as to promote fearful and alarming atmosphere. Terrorists' actions are the result of frustration and they feel that use of weapon is the best way to transmit a message. They function like an individual under stress.[12]

TERRORISM AS A GLOBAL SOURCE OF ENDANGERMENT

Terrorism is one of the most important and at the same time most dangerous threatening phenomena of our time. A superficial insight into concrete data undoubtedly proves this. Data show that over 600 different terrorist organisations (25% of them having more than a hundred members and some of them even hundreds of members, but according to american administration 29 are especially significant, having in mind they are labeled as international terrorist organisations). For example, between 1975. and 2000. there has been 12 thousand terrorist attacks (11860) in the world which is 480 attacks on an annual basis, (most of them in 1987-666 attacks, and least in 1998-274 attacks). We come to the conclusion that the world struggles with more than one attack per day. An important fact is that in recent years there has been an increase in the number of terrorist attacks. In these isolated attacks 40 thousand people have been killed.[13]

These data do not give a complete picture. We speak about isolated terrorist acts of international character. If we add up data from events who have terrorism and fight against it as a basis lasting for more than ten years in some parts of the world, the data are even more terrifying. More complete picture of consequences of terrorism can be seen if we add data about material damage caused by terrorist attacks. Although we do not have precise statistics, it is dobtless that a damage done in terrorist attacks, is estimated at tens of billions american dollars. Terrorism becomes endangering and more and more dangerous thanks to possiblities, scope and results. In contemporary conditions it is capable to cause much more damage to the world than it caused in the past. This is the reason why it becomes a global issue.

12 Đorđević, Obren.: Leksikon Bezbjednosti, Partizanska knjiga, Beograd, 1986., str. 24.
13 Combs, Cindy C.: Terrorism in the Twenty-Firs Century, New Yersey, 2003.

TERRORISM IN MONTENEGRO

Thanks to recent events in the world, as well as the fact that terrorism is a global and socially dangerous phenomenon, Montenegro which is a young country oriented towards integrations into international military-political organisations, attratcitve turist destination, hasn't been immune to potential terrorist threats.According to data of the Police Directorate for the period 1991 – 2015 Montenegro suffered two terrorist acts, i.e. the first one in 1991. and the second one in 2006. The terrorist attack from 1991. Happened in Herceg Novi, during a war in neighbouring area. In 1991. On 14th August four people came from Višegrad in Herceg Novi, two young men D.I and K.M, and two young women T.L and T.M. came with a clear attempt to perform a terrorist attack. Their final goals were to set up explosive devices in hotel Plaža where an international seminar was held at the time as well as military facilities at montenegrin coast. In order to perform the act, they brought some amount of military explosive in Montenegro as well as three clock works to activate the explosive. While setting up the device, D.I and K.M noticed a police patrol, so they decided to walk around the facility, and tried to move the clock work forward, because they hadn't planned interruption by the police. That moment was fatal for the two of them, because K.M caused short circuit while moving clock hands on the clock work and activated the device which kills them on the spot. Efficacious police action, girls T.L and T.M were deprived of freedom for providing logistics for this criminal act. They have been released later for the lack of evidence and the case was not proceesed.

The second terrorist attack in Montegro happened in 2006. in one of the biggest police actions at montengrin teritory, the officers of the Police Directorate using secret surveillance measures, approved by investigative judge of the Higher Court, and upon approval of Special prosecutor, learned that V.D. organised a criminal group whose member were: A.S, D.Lj, Đ.D, S.I, N.Lj, Đ.I, P.D, V.S, K.D, R.D, Z.B, M.I, Đ.D, Đ.Lj, V.K, i V.D, with a goal to perform terrorist acts and with an attempt to jeopardize Constitution or security in Montenegro, causing explosions and performing other dangerous actions.

In order to do the criminal plan which having been prepared for a longer time period the group bought and brought in Montenegro a huge amount of weaponry (wasps, machine guns, light machine guns, automatic guns, antitank mines, bombs, exsplosive devices and a huge amount of ammunition) with the help of people from Kosovo and Albania.

The members of terrorist group had allegedly hidden the weaponry and explosives in caves and other secluded places in Tuzi and Malesija, aiming to use them for the purpose of endangering Constitution or security of Montenegro on 10th September 2006. And all it on the basis of a terrorist plan having been prepared for a long period.

Using intellingence obtained from secret surveillance measures, search of apartments, houses and other premises and facilities owned by the organiser V.D. and other members of the group ws ordered.

On this occasion apart from weaponry the police found and seized a notebook in Albanian language which contained information about meetings and contacts of the group regarding purchase of weapons and drafting the terrorist plan for performing terrorist acts in Montenegro. The notebook was was examined in permises of the Police Directorate by an authorised police officer whose mother tongue was Albanian and the data showed that the plan had been to start a war. The importance of this notebook was it contained information that a truck full of weapons had already arraived in Montenegro. Also, while describing events in the notebook for the first time they found out official name of this illegal organisation "Movement for achiving rights of Albanians in Montenegro"–LRDSHMZ.

Higher Court in Podgorica sentenced seventeen-member group of Albanians to imprisonment to 51 year. All accused were sentenced for terrorism and armed rebellion who had been arrested in the police operation „Eagle's flight" were found guilty and sentenced to imprisonment from two to six and a half years. D.Lj. was sentenced to 6,5 years, Đ.D. to 5 years, A.Š. to 6, and the rother members to 2 to three and a half years.

Following the situation in the field and in the neighbourhood, and regarding the importance, as well as the fact that a lot of tourists visit Montenegro both during summer and winter season, the main segments being popular beaches (Budva, Ulcinj, Bar, Herceg Novi), ski resorts (Žabljak, Bjelasica etc.), as well as historic places frequently visited by tourists, it is important to direct the whole security system of Montenegro in that direction, in order to secure all human and material resources of the country. Taking into consideration the previous, and depending on the current situation, weather and soil conditions, facilities and similar particularities of Montenegro, as well as its tourist offer, i.e. current economic and political situation, depends the level of engagement of some elements of security system, or whether its engagement will be increased or decreased.

COMBAT AGAINST TERRORISM

Combat against crime enxompases more intervwined unarmed and armed contents–political, diplomatic, intelligence, security, educational, informative, educational, promotional, financial, military etc. Combat against terrorism is a complex of tuned offansive and defensive, unarmed and armed measures and activities undertaken by subjects and forces of a passive subject in the process of terrorism, aiming at preventing terrorists from attacking an immediate victim, and if they have started to use weapons, to efficaciously and completely neutralise its perpetrators in the shortest period possible, while simultaneously continuing breaking and destroying other elements and their organisational structure. Precondition for sucessful combat against terrorism are certain anti-terrorist principles, the most important being: prevention, comprehensiveness, centrality,offansiveness, informity, consistency, self-assesment and legality.

Antiterroist activities can be systematic and functional. Carriers of these activities are state institutions (parlament, goverments, minsitries etc.) and their task is to pass adequate legal framework and create conditions for successful combat against terrorism. Functional activities of antiterrorist system encompass unarmed and armed engagement of its subjects in antiterrorist fight, and in every of them systematic activity is a precedent.[14]

In order to be sucessful, each and every antiterrorist action must be well prepared and planned, and the preparation comprises planned and organised activities of a country and other subjects which are engaged in the operation in order to create most favourable conditions for performing combatant and noncombatant tasks in an operation.

The very start of a terrorist action is characterised by a timely and sudden begining of an antiterorist action, primarily towards armed groups of terrorists, in order to neutralise them completely or to such an extent that they will not be able to consolidate and resist in the following phase of the operation. Operation result must be capitulation, i.e. deprivation of freedom of terrorists or their physical anihilation.

14 Mijalkovski, Milan.: Terorizam i protivterroristička borba, Beograd, 2003., p. 63.

CONCLUSION

Despite explosion of terrorism on a global level, this phenomenon hasn't had a precise definition, not even acceptable one, until today. Some representatives of a goverment tend to link all violent activities done by their oponents, while nongoverment extremists claim the opossite, that they are victims of goverment terror. Imprecise nature of this term enables it to be implemented, i.e. that it can be used to label all the actions which "cause fear" in order to achieve certain goals. In teh most general sense it can be applied to some similar acts of violence like kidnapping and airplane hijacking, whom perpetrators haven't planned to develop into terror. Political sociologists think that unique universal definition, in principle cannot be made, because the very process of defining presents a part of wider constelation of ideological and political goals. Efforts in defining support the argument that perspectives change depending on where and when terrorists performed a terrorist act. Question of understanding terrorism is crucial for understanding this phenomenon, as well as for successful measures undertaken against it. For many observers a violent act is terrorism, while the others do not term violent activities done in a revolutionary context this way. Apparently similar acts of violence done by an individual, criminal or mentally ill person can be confusing.

Problems in determining sense and essence of terrorism stay undiscovered. Confronted with a lack of general and acceptable universal definition, each country can sign a declaration against terrorism, and not having to entirely perform undertaken obligations in practice. Countries which signed Convention on combat against terrorism, frequently define it in a different ways (double-standard principle). Terrorist activity within state borders is punished rigorously, while violent political activities happening at other states' borders are considered fanatical, or ignored. On the other hand, it is necessary to provide minimum of basic compliance with a main definition which determines terrorist activities as an intent to use violence ouside of a battle field, directed to civil society in order to achieve a certain political goal. Brutal attacks of this kind are considered barbaric and unacceptable form of behaviour. They wouldn't have anything in common with conventional war lead between opposing military forces whose characteristics, principles and limitations are strictly defined by Geneva and Hague conventions. They should be different from gerilla war, which is significantly different from terrorism, because its targets are military and not civilian.

In a fateful contrast towards the tendency for further development, greater freedom and equality, richness of life stiles, compulsion and power, crisis and social conflicts, discontinuity and civil wars emerge. Within this contrats the face of world may have changed as well. Contemporary society seems to be drifting in an enchanted circle – to total fiasco. Real writers of this history treat human lives in a completely soulless ways. There are a few types of actors that lead to terrorist actions which are harder to fulfill than political goals. A number of terrorist attacks and terrorists who do not represent a particular country is bigger and bigger. They come from the underground or religious sects, who are in a position to act as terrorists or to support terrorist groups and actions.

There are not deffensive means which could itself be enough against terrorism, but it has to be seen as a chronical disease, appearances of its symptoms need to be constantly monitored, and we should be ready to continually implement combined, preventive and represeive treatment with a focus on preventive measures.

REFERENCES

1. Babić, M. Marković, I.: Krivično pravo, Posebni dio, Banja Luka, 2005.
2. Bajagić, M.: Terorizam i međunarodno javno pravo, Bezbjednost, 2000.
3. Bassiouni, M. Ch.: „Terrorism, Law Enforcement and the Mass Media: Perspectives, Problems, proposals", The Journal of Criminal Law and Criminology, vol. 72. No 1, pp 1/51, New York, 1981.
4. Čejović, B.: Krivično pravo, Opšti i posebno dio, Beograd 2006.
5. Čejović, B.: Krivično pravo, Opšti i posebni dio, Beograd, 2006.
6. Cluterbuck, R.: The Future of Political Violence, London: Macmillan Rusi, 1986.
7. Combs, Cindy. C.: Terrorism in the Twenty First Century New Jersey 2003.
8. De Lillo, Don: Mao II, New York: Penguin, 1992.
9. Dimitrijević, V.: Savremeni oblici terorizma – Beograd, 1980.
10. Đorđević, O.: Leksikon bezbjednost,. Partizanska knjiga, Beograd, 1986.
11. Fairburn, G.: Revolutionary Guerrilla Warfare: The Countryside Version, London: Penguin, 1974.
12. Forca, B.: Prioritetna načela ratne vještine, Vojni informator, 2002.
13. Fromcin, D.: The Strategy of Terrorism", Foreign Affairs, vol 53, no 4, Washington, DC, 1975.
14. Gaćinović, R. Terorizam, Beograd, 2005.
15. Grupa autora, Strategija oružane borbe, Centar vojnih škola, 1998.
16. Hacker, F.J.: Contagion and attraction of Terror and Terrorism in Alehander. Yand Gleason, J.M Behavioral and Quantitative Perspectives on Terrorism, New York, Pergamon Press, 1981.
17. Held, D.: New Global Terrorism.
18. Jakovljević, D.: Terorizam sa gledišta krivičnog prava. Službeni list. SRJ. Beograd,1997.
19. Jović, S.: Specijalne snage, Montenegro Harvest, Podgorica,.1994.
20. Kaseze, A.: Međunarodno krivično pravo, Beogradski centar za ljudska prava, Beograd, 2005.
21. Kešetović, V.: Terorizam u savremenim uslovima, Banja Luka, 2002.
22. Kovačević, S. Terorizam i Jugoslavija, Arkade print, Beograd, 1992.
23. Latter, R.: Terrorism in tale 1990. Wilton Park Papers, no 44. London, HMSO.
24. Lazarević, Lj. Komentar KZ RS, Beograd, 2006.
25. Lazarević, Lj. Vučković, B. Vučković, V.: Komentar KZ CG. Cetinje. 2004
26. Leiteneberg, M.: Terrorism and Weapons of Mass Destruction countering terrorism through international Cooperation, our mayer mont vlanc, Italy, 2000.
27. Mijalkovski, M.:Terorizam i protivterrorističkа borba, Beograd, 2003.
28. Pašanski, M.: Savremene kamikaze, NIRO: književne novine, Beograd, 1987.
29. Petrović, D.: Moderni koncept terorizma, Kragujevac, 2007.
30. Pinjo, E.: Islamski terorizam htp.www.mm.cp.ba/printart 123 html.
31. Prečišćen tekst sa izmjenama i dopunama, Pravno istraživački centar, Beograd, 2003.
32. Rauccer,J.S.: Terrorism in its Sociological Aspects, Sociologia Internationaly. 1980.

33. Sederberg, PC: Global Terrorism: Problems of Challenge and Response, The New Global Terrorism, Chacacteristics Causes, Controls, 2003.
34. Sprinzak, E.: Samoubilački terorizam, Razumni fanatici, Vid. Htp:// www.bh dani. Com / arhiva/ 223/t22313. shtm.
35. St. John, P.: Air Piracy, Airport security and international terrorism winning the war against hijackers, New York, Quorum Books,1991.
36. Stajić, Lj.: Osnovi bezbjednosti, Policijska akademija, Beograd,1994.
37. Stojanović, Z.: Terorizam i srodna krivična djela, Beograd, 1998.
38. Suicide terrorism a global threat – Jane's Intelligence Review. Vid htp://www.janes.com/cecurity/international_security /news/ussole/jir 001020_1_n.shtml.
39. Thackrah, J.R. op.cit.
40. Tomaševski, K.: Izazov terorizma, Mladost, Beograd, 1983.
41. Tromp, H.V.: Terrorism and Political Violence, Brussels AFK/WK, 1979.
42. UN Convention for the Suppression of Financing Terrorism.
43. Wardlaw, G.: Political Terrorism Theory, Tactics and Counter Me assures Cambridge University Press, 1989.

UDC: 343.37(497.11)"2006/2010"
343.53(497.11)"2006/2010"

CRIMINAL OFFENCES AGAINST ECONOMY IN SERBIA IN PERIOD 2006-2010[1]

Dragan Cvetkovic, PhD
Ministry of the Interior of the Republic of Serbia,
Police Department Belgrade
Marija Micovic, MA
Academy of Criminalistic and Police Studies, Belgrade
Marta Tomic, MA[2]
Academy of Criminalistic and Police Studies, Belgrade

Abstract: Criminal offences against economy are undoubtedly one of the most current problems in the modern world. The problem of criminal offences against economy is becoming increasingly important as societies and their economies develop. In recent years it has been increasingly a negative social phenomenon that occurs as a serious impediment to both economic and social development. Data on criminal offences against economy, and especially the material consequences caused by taking into account the dark figure of this criminal phenomenon leave the worrisome impression. In fact, this type of crime has resulted in higher material damage, and often the perpetrators come from the higher social strata, public bodies or other political structures. Thus, the effects of criminal offences against economy on the society are multiple: direct damage to businesses, state budget, total industrial and economic developments and the country as a whole. It is therefore of utmost importance to look at the proper statistics for this criminal phenomenon and structure of behaviour that manifests itself through criminal offences against economy, followed by changes in their scope and manifestations. In this paper we have analysed the quantitative characteristics of criminal offences against economy, the relative share of criminal offences against economy in the mass of the entire crime, and their dynamics; then the structure of criminal offences against economy, which includes types of alleged conduct, their relative participation in criminal offences against economy, as well as their dynamics, and other special features. The criminal conduct, analysed on the basis of the available statistical data, which in addition to all has known limitations and disadvantages, however, represents an irreplaceable source of information on discovered crime.

Keywords: economy-related crime, problem, economic system, statistical data, analysis.

1 This paper is the result of the research on project: "Crime in Serbia and Instruments of State Response", which is financed and carried out by the Academy of Criminalistic and Police Studies, Belgrade – the cycle of scientific projects 2015-2019 and "Development of institutional capacities, standards and procedures for combatting organized crime and terrorism in the conditions of international integration" (No. 179045), funded by the Ministry of Education, Science and Technological Development of Republic of Serbia, and implemented by The Academy of Criminalistic and Police Studies.
2 e-mail: marta.tomic@kpa.edu.rs.

INTRODUCTION

Criminal offences against economy are a part of the overall criminality which is manifested through undertaking of illegal activities with the intent of acquiring illegal material benefit. This crime harms all societies and does it at all levels of development, but the problem is more difficult and more complex in the societies such as Serbia, which is on the road to European integration. Serbia is losing 3-5% of gross domestic product annually because of criminal offences against economy.

Due to their specificity, clearly different from other criminal phenomena, criminal offences against economy are the subject of interest of criminology, criminal policy and criminal law, both at international and national level. Criminal offences against economy are characterized by extreme variability of forms of expression, which is quite logical, because of their being conditioned by emerging socio-economic and political relations which inevitably create the conditions for change and the emergence of new forms. Therefore, there is a need for permanent monitoring of these issues such as changes to the law and compliance of definitions of criminal offences against economy and their content and characteristics in a given period of social development, both at the national and at the international level.

Criminal offences against economy are distinguished according to the general and specific characteristics, including: quantitative characteristics of criminal offences against economy (in volume or mass), the relative participation of criminal offences against economy in the total crime, their territorial distribution and dynamics. The structure of criminal offences against economy includes types of alleged conduct that we believe in criminal offences against economies, as well as their participation in the mass of criminal offences against economy.[3]

The analysis of crime statistics is very interesting and challenging because in some ways it is an attempt to come up with an answer to the question of how changes in crime trends result from deliberate social activities aimed at combating crime, and how the sum of individual circumstances is beyond the possible national impacts. Statistics in criminology is an ongoing challenge, especially when analysing the trend of crime in larger geographical units. Reviews and interpretations that are made on the basis of such analysis have their practical application because the developed countries on the basis of such findings invests a respectable financial and technical resources for the creation and implementation of programs for prevention and control of certain forms of crime for which the observed trend of increase or adverse changes were observed in the structure. And this work, given the available data sources, is relying on official statistical indicators of crime, and the data obtained from such an analysis can serve as indicators of the dynamics and structure of crime.

DEFINITION

A serious approach to criminal offences against economy has consequences for the social and economic relations in economy, and the possibility of action and the implementation of measures aimed at combating this phenomenon in contemporary society, starting from the definition of the concept of criminal offences against economy. In relation to understanding and defining the concept of criminal offences against economy, there is a variety of viewpoints, which vary not only from country to country, but also among different authors.

Given the complexity of the problem, it is essential that the definition reflects the essence of the concept, and explains exactly those criminal offences against economy that are real in

3 Pesic, V. (1977) The essential characteristics and economic condition of criminality in modern conditions, the Commercial Crime, IKSI, Belgrade, p. 9th

practice. Only such designation concept of criminal offences against economy can contribute and be successful in suppression and prevention of crime.

Accordingly, we have committed substantial efforts to get a single definition of criminal offences against economy in both the domestic theory and practice, as well as foreign. However, there is still no unified opinion on the concept of criminal offences against economy. Most likely, the reason for this international attitude is lack of a unified and integrated definition of criminal offences against economy, the variety of socio-economic and political systems. Within a single country in a legal and criminological literature there is no uniform definition of criminal offences against economy.

One of the most commonly cited definitions of criminal offences against economy comes from Edwina Sutherland, the President of the American Sociological Association, which for criminal offences against economy uses the term 'white collar'. This author defines this phenomenon as a "crime that occurs in the area of commercial operations and points out that its basic form are usually in machinations in connection with the purchase and sale of various actions, false expression condition and operations of individual corporations, false advertising of goods, business partners and bribery civil servants in order to achieve favorable business arrangements, misuse of funds, tax evasion, etc." The same author gives a new definition of crime, where white collar crime is a crime which is in the context of professional activities performed by persons of high social standing.[4]

The Council of Europe (2001) points to the strong correlation between organized crime and criminal offences against economy such as corruption, money laundering and fraud. The Council of Europe Report on organized crime for South East Europe for 2006 states that the difference between organized and criminal offences against economy is in the fact that "organized criminal groups established criminal enterprise to commit crimes even in legitimate jobs, while the economic benefits of crime legal enterprises for legal business, which is based on fraud, cartels, monopolies, and corruption in order to stay competitive in the market". According to the Council of Europe, criminal offences against economy have a negative effect which is beyond individual victims and material damage and it affects a large number of people, society and the country as a whole. It is regarded functioning of the national or international economy and caused a loss of trust and confidence in the economic system.[5]

Analysing the literature we can say that the authors largely agree on the concepts of criminal offences against economy as "all those illicit behaviours that attack the economic system, regardless of where it came from and attacks officials, companies, or even persons outside the business organizations or indirectly attacking the economic system". In a narrower sense under the criminal offences against economy we consider only criminal legal economic and financial offenses. That does not include economic offenses and misdemeanours. In a broader sense under the criminal offences against economy we consider a behaviour that competent national authority (court or other authority) qualifies as a punishable felony. Very often instead of the term criminal offences against economy, terms of financial, criminal offences against economy, criminal corporations and white collar crime are in use in literature.

The criminal justice system of the Republic of Serbia includes under the criminal offences against economy the categories of offenses defined by the Criminal Code of Republic of Serbia, such as money counterfeiting, money laundering, abuse of economy authorization, tax evasion, illicit production and trafficking, smuggling, causing bankruptcy, etc. Also, they include crimes against official duties (abuse of power, violation of the law by a judge, public

4 Sutherland, H. Edvin. (1940), *White-Collar Criminality*, American Sociological Review, February, p. 1-12.
5 *CARPO report (Development of reliable and functional policing systems, strengthening the fight against criminal activities and police co-operation) Council of Europe report on organized crime in 2006;*

prosecutor and his deputy, improper use of budgetary funds, illegal payments and billing, fraud, bribery, etc.) as well as criminal offenses under special set of laws.

Finally, on the basis of all the foregoing, the term criminal offences against economy can be defined as a crime that covers all crimes against the economy, business process, flows and activities, which cause consequences in the overall economic relations, either in the economic or non-economic, but the perpetrators were usually persons who have the authority of direct or indirect disposal of assets, as well as other powers in economic relations on the basis of which these relations are based, and which result in direct damage to the property, as well as jeopardizing economic relations.

CURRENT SITUATION AND DYNAMICS

For the analysis of quantitative characteristics of criminal offences against economy (scale or mass), we took the relative share of criminal offences against economy in the mass of the entire crime, and their dynamics, then the structure of criminal offences against economy, which includes the types of alleged conduct that we believe are in criminal offences against economies, the relative participation of each of them in the mass of criminal offences against economy as well as their dynamics, and other special features which represent an irreplaceable source of information on discovered crime. As a source of data, we take the annual statistical reports of the Ministry of Internal Affairs of the Republic of Serbia on reported crimes.

In Republic of Serbia, the period 2006–2010 registered by the police, there is total of 511,024 criminal offenses. More specifically, the average annual 102,204.8 crimes or every day there is 280.02 crimes, or every hour 11.66 crimes.

Table1: *Scope of criminal offences against economy reported in Republic of Serbia 2006-2010*

year	sum	sum	percent
1	2	3	4
2006.	98414	10499	10,46
2007.	104118	10697	10,09
2008.	105203	10481	9,54
2009.	102261	10889	10,30
2010.	100028	10451	9,92

When it comes to the scope of criminal offences against economy in the territory of the Republic of Serbia and its relative share in the total volume of crime, the above table shows that every year the participation of criminal offences against economy has not exceeded 11%.

In 2006 fraud was discovered in 10.499 cases. The amount of damage caused by these crimes is around 66 billion dinars, and material gain is about 64 billion dinars. Among the criminal offences against economy the prevalent offenses include the abuse of authorized person position (1943), falsification of official documents (1,459), fraud in business operations (985), and fraud (510). Criminal charges that have been filed with the competent prosecutors are 6,292 persons on suspicion of having committed offences against economy. Police arrested 200 persons who were charged with the commission of offenses in the field of criminal offences against economy.

During 2007, 10,679 criminal offences against economy were discovered and prosecuted in Serbia. Compared to the previous year it is an increase in the detection of criminal offences against economy by 2%. The amount of damage caused by crimes is around 24 billion dinars and material gain is about 20 billion dinars. Among these crimes the abuse of authorized person position (2214), falsification of official documents (1,630), fraud in business operations (1,290), embezzlement (391) are prevalent. Criminal charges that have been filed include 5,989 persons who have committed economic criminal offenses. 216 persons were arrested, who were charged by commission of offenses in the field of criminal offences against economy.

During 2008, 10.481 criminal offences against economies were discovered and prosecuted in Serbia, and criminal offences against economy recorded a decrease of 1.9% compared to the previous year. The amount of damage caused by the execution of these crimes was around 28 billion dinars and material gain was about 22 billion dinars. Among these crimes prevalent were the offenses of abuse of authorized person position – 2,764, falsification of official documents - 1,879, fraud in business operations - 1,398, embezzlement - 413, abuse of economy authorization - 305, which by their social hazards are serious criminal acts. Criminal charges that have been filed by prosecutors cover a total of 6,304 persons suspected of having committed criminal offences against economy. 175 persons were deprived of freedom, who were charged with the commission of offenses.

In 2009, 10,889 crimes were discovered and reported by prosecutors in Serbia, so that criminal offences against economy recorded an increase of 4% compared to the previous year. The amount of damage caused by execution of these crimes was around 15 billion dinars in material gain. Among these crimes prevalent offenses were the abuse of authorized person position – 2,580, falsification of official documents – 1,998, fraud in business operations - 1,419, embezzlement - 422, which by their social hazards are serious criminal offences against economy. Particularly good results have been achieved in combating all forms of corruption and abuse in banking business. Criminal charges that have been filed by the competent prosecutors cover a total of 6,492 persons suspected of having committed criminal offences against economy. 180 persons was deprived of freedom and charged for the commission of offenses.

In 2010, 10,451 crimes were discovered and prosecuted in Serbia, so that criminal offences against economy recorded a decrease of 3.5% compared to the previous year. The amount of damage caused by the execution of these crimes was around 22 billion dinars, and material gain was about 20 billion dinars. Among these crimes prevalent were the abuse of power - 2,783, followed by falsification of official documents - 1,938, fraud in business operations - 1,014, embezzlement - 425, abuse of economy authorization - 413, etc., which by their social hazards are serious criminal acts. 6,843 persons were reported to the prosecutors who were suspected of having committed criminal offences against economy. 155 persons were apprehended, who were charged for the commission of offenses in the field of criminal offences against economy.

The lowest number of crimes was recorded in 2006 and the most in 2008. In the analysed period compared to the total number of registered criminal offenses during the period (511,024 crimes) the share of crimes in the area of economic criminality on average moved to 10.06%. In the analysed period (2006-2010) significant fluctuations were not recorded in the field of criminal offences against economy, and we were short of growth and decline trends.

To gain an objective conclusion about the trend of crime in one country an analysis is required of its structure, namely the analysis of the percentage share of the most serious offenses in overall crime. When it comes to the structure of detected and reported criminal offences against economy from the data shown in the table below, we can see that abuse of authorized person position under Article 359 of the Criminal Code of the Republic of Serbia (hereinafter: CCRS) dominates in the structure of criminal offences against economy in the Republic

Serbia in the period 2006-2010. The minimum number of these offenses was in 2006 and the most of them in 2010, the abuse of authorized person position being 18.1% of total number reported criminal offences against economy in 2006, 20.7% in 2007, 26.3% in 2008, 23.7% in 2009 and 26.6% in 2010, i.e. about 23.1% on average for that period.

Falsification of official documents (Article 357 CCRS) follows, making 13.9% of the total number of criminal offences against economy in 2006, 15.2% in 2007, 18.1% in 2008, 18.3% in 2009 and 18.5% in 2010, or on average about 16.8% of the total number of criminal offences against economy in the observed five-year period. The minimum number of this offense was recorded in 2006 and 2009. Fraud (Article 208 CCRS) makes 9.4% of the total number of criminal offences against economy in 2006, 12.0% in 2007, 13 3% in 2008, 13.0% in 2009 and 9.7% in 2010, an average of 11.4% in relation to the total number of criminal offences against economy. The minimum number of this offense was recorded in 2006 and the maximum in 2009. Fraud (Article 364 of CCRS) seems to account for 4.5% of the total number of criminal offences against economy in 2006, 3.6% in 2007, 3.9% in 2008, 3.9% in 2009 and 4.1% in 2010, an average of 4.0% in relation to the total number in applicants of criminal offences against economy. The minimum number of this offense was recorded in 2007 and maximum in 2006.

The aforementioned crimes in the structure of the discovered and reported criminal offences against economy make over 55%. However, given the known crime factors of criminal offences against economy, with a high degree of probability it can be assumed that the structure of criminal offences against economy, which are in the sphere of "dark figure", looks much different.

Table 2: *Number of submitted crimes, reported persons, the amount of damages to property and property gain acquired in the field of economic crime in the territory of the Republic of Serbia in the period from 2006 to 2010*

year	Number of criminal charges	Number of reported persons	The number of persons deprived of freedom	Number of detainees	The amount of damages to property	Illicitly acquired assets
1	2	3	4	5	6	7
2006.	5.110	6.292	200	237	65.974.357.058	63.609.772.533
2007.	4.690	5.989	216	351	24.197.941.424	20.204.783.879
2008.	4.958	6.304	175	338	27.906.061.000	21.840.049.285
2009.	5.022	6.492	180	377	15.059.169.274	14.030.714.570
2010.	5.121	6.843	155	434	21.909.078.012	19.834.599.575

Table 3: *The structure of certain economic crime*[6]

year	Total economic crime												
		Art. 136	Art. 139	Art. 147	Art. 171p	Art. 242	Art. 245	Art. 247	Art. 248	Art. 251	Art. 254	Art. 255	
		Art. 234	Art. 238	Art. 243	Art. 208-p	Art. 359	Art. 361	Art. 363	Art. 357	Art. 364	Art. 367	Art. 368	Art. 231
2	3	4	5	6	7	8	9	10	11	12	13	14	15
2006.	10.499	78	246		985	1943	54	7	1459	510	54	27	12
2007.	10.697	59	239	277	1290	2214	60	21	1630	391	111	111	38
2008	10.481	30	305	284	1398	2764	66	64	1897	413	46	31	45
2009.	10.889	52	409	190	1419	2580	91	44	1998	422	148	120	34
2010.	10.451	31	413	279	1014	2783	31	9	1938	425	79	70	90

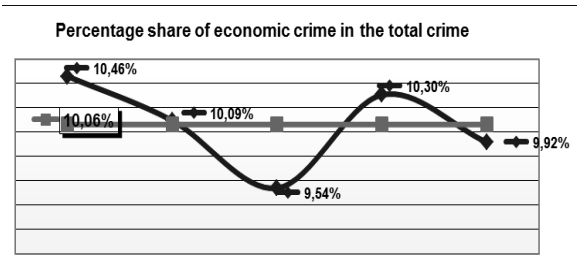


Chart 1: *Percentage share of economic crime in the total crime (2006-2010).*

It is indicative that in period 2006 to 2010 the participation of bribery in the structure of criminal offences against economy recorded a slight increase but not enough to take up a significant place in the overall structure of discovered criminal offences against economy. Receiving bribes in the structure of criminal offences against economy takes up less than 2% of total number. The minimum number of this offense was recorded in 2006 and 2009. The lowest number of this offense was recorded in 2008 and highest in 2009.

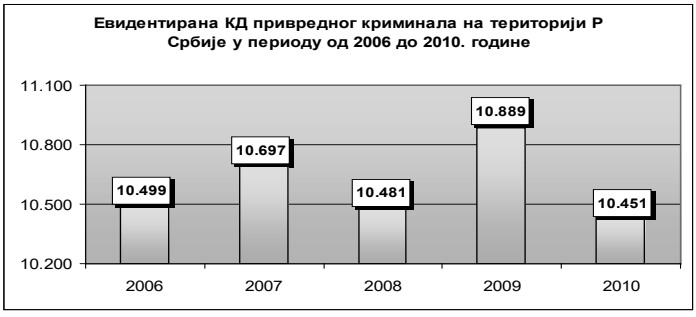


Chart 2: *The dynamics of economic crime in the period from 2006 to 2010.*

6 On May 06, 2005, new Criminal Code of the Republic of Serbia was adopted, according to which the articles of the law changed, but mostly in numerological terms of articles of the same changes, for instance the crime of misuse of official position used to be regulated by Article 242 CCRS, but under the new law, the articles of the CCRS 359, and so on. It should also be noted that the content of the above offenses is not pro Menu.

Chart 3: *Number of criminal charges in the period from 2006 to 2010.*

This period was characterized by the occurrence of money laundering in criminal offences against economy, which is a criminal offense (Art. 231 of CCRS) envisaged by the Criminal Code since 2006. This offense along with others in the field of criminal offences against economy attacks the economic system of the country and its essential part (monetary, fiscal, foreign exchange, foreign trade, etc.). The data in Table 3 show that the number of detected money laundering grew from year to year. Figure 7 shows that the least number was recorded in 2006 and most in 2010. These talks were marred by economic flows led to the expansion of economic and financial crime and the grey economy. Its growing caused a certain reaction by the prosecutors, which was reflected in a permanent increase in the number of detected crimes in the area of economic and financial crimes and their perpetrators, which grew from year to year in the period from 2006-2010, including also the criminal offense of money laundering as a derivative of the offense.

Balance and movement (dynamics) of criminal offences against economy can be seen if the statistical data relating to the detected and reported crimes can correct the factors that contribute to the execution of these crimes. Comparing both the estimated actual situation and what is stated in statistics, we can see the real number of 'dark figure', and get insight into the condition and dynamics of criminal offences against economy. When it comes to the structure of criminal offences against economy, it should be noted that the largest percentage was in just a few articles. These are the articles from the criminal Code of the Republic of Serbia and against the economy: the abuse of power in the economy, dereliction of business operations, illicit trade against property, etc.

The data shown in Table 2 related to property damage showed that in the analysed period, the total damage was about 155 billion, or on average about 33 billion. Minimum damage caused by criminal offences against economy was registered in 2009 (15 billion), and the highest in 2006 (about 66 billion).

Trend of property gains obtained (commission of criminal offences against economy in the period from 2006 to 2010). The overall benefit obtained through the commission of these offenses in the analysed period was about 140 billion, or an average of about 28 billion. Minimum property gain obtained by commission of criminal offences against economy was recorded in 2009 (14 billion pounds), and the highest in 2006 (about 63 billion).

With regard to the "latent clandestinely" criminal offences against economy, there is no doubt that there has been a lot more of these crimes than shown in the data presented in this paper. The concealed nature of this type of crime significantly hinders or prevents detection of criminal offences against economy and their perpetrators.[7]

7 The dark figure represents the difference between the actually officially recorded crimes. In criminology, dark figure indicates an unknown, i.e. undetected crimes. Estimated dark figure is usually

Unlike other crimes, such as crimes against life or body, or crimes against property in which there is a visible result of their perpetrator, in the field of criminal offences against economy work is cleverly disguised as the perpetrators act within their workplace, in which the commission of a criminal offense is approached with a pre-conceived plan. Similarly, the consequences arising from the commission of these offenses are not immediately visible and well-known. Due to these characteristics it is very difficult to determine the exact extent of this crime and the 'dark figure' is significantly higher than for other crimes. Thus, the mentioned data reflect more the activity of the detection body, primarily the police, but the real situation in the field of criminal offences against economy.

CONCLUSION

Based on these data (the data on crimes reported to the police or discovered by police), we can conclude that in the analysed period (2006-2010) the police registered 511,024 crimes. More specifically, the annual average was 102,204.8 respectively; every day 280.02 crimes, or 11.66 crimes per hour were detected. The lowest number of crimes was in 2006 and 2008.

In that period compared to the total number of registered crimes, the proportion of criminal offences against economy on average was 10.06%. Based on these data, it can also be concluded that criminal offences against economy range from 9.54% to 10.46% of the total crime number. However, this relatively low share of criminal offences against economy in relation to the total criminality is not a true indicator of social identification and the threat of criminal offences against economy. The analysed period shows that there was not recorded a significant fluctuations in the field of criminal offences against economy. The data show that the abuse of authorized person position (Article 359 of the Criminal Code of RS) dominates in the crime structure in Serbia for the period under consideration. There follows falsification of official documents (Article 357 CCRS). The aforementioned crimes occupy about 40% of all crimes in economy.

Overall, it shows that the largest percentage has only a few crimes. These are: abuse of power, illicit trade, and scam, abuse of authorized person position, official documents falsification, and embezzlement. The Ministry of Interior of the Republic of Serbia marks the fight against all forms of corruption as a priority in their work.

In the end, there is no doubt that there are considerably more offenses in the field of criminal offences against economy than was shown in the data presented here.

REFERENCES

1. Banović, B., Đokić. Z. (2007) *Ekonomsko-finansijski kriminal u tranziciji u Srbiji* u: Kriminalitet u tranziciji: fenomenologija, prevencija i državna reakcija, Institut za kriminološka i sociološka istraživanja, Beograd.
2. Becket, K., B. Western (2001) *Govering Social Marginality: Welfare, Incarceration, and Transformation of State Policy*, Punishment&Society, Vol. 3/1
3. Godišnji statistički izveštaji Ministarstva unutrašnjih poslova Republike Srbije

between 5 and 20. It is important to note that the dark figure is not the same as the gray figure of crime, which is a comprehensive number of reported crimes that subsequently are not accounted for, i.e. not establishing their offender. For more see: Cvetković, D. (2013) Design of indicators of economic efficiency of nonprofit organizations - with special emphasis on combating illicit investment income, (doctoral thesis), Faculty of Economics - University of Novi Sad; Kovačević J. (2014) Revision - part of a system of fight against economic crime, master thesis, University Singidunum.

4. Darlauf, S. N. Nagin, D. S. (2011) *Imprisonment and Crime: Can both be reduced*?, *Criminology &Public Policy,* Vol. 10/1.
5. Đurđević, Z.& Radović, N. (2012). *Kriminalistička operativa*. Kriminalističko-policijska akademija, Beograd.
6. Žarković,, M., Banović, B, Stupar, Lj., Ivanović, V.., 1997., *Kriminalistika*, VŠUP, Beograd.
7. Kovačević J. (2014) *Revizija – deo sistema borbe protiv privrednog kriminala*, master rad, Univerzitet Singidunum
8. Krivični zakonik RS, „Službeni glasnik RS", br.85/05.
9. Milosavljević, B., (1997) *Nauka o policiji*, Policijska akademija, Beograd,
10. Milutinović M. (1957) *Kriminalitet kao društvena pojava*, Savremena administracija, Beograd,
11. OEBS (2006) *Izveštaj o pranju novca i predikatnim krivičnim delima u Srbiji za 2000-2005.*
12. Pešić, V. (1977) *Bitne karakteristike i stanje privrednog kriminaliteta u Jugoslaviji u savremenim uslovima, Privredni kriminalitet*, IKSI, Beograd,
13. Sutherland, H.Edvin.,(1940) *White-Collar Criminality*, American Sociological Review, 1940. February,
14. Sutherland, H.Edvin.,(1945) *White-Collar Criminality. Crime?*, American Sociological Review, 1945. April,
15. Stojanović, Z. (2006) *Komentar Krivičnog zakonika*. Beograd: Službeni glasnik.
16. Tanzi, V. (1996). *Money Laundering and the International Financial System*", International Monetary Fund, Fiscal Affairs Department, Working Paper 96/55, Washington, D.C.
17. Teofilović, M., i Jelačić, M., (2006) *Sprečavanje, otkrivanje i dokazivanje krivičnih dela korupcije i pranje novca*, Policijska akademija, Beograd.
18. Cvetković, D., (2013) *Dizajniranje pokazatelja ekonomske efikasnosti neprofitnih organizacija – sa posebnim osvrtom na suzbijanje ulaganja nezakonito stečenih prihoda,* Ekonomski fakultet - Univerzitet Novi Sad.

UDC: 005.21:343.85
341.456

IDENTIFICATION OF PRIORITY THREATS AND CRIME AREAS AS A BASIS FOR A STRATEGIC POLICE PLAN

Vladimir Šebek, PhD[1]

Ministry of the Interior of the Republic of Serbia

Aleksandar Milošević[2]

Ministry of the Interior of the Republic of Serbia

Abstract: Planned preventive police work based on information analysis and identification of priority threats and crime areas represents a common societal goal. Starting from this notion, contemporary police organizations have developed a strategic plan of police work as a precondition for protection of fundamental freedoms and planned approach in dealing with priority security issues.The purpose of identifying priority threats and crime areas is a development of a strategic plan of police work and, in accordance with that, forming an adequate response of the police and other subjects.

In the light of absence of such a strategy in Serbia and lack of a clear course in targeted activities of the police, the aim of this paper is to draw attention to the necessity of identifying priority threats and crime areas and, in relation to that, developing an action plan. It is, conditionally speaking, a new concept that is novel in theory and even more in practice in our country, while it represents everyday practice as well as an anti-crime strategy in law enforcement agencies around the world.

For our purposes, it is of particular importance to identify attitudes of police officers about threats and crime areas that can be considered a priority.With that aim, empirical research was conducted which included the analysis of practice and perception of intelligence officers of the Department for criminal-intelligence activity and undercover agents, with regards to priority threats and crime areas in police work, with a tendency to define and present these areas, at least on this level. This particularly gains in importance because criminal intelligence activity, in theory, has a key role in the analysis and evaluation of trends in the state, movement and structure of crime in the whole country.

The obtained results will be compared in the discussion section with the current priority crime areas defined in the actual national strategic document (SOCTA of the Ministry of Interior of the Republic of Serbia) as well as in the strategic document of Europol Serious and Organized Crime Threat Assessment (SOCTA). The obtained results indicate an outstanding importance of intelligence officers' activities in detecting the most common security threats and crime areas as priorities for the work of police.

Keywords: strategic plan; police-intelligence model; targeted information gathering; analysis; Serious and Organised Crime Threat Assessment (SOCTA); Europol.

1 dr.vladimir.sebek@gmail.com
2 aleksandar.milosevic1977@gmail.com

INTRODUCTION TO STRATEGIC PLANNING

Police organizations, not only in Serbia but in countries around the world, focus their activities on addressing a wide range of problems relating to crimial activities. This approach in problem solving is recognized at the international level. Thus,there is a growing number of documents of Interpol, Europol and other organizations of the European Union that define priority threats and crime areas, in that way creating a strategic policy of police work. Strategic activity of criminal police is observed by Simonović as an integrated, comprehensive approach of a crime investigationdepartment in control/supression of certain types of crimes and improvement of its work with that aim, which is oriented towards: 1) optimization/improvement of the use of one's own resources and potential; 2) development of strategic partnerships with others (internal and external partnerships); 3) strategic action towards certain actors that are important for accomplishing strategic goals in control/supression of certain types of crimes; 4) detection, analysis, exploitation, appreciation and influence on specificities and tendencies inside criminal milieu, or social context, within the limits of power and authorization of criminal police (or giving proposals to persons in authority).[3]

Contemporary forms of crime, particularly serious and organized crime, pose a great threat to every country. Success in their supression, appropriate organization and implementation of legal instruments by which the number of criminal acts performed by foreign criminal groups can be reduced to a reasonable level directly depends on the development of objective, complete and timely threat assessment.[4]

The concept of police work led by criminal-intelligence (*Intelligence Led Policing – ILP*) has made a decisive impact on the increase of knowledge about a strategic approach in the police work in suppressing crime. By implementing this model of work, possibilities for the change in general understanding of criminal intelligence have opened up, demonstrating that analysis of information obtained from a wide range of sources can be used in directing activities against crime and help in more effective usage of resources. In that way, results of intelligence-led policing are becoming increasingly useful not only for tactical and operational purposes, but also for strategic planning.[5]

Definition of strategic priorities can be a very complex process, considering the fact that law enforcement agencies have a wide spectar of potential obligations ranging form traffic control to fighting terrorism.Practically, due to the obvious limitation of resources, these obligations can not be equally treated. Therefore, a priority needs to be assigned to each obligation that will influence the distribution of funds and the amount of organizational efforts that will be directed towards solving a concrete problem. Absence of a planned approach and reducing police activities to a routine work and without guidelines for work priorities will necessarily lead to improvization and disfunctional tendencies in everyday work.[6] In police organizations, creation and verification of *a strategic plan* is one of the most important activities.

Strategic plan represents a fundamental, key conceptual scientific-technical document that implies a systemic determination of ways, methods, tools and other necessary service resources (organizational, material-technical, human resources, etc.) with the purpose of ef-

3 **Simonović, B.**, *Research of the attitudes of the criminal investigation police officers MIA Serbia on strategic approach to crimecombating*, Bezbednost No. 1/2011, p. 8

4 **Đurđević, Z., Jokanović, S., Sovtić, S.**, "Methods of assessment of threat from serious and organized crime", Suprotstavljanje savremenim oblicima kriminaliteta – analiza stanja, evropski standard i mere za unapređenje (Tom I), Tara, 2015, p. 313

5 **Newburn, T. & Williamson, T. & Wright, A.,** (Edit.) (2007). *Handbook of Criminal Investigation*, Willan Publishing, Devon, pp. 220-221

6 More in the article: **Gottschalk, P., Gudmundsen, S.Y.**, *An empirical study of intelligence strategy implementation*, International Journal of Police Science & Management, Vol. 12, Number 1, pp. 55-67

fective and professional operationalization, i.e. acheiving those goals arising from the defined politics and priorities determined by users and providers of guidelines in accordance with the law.[7] In the past years, this activity was neither targeted nor scientific, and it was often subjected to attitudes, values and beliefs of officers. It is important to note that there is neither a unified plan for all crime areas and priorities nor a unique methodological criterion for accomplishing desired goals. Instead, there are "tools" that can be used in order to identify information needs of an agency and then create a policy and processes, which will make police work functional for every organization.[8]

A strategic plan is usually adopted for a specified period of time. Some experiences of the countries with developed criminal-intelligence functions show that such a plan is adopted for the period of one to two years, of course with periodical updating.

Identification of threats and crime areas that can be marked as priority areas, as can be concluded, is an important segment of public security. However, a strategically oriented criminal activity is only one piece of the security equation; the next critical step is that operation managers develop intervention that will stop or mitigate a threat. This actually means that police activities should be planned and oriented towards gathering necessary information, i.e. should rely more on the use of criminal-intelligence requirements as methods for defining a kind of "raw" information necessary to develop a quality strategic or tactical product. The need, or necessity, for gathering certain type of information leads to defining a notion of criminal-intelligence gap. *Criminal-intelligence gap* represents a shortage, i.e. lack of information needed for effective analysis. Analogous with that, *criminal-intelligence requirement* represents identification of information needed to fill a criminal-intelligence gap.[9]

At the time of conducting this research, the Ministry of Interior developed a strategic document *Serious and Organized Crime Threat Assessment*, creating in such a way a strategic picture of crime in Serbia without which it is hard to construct a strategy oriented towards the most serious security threats. However, a difficult process towards the development and implementation of the action plan for implementing this strategy remains, taking in consideration that more than a half of designed strategies have never been carried out.[10] This is at the same time an opportunity to compare the results of our research with the key national strategic document.

APPROACH TO THE PROBLEM OF RESEARCH

Before we engage in presenting the research methodology and results, the inevitable question arises regarding the extent to which a strategic approach and identification of priorities in police work are indeed present in everyday police practice in the Republic of Serbia. There is no doubt that we can partly agree with the opinion of scientific and professional community about the absence of a strategic approach in planning activity against criminal acts, but we as well cannot neglect efforts of the management the Ministry of Interior of the Republic of Serbia in the part concerning the development of serious and organized crime threat assessment, which enables the creation of the strategic plan and identification of work priorities. However, the implementation of adopted national assessments and strategies is slow failing to meet the envisaged deadlines for their realization.

7 **Masleša, R.**, *Kriminalistička strategija*, Univerzitet u Sarajevu – Fakultet kriminalističkih nauka, Sarajevo, 2006, p. 79
8 **Carter, L. D.**, *Low Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies – second edition*, p. 99
9 *Ibid*, p. 251
10 **Atkinson, H.**, *Strategy implementation: a role for the balanced scorecard?* Management Decision, *44*(10), 2006, 1441–1460.

It is quite understandable that some types of crime (especially serious and organized crime) cannot be successfully suppressed without a strategic approach in policing. Therefore, due to the lack of such strategic orientation, a whole range of problems emerge in work practice among which the following ones are the most important: nonfunctional distribution of resources and their unplanned spending; information deficit in areas that can be defined as priority areas; absence of indicators of the necessity of cooperation in areas that require cooperation with public-private partners; development of traditional (reactive) model of police work but also the most important every day *ad-hoc* practice and unbalance action of police officers.

Apart from the above mentioned practical problems, criminal scientific and technical literature is dominated by research from police practice and theoretical debate on which conclusions and proposals for strategic approach and identification of prioroty threats and areas of work suitable for our environment are made, without appropriate research performed, considering the fact that empirical research on attitudes of police officers about the most important crime areas and threats is practically non-existent. Only recently could the papers be found that are based on research conducted in the MOI of the Republic of Serbia. One of them, which is already mentioned in the introduction of this paper, is the paper written by Simonović on the topic of research on the attitudes of criminal police officers about strategic approach in crime suppression.[11]

Under the influence of the aforementioned considerations, the problem of research is further complicated by the fact that apart from the need for proclaimed and strategically oriented police work, the idea of directed (targeted) police activity is still not widely accepted by scientific, professional and general public in Serbia.

On the basis of what we have previously presented, the subject of this research is twofold: on the one hand, it is focused on measuring subjective estimation and awareness of police officers in the Service for criminal-intelligence activities and undercover agents about the way they detect, recognize and record certain categories of criminal activities in formal reports, which represent the basis for analysis and creation of final criminal-intelligence. These results represent a theoretical basis for developing a model of intelligence-led policing (ILP). On the other hand, the subject of research is directed towards identifying the presence of individual forms of criminal activities in the overall process of collecting and recording information, which presents the basis for generalization and identification of priority threats and crime areas. This actually means that the results of the analysis represent an objective basis for identification of the most important threats and crime areas and, in line with that, for determination of priorities. In this part, the role of managers of criminal-intelligence department becomes prominent in determining priorities in accordance with analyzed information.

METHODOLOGY

The research was conducted on the basis of materials, i.e. studies and analyses of the work of intelligence officers in the Department for criminal-intelligence operations, Service for criminal-intelligence activities and undercover agents of the MOI of RS. The research was performed in a way that the first step included a systematic and comprehensive processing of data in terms of operational reports by intelligence officers for the year 2015. In this way, a possibility was created to group the data and calculate frequencies and percents of observed variables using statistical methods (descriptive statistics). The results of processing quantitative data are presented textually, graphically and in tables.

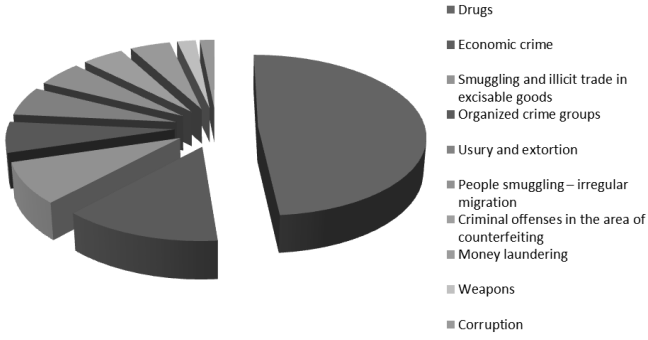
11 See: **Simonović, B.**, *Research of the attitudes of the criminal investigation police officers MIA Serbia on strategic approach to crimecombating*, Bezbednost No. 1/2011.

Certainly, this paper also took into account a good practice of developed police organizations around the world as well as methodology of identifying priority threats defined by the European strategic document SOCTA.

The target population of this research were all intelligence officers of the Department for criminal-intelligence activities, Service for criminal-intelligence activities and undercover agents. This means that according to the scope of the research subject, this research can be marked as complete (i.e. total), which implies a comprehensive analysis of all elements of the subject in the total time duration (bound by the calendar year of 2015) and the overall prevalence of the subject.Iin this way, sampling prevented subjectivity and bias in selection and ensured adequate use of statistical methods in order to provide a complete picture of identified priorities and criminal areas. There is no doubt that the research results should be verified and complemented on a larger sample and in further projects so as to make a thorough contribution to the improvement of police work in Serbia.

RESEARCH RESULTS

In this section, we will provide an overview of the actual state in certain areas of crime that can be labeled as priority areas on the basis of analysis. In the structure of the paper, presented crime areas will be ranked by the importance assigned to them by intelligence officers in the Service for criminal-intelligence activities and undercover agents, i.e. according to threats and risks in relation to the object of criminal-law protection. In that sense, presented crime areas are more than 70% present in criminal-intelligence reports. A general results overview is given in *Graph 1.*



Graph 1: *Identified priority crime areas*

Drugs – in the total structure, the most common crime area is organized trade and drug trafficking. To all appearances, this area (besides the dominant form) still represents one of the most dangerous and most profitable crime areas. In terms of proportionality, this area of crime, in its different forms, is present in over 36% of criminal-intelligence reports.

Economic crime - criminal offenses in this area are recorded in every tenth criminal-intelligence report. Observed through the amount of material damage, these acts can be categorized among top crime areas that damage the state budget.

Smuggling and illicit trade in excisable goods – in most cases it is tobacco and tobacco products, alcoholic beverages, coffee, oil and oil derivatives. As the results of this research showed, this type of crime is identified as a priority area in most of the security strategic documents as well as in the economic ones.

Organized crime groups – one of the most important activities of intelligence officers in the observed period was identification of a number of organized crime groups making up a significant portion of recorded OCG in Serbia.

Usury and extortion–due to the fact that extortion frequently accompanies usury, these crime areas are observed jointly. In the overall structure, they account for a little less than 5% of the content in the reports.

People smuggling – illegal migration – athough it has been a problem in our country for many years (primarily due to the geographic position), this area reached the largest proportions during 2015; therefore, primarily because of the operation of organized crime and terrorist groups, this area is defined as a priority.

Criminal offenses in the area of counterfeiting – criminal activity in the area of counterfeiting (which includes counterfeiting of money and documents), along with the above mentioned, can be classified as a priority. In the overall structure, there is almost equal number of contents of the reports with the subject of counterfeiting of money and documents.).

Money laundering – this type of crime represents accompanying activity of both economic and general crime (both organized crime and crime not marked as organized). Considering a high priority rank of these areas (economic crime, organized groups, drugs etc.), the importance of this crime area was significant for intelligence officers during 2015.

Weapons - after armed conflicts in the former Socialist Federal Republic of Yugoslavia, a large amount of weapons arrived in the territory of Serbia where it has been present on the illegal weapon market for nearly two decades. Actuality of this area of crime in the observed period was significant and after analysis it can be marked as a priority area.

Corruption – as an extremely socially dangerous area of crime, corruption is present in all spheres of society where besides the identified acts of corruption a significant number of them remain out of sight of the police and other subjects of formal control due to the undercover operation, i.e. dark figure.

DISCUSSION

After the research results are presented, some questions inevitably arise that will be suitable for a constructive discussion. Among them, we can select some of the most important ones: Why strategically oriented crime investigation activity is not grounded in our police organization? What is the reason that, although identified, serious and organized crime threats are not implemented as priorities in police work? Additionally, we cannot avoid discussion on the subject of experience of world police organizations in identification and implementation of priorities as targeted areas of police work. Moreover, we can express criticism through discussion that activities dealing with identification of priorities in police work and implementation of such work generally lack attention from academic and professional community. Therefore, this represents an excellent opportunity to motivate scientists and practitioners to make contribution to the development of strategic planning of police activities and a call for reconsidering the necessity of developing a new criminal discipline - policing strategy, which would, among other disciplines, bring improvement to crime science.

Certainly, detailed considerations and attempts to answer all the questions would exceede the planned scope of work and the aim that we want to achieve; thus, in the discussion section we will make a comparative review of the results of our researchwith an actual document at national strategic level - *Serious and organised crime threat assessment* of the Ministry of Interior of the RS,[12] as well as with the priorities of the European Union in the field of crime com-

12 Ministry of Internal Affairs, *Serious and Organised Crime Threat Assessment*, Belgrade, 01 No. 118/15-12, 31.12.2015 (www.mup.rs).

bating, defined in the strategic document of Europol *SOCTA* (*Serious and Organised Crime Threat Assessment*) [13] and *The European Agenda on Security.*[14]

The results are displayed in *Table 1* which provides an overview of the priorities defined in the key national document, as well as in the aforementioned European strategic documents, which can be simultaneously compared with identified priorities defined through the conducted empirical research. In the structure of the above mentioned documents, identified priorities and crime areas ad ranked according to the object of protection.

Table 1: *Priority review*[15]

SOCTA 2013	Interim SOCTA 2015[16]	SOCTA MOI of RS	Priority areas (research results)
Facilitation of illegal immigration; Trafficking in human beings; Counterfeit goods; Excise and MTIC fraud; Synthetic drugs; Cocaine and heroin; Illicit firearms trafficking; Organised property crime; Cybercrime	Counterfeit goods; Cybercrime; Facilitation of illegal immigration; Excise and MTIC fraud; Money laundering; Organised burglaries and thefts; Synthetic drugs; Trafficking in human beings	Drugs; People smuggling – irregular migration; Trafficking in human beings; Robbery; Usury and extortion; Vehicles; Illicit firearms trafficking; Economic crime; Money laundering; Corruption; Cybercrime; Organized crime grups	Drugs; Economic crime; Smuggling and illicit trade in excisable goods; Organized crime grups; Usury and extortion; People smuggling – irregular migration; Criminal offenses in the area of counterfeiting; Money laundering; Illicit firearms trafficking; Weapons; Corruption

Empirical study on which this paper is based presents an important segment of understaning the significance of criminal-intelligence activity for establishing a model of intelligence-led policing (ILP). From the empirical analysis, it can be consluded that activities of intelligence officers performed with the purpose of information gathering, although without strategaclly defined areas, for the most part are consistent with identified priority threats and crime areas defined in the strategic document *Serious and Organised Crime Threat Assessment* of the Ministry of Interior of RS. Thus, they are in line with the priorities of the European Union in the field of crime combating defined in the strategic document of Europol *SOCTA* (*Serious and Organised Crime Threat Assessment*) and *The European Agendaon Security.* This actually means that the quality of evaluation of the current SOCTA document, as well as the quality of the next threat assessment in the Republic of Serbia, will to a large extent depend on the quality and level of the implementation of ILP model of police work in our country.

CONCLUSION

Emphasis on the need to define key threats and crime areas in police work, which can be marked as priorities, is made by scientists and practitioners as well. At the same time, the implementation of such strategically oriented work in our country is, to put it mildly, slow. In

13*EU Serious and Organised Crime Threat Assessment*, European Police Office, 2013, p. 9

14 European Commission, *The European Agenda on Security*, Strasbourg, 28.04.2015. COM (2015), No. 185 Three priority areas: 1) *Tackling terrorism and preventing radicalisation*; 2) *Disrupting organised crime* 3) *Fighting cybercrime*.

15 Interpretation of the authors.

16 Council of the European Union, *Inerum SOCTA 2015: An update of Serious and Organised Crime in the EU*, Brussels, 16.03.2015. Документ доступан на адреси: http://www.statewatch.org/news/2015/mar/eu-europol-interim-SOCTA-7271-15.pdf (seen 10.01.2015.)

order to change the situation from the current (unfavorable) to the desired (favorable) state, it is necessary to adjust two interdependent processes: on the one hand, the analysis of security situation will allow proper detection of the most common security threats and crime areas as priorities for the police. From that moment on, the police will have a clearer mission that will be devoted to planning work and activities for solving or controlling of identified priorities. On the other hand, in the next phase there is a forthcoming action through a long-term strategic planning of measures to improve security, as well as action planning of projects and activities for solving specific individual and concrete security threats.

This research paper provides contribution to scientific literature, developing a research model of identifying priorites of policing in the context of theoretical defining on criminal-intelligence activity as a basis for intelligence-led policing. Indeed, it would be unreal that categorically defined priorities in intelligence-led policing are sufficient for a police organization to eradicate identified threats and crime areas only on that basis. This in fact means that such an approach is only one element of the equation of crime regression. The main finding from the empirical research is that criminal-intelligence activity plays an important role in strategically oriented work, so that it certainly serves as a "barometer" of the situation in the criminal environment, which we consider as a very positive fact.

REFERENCES

1. Atkinson, H., *Strategy implementation: a role for the balanced scorecard?* Management Decision, *44*(10), 2006.

2. Carter, L. D., *Low Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies – second edition*.

3. Council of the European Union, *Inerum SOCTA 2015: An update of Serious and Organised Crime in the EU*, Brussels, 16.03.2015.

4. EU Serious and Organised Crime Threat Assessment - SOCTA, European Police Office, 2013.

5. European Commission, *The European Agenda on Security*, Strasbourg, 28.04.2015. COM (2015), No 185.

6. Gottschalk, P., Gudmundsen, S.Y., *An empirical study of intelligence strategy implementation*, International Journal of Police Science & Management, Vol. 12, Number 1.

7. Newburn, T. & Williamson, T. & Wright, A., (Edit.) *Handbook of Criminal Investigation*, Willan Publishing, Devon, 2007.

8. Đurđević, Z., Jokanović, S., Sovtić, S., "Methods of assessment of threat from serious and organized crime", Suprotstavljanje savremenim oblicima kriminaliteta – analiza stanja, evropski standard ii mere za unapređenje (Tom I), Tara, 2015.

9. Masleša, R., *Kriminalistička strategija*, Univerzitet u Sarajevu – Fakultet kriminalističkih nauka, Sarajevo, 2006.

10. Ministry of Internal Affairs, *Serious and Organised Crime Threat Assessment*, Belgrade, 01 No 118/15-12, 31.12.2015.

11. Simonović, B., *Research of the attitudes of the criminal investigation police officers MIA Serbia on strategic approach to crimecombating*, Bezbednost No. 1/2011.

UDC: 343.91-053.6(497.7)
343.95:159.97(497.7)
343.238(497.7)

RECIDIVISM AND THE JUVENILE OFFENDER

Ivona Shushak, LLM[1]
University "St. Clement Ohridski", Faculty of Law, Kichevo

Abstract: Reducing juvenile crime is one of the biggest challenges which society is facing today. Juvenile crime is not as vast and unmanageable as the myths and misconceptions surrounding it suggest. The overwhelming majority of young people have no contact with criminal justice system. Of those who have contact in the form of a court appearance, some have only one appearance. A sizeable minority of juveniles has however several court appearances leading to conviction.

Knowledge regarding juvenile offenders and offending is limited. Very little is known about causes underlying juvenile engagement in crime. In addition, our knowledge about characteristics and dynamics of juvenile offending is incomplete. It comes to no surprise that attempts to tackle the problem have a high risk of failure.

The recidivism of juvenile offenders and their offending patterns are among the most important issues relating to juvenile crime. Overseas research supports the popular conception that adult criminals begin their careers in juvenile years. Therefore, understanding the factors underlying juvenile reoffending is crucial to the development of policies aimed at breaking the crime cycle, especially when recidivism among juveniles is unfortunately present in a large percentages, which this survey will show.

Methods: The paper will analyse data from a research of completed court cases in the area of Primary Court in Bitola, Republic of Macedonia. The focus will be on cases against persons who were under 18 years of age in the time of committing the crime (juveniles), in the period 2005–2014.

Keywords: juvenile offenders, recidivism, court cases.

INTRODUCTION

Since most ancient times, when life processes and relations between people were created in freedom, uniformity, equality without imposing one's will on others by force and violence, since the complete dependence of man on nature, up until now when the people are on their way to overcome and subdue the forces of nature and laws of people's needs, to discern contradictions of social development and find ways to resolve them, one of the central questions of human relations remains open. That is: how and in what way we can resolve contradictions between individual and social relations and interests as well as the goods and values created by people in order to protect themselves from the wrong and the illegal things. Community has always tried to force people to act in accordance with its social norms, mostly those people who attack social values, those with criminal behavior, those who do not comply with generally accepted values. This problem is even more complex when these problems happen among young people. Every society, also Macedonian one, is making efforts to preserve social values and tradition and of course to work for a perspective development and conditions for normal living of next generations.

1 E-mail: susak.ivona@gmail.com.

Crime among children[2] is a serious social problem. Young people more frequently engage in criminal activity and thus they accept criminal behaviour as a life choice. Time and time again it is emphasized that criminality in children deserves full attention from the perspective of rational policy for suppression of crime because many criminological analysis has scientifically verified the data that recidivists, multiple recidivists and delinquents, which constitute "the hard-core of every criminal population, resistant to all measures of penological treatment"[34], are recruited from the young delinquent population.[5] If this problem is recognized by the community within all its gravity, weight, danger, long-term consequences, etc. there is a bigger opportunity for the community to organize, mobilize and achieve greater efficiency in the prevention and control of this negative social phenomenon.

By emphasizing this problem, this paper will analyse the data from the survey of enforceable and executive judgments on the territory of the Basic Court in Bitola, Republic of Macedonia.[6] Focus of the research covered criminal cases regarding persons under 18 years that occurred between 2005 and 2014.

THE TERM RECIDIVISM AND TYPES OF RECIDIVISM

The term recidivism originates from the Latin word *recidive* (the repeating of or returning to criminal behaviour).[7] In theory, there are many different opinions about determining the term recidivism (repeating, return). There is no general and accepted definition, because this phenomenon is constituted by series of elements understood and treated differently. Among the various definitions that determine the term of recidivism, three can be distinguished: legal, criminological and penological.[8]

2Child- is a human being under the age of eighteen unless under the law that applies to the child, adulthood is attained earlier (Convention on the Rights of the Child, Art. 1)

- is any person under the age of 18 years (Law on justice for children, Art. 19).

3 E. Frey states that there is a necessary and proven relationship between crime in early age and recidivism, that about 20-25% of young people later become criminals "incorrigible recidivists", thus extending its chain of criminal activities during the entire life. (ОР Mag. Милутиновић, М., *Криминологија*, Савремена администрација, Београд, 1990, p. 246).

4 Singer,M., *Kriminologija – drugo izdanje*, Nakladni zavod Globus, Zagreb 1996, p. 193.

5There are many cases where case file of a child includes dozens even hundreds of crimes. (Јашовић, Ž., *Slobodno vreme i prestupničko ponašanje mladih*, Institut za kriminološka i sociološka istraživanja, Beograd, 1974, p. 50)

6Method of content analysis was applied in the research. Tabular views were used as a model of recording data, which due to the need to analyse the specified content were defined as categories and their codes were constructed. Next, the material was coded and was imported in the analytical table, which was processed with software solution SPSS. Content analysis also involved application of statistical method. (Мојановски ,Ц., *Методологија на безбедносните науки-истражувачка постапка*, Скопје, 2012).

7In fact, this term in criminology and criminal justice was taken from medicine and used by those criminological and criminal justice schools that try to explain aetiology of crime based on the inherited and acquired characteristics of the person, primarily used by anthropological and positivist school. (Арнаудовски, Љ., Чачева, В., *Повторот и повторниците (Повторот кај сторителите на кривични дела),* Институт за социолошки и политичко-правни истражувања, Скопје, 1979).

8 The necessity of defining recidivism through these three approaches also highlights the III International Congress on Criminology (London 1955). (Арнаудовски, Љ., *Криминологија*, 2-ри Август С- Штип, Скопје, 2007, p. 499). It is grounded that criminologists need more definitions for the recidivism to realize various goals. So, recidivist means: 1) a person who once committed an offence provided by law and was sentenced for it, or treated in some other way by the state, committed another crime – recidivist *stricto sensu* and 2) a person who once committed an offence provided by law or was officially treated differently, again engages in a criminal activity due to its "dangerous condition" – recidivist *lato sensu* (Skakavac, T., *Recidivism of juvenile offenders*, Doctoral dissertation, Niš, 2014, p. 34).

In *legal* terms, recidivism means the commission of an offence by a person who had already been sentenced for a committed crime. This definition starts from the existence of one or effective court decisions before the committed crime, which is the subject of trial proceedings; the nature of the offense, the time interval between the crimes committed and the number of committed crimes.[9] In legal terms, recidivism is important for the sentence and its weight. Article 39 of the Criminal Code of the Republic of Macedonia states that "when the court metes out punishment to the offender for a repetition of a crime, it specifically considers whether the previous case is of the same type as the new crime, whether the crimes were committed with the same motive and how much time has elapsed since the previous sentence, i.e. since served or pardoned sentence".[10] Thus the recidivists are a category of socially dangerous offenders, and that is exactly why they should be rigorously punished (because previously imposed sanctions proved ineffective, and with the new offence increased guilt is manifested).[11]

Unlike legal understanding, the criminological one starts from committing new criminal offence regardless of previous convictions.[12] It is important that a person has committed more than one offence of the same kind or a different offence.[13] Criminological definitions treat the term recidivism extensively because, besides the elements of criminal justice definition, they add elements that refer to the personality of the delinquent and dangerous condition of the criminal personality. This approach indicates the aetiological factors that conditioned this phenomenon, are those objective and subjective factors which are part of social measures system. This system is used for suppression of those conditions and depends of how much they were already realized..[14]

9 Within the criminal justice definition, there are general and special recidivism. General recidivism is when the offender commits another crime again after serving the sentence for previously committed one. Special recidivism is when the offender appears as a perpetrator of the same offence. (Singer, M., *Kriminologija – drugo izdanje*, Nakladni zavod Globus, Zagreb 1996, p. 250). Multiple recidivism is the heaviest kind of recidivism, which occurs when a person repeatedly commits crimes showing propensity and habit of committing the same or different crimes. (Konstantinović-Vilić, S. Nikolić-Ristanović, V. Kostić,M., *Kriminologija*, Prometej, Beograd, 2010, p. 232).

10 This way in which the Penal Code determines the place of recidivism as a criminal justice problem with all objective and subjective characteristics of the crime, should contribute to an appropriate choice of sentence which would achieve the objectives of punishment as well as the penal policy. (Арнаудовски, Љ., *Криминологија*, 2-ри Август С- Штип, Скопје, 2007, p. 501).

11 Сулејманов, З. *Македонска криминологија*, Графохартија, Скопје, 2000, p. 804.

12The existence of the offence does not have to be determined in a formal criminal procedure. A criminal offence can exist without conducting a criminal procedure or not completed due to procedural or other reasons.

13 Konstantinović-Vilić, S. Nikolić-Ristanović, V. Kostić, M., *Kriminologija*, Prometej, Beograd, 2010, p. 232.

14 According to criminological understanding, recidivists are divided into:

1) **Habitual delinquents** – They are not characterized by the number of committed offences, but by the tendency towards committing criminal offences. They are a kind of people which are not adapted to the living conditions, due to some internal (endogenous) reasons, and the external reasons only emphasize their flaw. (Сулејманов, З. *Македонска криминологија*, Графохартија, Скопје 2000, p. 804) They start committing criminal offences in their childhood, and that activity becomes an integral part of their life. (Singer, M., *Kriminologija – drugo izdanje*, Nakladni zavod Globus, Zagreb, 1996, p. 251).

2) **Professional delinquents** in a criminological sense, are considered those offenders of crimes who have some characteristics similar to the habitual delinquents, but there is rationalization of criminal orientation among them, i.e. they commit criminal acts as a profession, occupation, source of income, and out of greed, which is not evident among habitual delinquents. (Бошковић, М., *Криминологија,* Правни факултет, Нови Сад, 2007, p. 249).

3) Potential delinquents also have a propensity for criminal behaviour, but they differ from habitual delinquents by the origin of that propensity. Unlike habitual delinquents whose criminal behaviour is mostly conditioned by external factors, among the potential delinquents dominate factors associated with personality, bio-psychological conditions (usually inherited). (Konstantinović-Vilić, S. Nikolić-Ristanović, V. Kostić, M., *Kriminologija*, Prometej, Beograd, 2010, p. 234).

It is also believed that criminology must necessarily deal with those offenders who never appeared in court or similar institutions, as undiscovered criminality has its own problems which are very important for understanding the phenomenon itself and for taking the appropriate measures of criminal policy.[15]

Penological definition creates small number of problems compared to the elements that determine the term recidivist. Recidivist in penological sense is a person who has committed a crime for which he/she was sentenced to an effective sentence – prison, which he/she has served fully or partially, and committed a crime again, for which he/she has been sentenced to prison and appeared in a penitentiary correctional facility for its execution.[16] Penological analysis of recidivism suggests two possible factors: *inadequate social reaction* – improper choice of sanction or inappropriate rehabilitation treatment and re-socialization process, also treatment in penitentiary and correctional institutions that do not match the personality of the perpetrator. Another penological factor of recidivism is *inadequate treatment*, which consists in the limited possibility even inability of the delinquent to be involved in the community after the served sentence.[17]

RECIDIVISM AMONG CHILDREN

Recidivism among children, as a special category of criminal behaviour, draws the attention of criminal justice and criminological theory, especially the social response to prevent and suppress this phenomenon. Recidivism and repeated commission of crimes especially among children as subjects primarily is considered as an indicator that their behaviour is not a product of accidental circumstances and has not an episodic character, but that it is conditioned on the permanent and profound subjective and objective factors.[18]

Recognizing the scope and pace of recidivism among children, all three notional definitions can be used in principle: criminal justice, criminological and penological. However, from the perspective of the special criminal justice status of the child, penological and legal aspects of recidivism showed a relatively limited and insufficient understanding of the true extent of this phenomenon.

It is known that Macedonia has a quite developed system of criminal sanctions for children. But in this system there is only one specific punitive measure – main sentence, prison for children. This sentence applies only and exclusively to criminally responsible children above 16 years of age, because strict conditions for its application are provided.[19] If one takes into account the fact that this punishment is imposed for a period of one to ten years, and the other fact is that the child has only two wears to become an adult (18 years of age), then it is clear that penological recidivism among children can occur only as an exception.[20]

15 Бошковић, М., *Криминологија,* Правни факултет, Нови Сад, 2007, p. 509.
16 Арнаудовски, Љ., *Криминологија*, 2-ри Август С- Штип, Скопје, 2007, p. 501.
17 There are two types of classifications of delinquents in penological terms: *internal and external classification*. External classification is based on sex, age, health status, type of imposed sanction, while internal classification is made within the institution for execution of sanctions. However, it is undisputed that both internal and external classification are interconnected and serve the same purpose – to achieve successful re-socialization by using adequate treatment.
18 Factors related to personality (biological and psychological) and social factors.
19 Prison sentence for children can be imposed on a criminally responsible child over the age of 16 who has committed a criminal offence prohibited by law, for which it is sentenced to prison five years or more, if the offense is committed in particular aggravating circumstances and with a high degree of criminal responsibility of the child, and thus it is not justified to impose an educational measure. (*Law on Justice for Children* – "Official Gazette of RM" No.148 of 29/10/2013, the Article 51 paragraph 2).
20 Јашовић, Ж., *Криминологија малолетничке делинквенције*, Naučna knjiga, Београд, 1991, p. 137.

It is the same with legal approach. In legal approach of recidivism, those persons who have already committed an offence and were punished, and then committed another crime which is punishable, are considered as recidivists. According to this criterion, as recidivists would be treated exclusively children who have been sentenced to prison for children. Thus all other children on which other sanctions are imposed would not be considered as recidivists. Without going into details for disassembling this issue, given the importance of recidivism for criminality among children, we believe that as recidivism should be considered any new commission of an offence by a child, who was imposed any of the criminal sanctions provided for children with a final court decision,[21] which would give recidivism criminological dimensions.[22]

This term of recidivism would not be sufficient for child offenders. Nearly a third of reported children are not brought to justice because at the time of committing the crime they were not 14 years old.[23] Among young delinquents, 14–18 years old, principle of opportunity of criminal prosecution is applied significantly more often.[24] Hence, when children recidivists are considered only those on which any sanctions were imposed, given the attention in studying such phenomenon, we would completely avoid the above-mentioned offenders. Thus, approach to recidivism among children is broadly understood and certainly has some shortcomings, but in any case it should be taken into account in the interpretation of data.

RESULTS OF THE CONDUCTED RESEARCH

Analysis of the types, structure and intensity of criminal recidivism among children provides insight into, on the one hand, the importance of this socially negative phenomenon, and on the other hand, into the success of the implemented measures and the degree of involvement of social subjects in charge for prevention of criminality.

The research which covered 330 final and enforceable criminal judgments, imposed on the territory of the Basic Court in Bitola, for the period 2005–2014 from a total of 476 offenders, 56.1% or 267 of them are repeat offenders.[25] The most numerous are those convicted two or more times, and that can be confirmed by taking into account the fact that in 19.6% of cases the procedure is suspended in expedience[26], a solution which applies when the Chamber finds

21 The following **corrective measures** can be imposed on a child offender: a) disciplinary measures: rebuke or referral to a centre for children, b) measures of intensified supervision: by parents or guardian, foster family or by the centre and c) institutional measures: sending to an educational institution or correctional centre. When it comes to sentencing a child, 16 to 18 years old, the following **sentences** may be imposed: a) imprisonment for children, b) a fine, c) prohibition for driving a motor vehicle of a certain type and category d) expulsion of a foreigner from the country. And **the alternative measures** for the criminally responsible children over the age of 16 are probation with protective supervision, conditional termination of criminal proceedings and community work. (*Law on Justice for Children* – "Official Gazette of RM" No.148 of 29/10/2013, Art. 34, 37, 50, 60).

22 Арнаудовски, Љ., *Малолетничко престапништво-предавања одржани на постдипломските студии во учебната 1979/80 и 1980/81*, НИО Студенски збор Скопје, 1981, p. 68.

23 If a child, who at the time of execution of the act (which in criminal law is considered as criminal act or offence), **was not 14 years old, a sanction under this Law cannot be applied**. (*Law on Justice for Children* – "Official Gazette of RM" No.148 of 29/10/2013, Art. 20).

24 Normally, the competent authorities and institutions **do not initiate court proceedings** for action of a child over 14 years of age, which by law is a criminal act or offence, in order to avoid the harmful impact on the child. (*Law on Justice for Children* – "Official Gazette of RM" No.148 of 29/10/2013, Article 17, paragraph 1).

25 From the criminological point of view, when talking about recidivism among children, very significant is the fact that as a rule they are judged for a series of crimes, and a series of crimes in criminological sense can be treated as recidivism. This means that the recidivism among children is shown in smaller relations than the number of offenses. (Арнаудовски, Љ., *Малолетничко престапништво-предавања одржани на постдипломските студии во учебната 1979/80 и 1980/81*, НИО Студенски збор Скопје, 1981, p. 70).

26 *Law on Justice for Children* – "Official Gazette of RM" of 29/10/2013, No. 148, Art. 129, paragraph 2).

that it is not compliant to impose a sanction on the child, because the child is serving another, earlier imposed sanction.[27]

When studying the aetiology of criminality among children recidivists, the fact that these individuals begin their criminal activity very early should especially be taken into consideration. It points out that the primary causes of criminality should be looked in socioeconomic situation of the repeat offenders at the time of their childhood, and in this regard socioeconomic status of their parents, their material and other possibilities, and human relationships necessary to achieve social, economic and psychological function, are particularly important. Poor material conditions in which they live (poverty, misery, unemployment) and the unfavourable family environment where they form their personalities[28] (incomplete families or dysfunctional families)[29] should also be mentioned. Namely, in the study of repeat offenders, 43.7% were from incomplete (deficient) families.[30] If one analyses a little deeper, it would become evident that only 26.1% of the rest 57.3% who have complete families, have satisfactory economic situation.[31] This shows that there is a link between the intensity of recidivism and completeness of the family of the child.[32]

Again, in the context of previously presented situation, usually property crime offenders (mostly children) are recidivists. Recidivists are 79% of the offenders who have committed grand theft; usually it is special recidivism, i.e. repetition of the same offence. A high degree of recidivism from 66 to 80% of the offenders appears among those who have committed robbery, plain theft, violence and stealing a motor vehicle. This confirms the existence of high impact between the type of crime and recidivism.[33]

Termination of criminal proceedings dominates among other sanctions for recidivists, in the analysed cases (because that certain person is serving another imposed sanction (32.6% of the cases). Increased supervision by a parent/guardian is present in 14% of cases, and its more vigorous version is accompanied by assistance and inspection by social agency, in 22.5% of the analysed cases. The sanction strengthened supervision by the Centre for social work is also often applied, in 17.8% of the cases. In 3.8% of the institutional measures with most rigorous treatment, reference to educational correctional home is imposed, and in a small percentage of only 0.2%-0.7% of the total number of sanctions, referring to an educational institution and a

27 Recent studies show that a minority, about 5% of registered delinquents (so-called intensive delinquents) commit 35-50% of all discovered offenses committed by children, mainly property offenses. (Кајзер, Г., *Криминологија-вовед во основите*, Александрија, Скопје 1996, p. 273).

28 Šilović emphasized the relationship between family circumstances and the deviation in children's behaviour more than half a century ago. "If we explore the reasons for moral neglect of habitual delinquents or repeat offenders, we would make sure that those reasons lie primarily in the neglected good parenting, bad example in the family and the dusty society which the family interacts with." (Singer,M., *Kriminologija – drugo izdanje*, Nakladni zavod Globus, Zagreb, 1996, p. 223).

29 Among other risk factors we could mention the low level of education, the use of inadequate treatment during the execution of the sentence, the impact of the prison environment, inadequate gradual treatment, and of course the very characteristics of a young person, but from the perspective of the research data at our disposal, we wouldn't rely on them in this particular situation.

30 15.38% live on social welfare, 14.6% do not have any assets, 26.1% have low income, and 17.7% have extremely difficult financial situation.

31Incomplete families are those where the parents are divorced, one parent is deceased, a parent is in penitentiary institution or has been imposed for compulsory admission and involuntary treatment in a medical institution, and children are raised by grandmother/grandfather/aunts etc., or are orphans.

32 Pearson's $x^2 = 20.320$, and has a theoretical value of 15.5073 (confidence level of 0.05). Since the empirical value is greater than the theoretical, it can be concluded that the null hypothesis is not accepted (intensity of connection exists).

33 Pearson's $x^2 = 69.156$, and has a theoretical value of 35.1725 (confidence level of 0.05). Since the empirical value is greater than the theoretical, it can be concluded that the null hypothesis is not accepted (intensity of connection exists). The Cramer V coefficient shows the same (0.425 – moderate correlation).

children's prison. Data about criminal policy applied towards recidivists, followed by applied sanctions, partially directs that recidivism is a facultative aggravating circumstance.

On the other hand, it is a general impression that, according to the "rigour", punishing recidivists is not significantly different from punishing primary young delinquents. Therefore, the whole stand, and whether recidivism is suppressed and prevented by more severe punishment, can be questioned. However, this question requires further monitoring and study not only from the perspective of its phenomenological features, but also from the perspective of funds from the "repressive nature" which would be applied for its prevention and suppression.

All these elements point out the complexity of this problem and the need for more intensive, organized and scientifically established engagement of all authorities, organizations and institutions in preventing and combating this phenomenon.

CONCLUSION

Recidivism is one of the hardest and most painful issues criminological science has ever discussed. It does not matter if it is defined as a simple repetition of the criminal act, or as repeating the criminal act after a legally effective judgment. All authors agree that this phenomenon among the young delinquent population is serious, present, and alarming especially since multiple recidivists and habitual delinquents become the category of persons, which constitute "the hard-core of every criminal population, resistant to all measures of penological treatment."[34]

In this study, with all the obvious deficiencies of the methodology of monitoring and processing of indicators of recidivism, aforementioned results clearly show that recidivism in the Republic of Macedonia is very common. According to the presented data, about half of the children who appear in court are recidivists, and most of them "are responsible" for two or more cases. Children who come from dysfunctional families with low socioeconomic status are the dominant ones, thus as a real epilogue to this situation are frequent property crime offenses, especially severe theft that is the most common crime among children.

This indicates the strength of micro and macro crime factors and impact on the specific personality of the young persons on the one hand, and inefficiency of state authorities and institutions in the suppression of crime on the other. The need of developing and implementing the necessary programs in the society focused on eliminating the factors that drive children towards recidivism derives from these general premises about the aetiology of recidivism.

REFERENCES

1. Арнаудовски, Љ., *Криминологија*, 2-ри Август С- Штип, Скопје, 2007.
2. Арнаудовски, Љ., *Малолетничко престапништво-предавања одржани на постдипломските студии во учебната 1979/80 и 1980/81*, НИО Студенски збор Скопје, 1981.
3. Арнаудовски, Љ., Чачева, В., *Повторот и повторниците (Повторот кај сторителите на кривични дела),*Институт за социолошки и политичко-правни истражувања, Скопје, 1979.
4. Бошковић, М., *Криминологија,* Правни факултет, Нови Сад, 2007.
5. Convention on the Right of the Child, General Assembly resolution 44/25, 20.11.1990.

34 Singer, M., *Kriminologija – drugo izdanje*, Nakladni zavod Globus, Zagreb, 1996, p. 193.

6. Законот за правда на децата – *"Службен весник на РМ" бр.148 од 29/10/2013.*
7. Jašović, Ž., *Slobodno vreme i prestupničko ponašanje mladih*, Institut za kriminološka i sociološka istraživanja, Beograd, 1974.
8. Јашовић, Ж., *Криминологија малолетничке делинквенције*, Naučna knjiga, Београд, 1991.
9. Кајзер, Г., *Криминологија-вовед во основите*, Александрија, Скопје, 1996.
10. Konstantinović-Vilić, S. Nikolić-Ristanović, V. Kostić, M., *Kriminologija*, Prometej, Beograd, 2010.
11. Мојановски, Ц., *Методологија на безбедносните науки-истражувачка постапка*, Скопје, 2012.
12. Мојановски, Ц., *Аналитички постапки*, Скопје, 2013.
13. Милутиновић, М., *Криминологија*, Савремена администрација, Београд, 1990.
14. Singer, M., *Kriminologija – drugo izdanje*, Nakladni zavod Globus, Zagreb 1996.
15. Сулејманов, З. *Македонска криминологија*, Графохартија, Скопје, 2000.
16. Skakavac, T., *Recidivism of juvenile offenders*, Doctoral dissertation, Niš, 2014.

UDC: 347.775(497.11)
343.534(497.11)

PROTECTION OF TRADE SECRETS

Dragana Anđelković Glišović[1]
Academy of Criminalistic and Police Studies, Belgrade
Zoran Milanović, MSc
Academy of Criminalistic and Police Studies, Belgrade

"The secret is best kept when we ourselves, for any reason, are not interested in discovering or publishing it; and it is the safest with the person who keeps it unconsciously. Otherwise, man can never be sure that he could keep a secret until the end, either his own or someone else's. It may be kept for years and years, and then revealed at one moment that reverses all the years of loyalty and silence."

Ivo Andric

Abstract: The Law on the Protection of Trade Secret, as unique general law, regulates the legal basis for the protection of trade secret against unfair competition in all areas of economic activities and scientific research. Concrete measures, that the holder of certain information would take in order to preserve confidentiality, depend primarily on the type, importance and value of the information. Examples include the signing of non-disclosure agreements, marking as confidential, limiting access to documents or files which contain confidential information, and the like. The balance between the need for confidentiality and liability is the result of good non-disclosure agreement that contributes to the success of the business cooperation between the Contracting Parties. In this paper, the authors deal with the conceptual definition of trade secret by analyzing the content of the legislation which protects it and by considering the conditions that must be fulfilled in order to treat a piece information as a trade secret. Without the intention to question the adoption of the said law, numerous scientific, professional and political opinions are given on the topic of regulation and protection of trade secret in Serbia. We will use the case of the "most expensive Serbian secrets" as a reminder of how signed contracts are broken or unfulfilled, promises are violated, requests are ignored, unnecessary funds are allocated and competitive advantage in the market is lost, all due to the loss of important business information.

Keywords: trade secret, protection of trade secret, data / information, non-disclosure agreement.

INTRODUCTION

After the adoption of general regulation – The Law on Protection of trade secret (hereinafter: the Law)[2], key terms and legal institutes relevant to the issue of the protection of trade secret were defined, which are applicable to the widest range of activities in the field of commercial operations, as well as in science and technology. The legal protection of classified in-

1 draganakrag@yahoo.com
2 "*Official Gazette of the Republic of Serbia*", number 72/2011

formation was provided, legally controlled by a natural or a legal person against all acts of unfair competition, and the sanction of any act of unauthorized disclosure, acquisition or use of confidential information was made possible. Former specific regulations treated the issue of trade secret in the strictest sense, and exclusively in the domain that referred to the specific case of legal regulation.[3]

The legislator wanted the Law to make sense from the standpoint of legal certainty and opportunity for businesses, for all those who invest in means of research, development and possession of information that can bring economic benefits and development.Therefore, fair competition is encouraged in a variety of business, economic and scientific-research activities, as well as the investment and operation of foreign business entities in the Republic of Serbia.[4]

Trade secret, as intellectual property, has property value, not ownership characteristics, starting from the confidentiality principle and unfair competition prevention. Institute of unfair competition is primarily aimed at preserving business ethics and morality, and above all is involved in a commercial behavior between competitors on the market. Confidential information that is protected by trade secret often becomes the subject of various acts of unfair competition, such as industrial espionage, breach of contract, abuse of confidence, etc. The Law introduced the possibility of taking a legal action for violation of trade secret, and also a strict penal policy for acting contrary to the Law, in terms of responsibility for economic offenses.

Serbian legal system is criticized for having imprecise procedure for classification of certain information marked with "secret". Fluctuation of personnel also passes on information on the economic, commercial, technological, technical and other potentials of competitors, business connections and weak points of persons who participate in the economy.

Through internal acts, business entities decide on the conservation, protection and conceptual definitions of data, information and knowledge that will be treated as confidential. Today, the conclusion of non-disclosure agreements is the most successful method for the protection of business critical data. They may be concluded for a longer period of time, depending on the will of the parties. The author of the paper takes as an example a non-disclosure agreement between the Government of the Republic of Serbia and Italian company "FIAT Chrysler Automobiles (FCA)".

The "most expensive Serbian secret" (affair "Satellite", affair "bulletproof", concession for the construction of the road Horgos-Pozega ...) will serve us as a reminder of some procedures and the agreements that Serbia concluded under the veil of secrecy, and which today attract the attention of the public and whose justification is suspected.

3 The Law on Companies *("Official Gazette RS"*, nos. 36/2011, 99/2011, 83/2014 – law and 5/2015, art. 72) regulates the trade secret in the field of company business; The issue of confidentiality of information which is conveyed to the authorities in the process of obtaining the marketing authorization is regulated by the Law on Medicines and Medical Devices *("Official Gazette RS"*, nos. 30/2010, art. 207) Data Secrecy Law ("Official Gazette RS", no. 104/2009) governs a single system of the classification and protection of secret data which are of interest for the national security and public safety, defence, internal and foreign affairs of the Republic of Serbia; as well as, article 50 of the Law on Trade ("Official Gazette RS", no. 53/2010); as well as, Article 50 of the Law on Trade stipulates that, among other things, the acquisition, use and disclosure of trade secrets without the consent of the holder, in aggravation of their position in the market is considered unfair competition.

4 During the negotiations for accession to the WTO, member states have indicated to Serbia the need to adopt common rules that would regulate the issue of protection of trade secret, under the Art. 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) and the provisions of the Paris Convention for the Protection of Industrial Property (Art. 10bis). Pursuant to Article 1.2 of the TRIPS Agreement, trade secret falls into the category of intellectual property rights, and Article 39 of the TRIPS Agreement provides that member states are obliged to provide remedies for the protection of trade secrets in their national legislation, in order to ensure effective protection against unfair competition under Article 10bis of the Paris Convention.

THE DEFINITION OF TRADE SECRET

Broadly speaking, any confidential business information which provides an enterprise a competitive edge may be considered a trade secret (i.e.*Coca-Cola* [5]formula, chemical formula in the pharmaceutical industry, etc.), because it is a secret and the holder of it takes efforts that are reasonable under the circumstances to maintain its secrecy.[6]

Thus, the subject matter of trade secret includes manufacturing processes, the results of market research, consumer profiles, financial information, business plans, lists of suppliers and clients, price lists, business strategies, advertising strategies, designs, drawings, architectural designs, etc. Similarly, test data and test results are a special type of classified information that a person, who controls them by law, must disclose when asking for the approval for the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical compounds. In addition, all creations that are protected by intellectual property rights incorporate a trade secret that has a commercial value, and as such should be protected against all acts of unfair competition.

As regards determination of the data that represent the trade secret in theory and in regulations, two concepts can be spotted. According to the subjective concept, the so-called *Theory of the will*, the holder of the trade secret determines what would be considered a trade secret by a statement of his will (included in documents of the trade secret holder, such as the corporation act or statute). According to the objective concept, the so-called *Theory of interest*, the scope of trade secret is determined regardless the will of the holder, considering the generally recognized economic interest which is defined by law and other regulations. Theoretically, there is a clear view that both concepts should be taken into account when determing trade secret.

5 Pharmacist John Pemberton, trying to find a cure for headache, made the most popular soft drink in the world, whose composition is strictly guarded trade secret. Company director Emesto Woodruff arranged a loan in New York Bank (1919), and as collateral he provided hand printed formula "Coca-Cola". When the loan was repaid (1925), the formula was placed in an underground bank safe "Sun Trust" in Atlanta, and at the 125th anniversary of existence, it was transferred to the museum "World of Coca-Cola". The company strongly adheres to the rule that only two employees in the "Coca-Cola" know the secret formula at the same time. Besides the fact their names are kept secret, they are strictly forbidden to travel by the same plane.
According to the company data, residents of more than 200 countries purchase 1.7 billion of 'Coca-Cola" products every day. This is certainly a brand that has a huge economic advantage over the competition. Its success is based on reputation, marketing and consumer confidence. Furthermore, the advantage is the fact that the owners did not apply for a patent at the very beginning, but protected their interests by a trade secret, with the possibility to experiment in revealing of the secret formula to a certain extent. The development of technology enables laboratories to obtain the syrup using reverse engineering process, however, the perfect mixture of ingredients, method of heat or any other treatment is known only to the "Coca-Cola".
Following The Code of Business Conduct, employees are bound to keep confidential and other non-public information. They can be shared within the company only if required by the needs of business. Outside the company they remain trade secret even after an employee leaves the company. This includes any information that the company has not disclosed or made publicly available, such as information on employees, inventions, contracts, strategic and business plans, major changes related to the management, the launch of new products, technical specifications, pricing, proposals, financial data, product costs, etc. In addition, the company respects information from other companies that are not public in the same manner it values and protects its own data, and does not seek competitive advantage in illegal and unethical practices. See more: Code of Business Conduct, http://www.coca-colahellenic.rs/.
6 Article 4 of the Law: Trade secret, under this law, is any piece of information that may have economic value, because it is not generally known and it is not available to third parties that could have economic gains from its use or disclosure and is protected by the holder with appropriate measures in accordance with the law, policy, contractual obligations or appropriate standards for the purpose of maintaining its secrecy and whose disclosure to a third party could cause damage to the holder of a trade secret.

In The Law on Companies ("RS Official Gazette", Nos. 36/2011, 99/2011 from 1.2.2012) Article 72, a trade secret is defined as any piece of information the disclosure of which to a third party could cause damage to a company, as well as any piece of information that may have economic value because it is not generally known and is not readily available to third parties that could have economic gains from its use or disclosure and is protected by the company concerned with appropriate safeguards for the purpose of maintaining its secrecy.[7]

The information may be production-related, technical, technological, financial or commercial information, a study, a research result or a document, formula, drawing, item, method, procedure, notification or instruction of internal nature, etc.

It was considered in theory whether the so-called negative information may receive protection as well (e.g. information on errors that should be avoided, a certain procedure that does not give the expected results or dead-ends encountered in research).[8] However, given the fact that any piece of information which meets the necessary legal conditions may be considered a trade secret, it can be negative information of course, regarding their importance in maintaining the competitive position of the company.

REQUIREMENTS FOR THE PROTECTION OF TRADE SECRETS

The mere fact that a piece of information is identified as confidential does not automatically mean that it would be treated as trade secret. The essential elements required for protection are:

1) **secrecy** – this refers to objective standards of secrecy, that information is not generally known and readily available to the relevant public circles, rather only a certain social circle knows it;[9] For example, it is possible to convey a certain piece of information to other parties without compromising its trade secret status provided that these parties are legally bound to safeguard it (e.g. with a contract, legal provisions on confidentiality and the like.) According to Professor Zabel, any information on operations or positions of a company, which is known by the will of holder to a certain social circle inside or outside a company, can be taken as trade secret.[10]

2) **market-value** - a piece of information has an economic (commercial) value if it provides an advantage over the competition to its holder, or a person who lawfully controls it. In proceedings for infringements of trade secrets, a court determines this fact in each case. Regarding that a trade secret is primarily protected for the competitive advantage of a company, this means that information having economic value or providing the advantage is under pro-

7 It shall be deemed that no breach of duty to keep trade secrets occurred in case of disclosure of information referred to in Article 72 of this Law if such disclosure is:
1) Obligatory under the law;
2) Necessary for the performance of operations or safeguarding of interests of the company concerned;
3) Made to competent authorities or the public with the sole purpose of proving an offence punishable under the law.

8 Arsic believes that treating such information as trade secret prevents the competing company to achieve savings, and it is not in the common interest, given that the safeguard of negative piece of information as a trade secret can lead to a waste of social resources (See Arsić, Z., Trade secret, Proceedings of Novi Sad Law School, nos. 1/3, 1989, p. 57); Simovic has the opposite opinion, and believes that a negative piece of information may be trade secret (see: Simović, S., Industrial espionage and the protection of trade secret, the doctoral dissertation, Kragujevac, 2012, p. 191)

9 See: Zabel, B., *Trade Secret*, Institute of Comparative law, Belgrade, 1970, p. 26

10 idem p. 11

tection, because it contributes to the preservation or improvement of the competitive position of a certain economic entity.[11]

3) "**Reasonable efforts"** to maintain its secrecy. The term "reasonable measures to preserve confidentiality" is a legal standard. What efforts are considered reasonable depends on each case and on the importance and value of the information.[12] As a rule, the more valuable the information is, the harder, more expensive, and more difficult it is to protect it. Some of the most common measures include: recipients of confidential information should be employees whose nature of work requires it; holders of confidential information must be aware of the fact that information is confidential or secret; everyone who could potentially see or receive confidential nformation should sign agreements on confidentiality or non-disclosure agreements including employees, business partners, external associates, consultants; confidential documents should be marked "confidential"; access to the premises or files containing confidential information should be appropriately restricted.[13] Trade secrets can enjoy an infinite term of protection so long as information it consists of remains secret.

All conditions must be met cumulatively, thus trade secret is information that has economic value, it is not generally known (only to a specific social circle inside or outside the company), and is the subject of the holder's efforts to maintain its secrecy.

Trade secret, as intellectual property, has property value (not ownership characteristics) and the holder may transfer the right of use of that trade secret to another person (e.g.the license agreement). The concept according to which trade secret does not have ownership characteristics is based on the principle of confidentiality and the protection against unfair competition. In other words, as long as the relation is based on trust, a piece of information has protection against unauthorized use. Moreover, the concept of unfair competition is aimed primarily at preserving business ethics and morality and delas with business conduct between competitors on the market. This conception, that trade secret does not have ownership characteristics, prevails in European law and it implicitly derives from the provisions of the TRIPS Agreement, which lays down an obligation on safeguarding trade secrets through the rules on the protection against unfair competition.[14]

Unlike other industrial property rights, which imply fulfillment of certain formalities in order to ensure protection, data protection via trade secret does not require any formal registration of those data. Therefore, the protection of trade secret does not require administrative procedure which would build it up.

For all these reasons, confidential information that is protected by trade secret can very easily become the subject of various acts of unfair competition such as industrial espionage, breach of contract, abuse of confidence, etc.Violation of trade secret constitutes an act of unfair competition. The Law introduced the possibility of bringing a legal action for violation of the trade secret, as well as a strict liability for acting contrary to the Law, in the sense of responsibility for economic crimes.

The efforts to safeguard trade secret may sometimes be excessive and potentially endanger human health. For example, only vaccine manufacturer knows the full list of vaccine ingedients due to trade secret, and is not obliged to reveal all the ingredients in vaccines to the state institution that provides the marketing authorization and guarantees that the vaccine is safe for health.[15]

11 idem p. 25

12 Safeguarding trade secrets shall be determined in accordance with the assessment of the risk of illegal acquisition, use and disclosure of information that constitutes a trade secret (Art. 5 of the Law).

13 In legal theory there is a view that a certain piece of information is kept as a trade secret even if measures are not taken, however, according to circumstances, it may be assumed that there is an interest to keep a certain piece of information secret. See: Zabel, op.cit, p.95

14 See: http://www.zis.gov.rs/upload/documents/pdf_sr/pdf_tajne

15 http://www.youtube.com/watch?v=v8n8ePYA7nM (The Assembly in Geneva on the subject of

There is no neutral study in the world that would prove the harmlessness of the vaccine and its protective function, i.e. a study conducted by an independent scientist. All officially accepted "researches" were conducted by the pharmaceutical companies that produced the vaccine. Rather, the "evidence" on the integrity of a vaccine is based solely on the pharmaceutical industry, scientific and politicial consensus.

Very often there are speculations on the subject of compulsory vaccination of children in our media, and statements that it is a biological weapon, directed against people's health. There are also opinions that a person who discloses a trade secret, in order to inform the public on a certain abuse, is more likely to end up in court than the person who has committed this abuse.

CRITICISM OF THE ADOPTED TRADE SECRET LAW

The adoption of the Trade Secret Law has prompted numerous speculations among scientists, professionals and politicans.Without the intention to question the adoption of the mentioned Law, we will give certain points that accompanied the issue of regulation and protection of trade secret in Serbia:

1. Can you protect a trade secret in Serbia? There is a famous saying "A secret is what only one man knows". Due to WikiLeaks dispatches,[16] many of which concerned important state interests, a change of attitude towards trade secrets in Serbia was imposed. There was the impression that the biggest "vaults of secrets" are not the National Security Council, the Government of the Republic of Serbia or business companies, but rather the foreign embassies. Therefore, the possibility to protect companies' interests and trade secrets was questioned, since the highest state officials and authorities were unable to protect state secrets and interests.

2. General provisions – the creation of general legal norms leaves room for abuse of trade secrets. Good business practices and trade secret are defined in broad terms. It is not concretely and concisely established what a trade secret is,[17] or what financial and economic

harmful use of vaccines and children health damage; partial control of the competent state institutions is "justified" by the application of legal provisions, and trade secret institutes in Switzerland, Austria, Germany and many other European countries).

16 Internet site WikiLeaks, which was founded by Julian Assange in 2006, collects and publishes sensitive documents and information that states consider confidential. WikiLeaks survives thanks to donations, and it guarantees anonymity and protection of information sources. The US government accused WikiLeaks of threatening the United States national security by releasing 251 000 classified diplomatic cables sent to the State Department by about 270 of its embassies and consulates. Assange published the dispatches of the US Embassy in Belgrade, and also an inexhaustible source of information on US policy towards Serbia, and the local, Serbian political scene. They confirm Assange's basic thesis: "If civil servants and politicians knew that everything they did and said would come out and become known to the citizens who elected and paid them, they would never do what they did or say what they said". The former Head of the Security Administration of the Yugoslav Army, General Aleksandar Dimitrijevic, pointed out that "for all governments in the world, the secrecy was the instrument they used to hide all the evil that they had done, in the name of the alleged higher goals, or in the name of national security". According to him, WikiLeaks made "the strategic and tactical mistakes" during the disclosure. Strategically, it is wrong that defamatory material, harmful for privacy and intellectual property, as well as confidentiality was published. Dimitrijevic pointed out that every country had its own secrets that needed to remain secrets. According to him, a tactical mistake is that what happened gives the US and all other governments the right to take rigorous measures. See: Blic, 11.9.2012 or beyond, "When Google met WikiLeaks", Julian Assange, Albion Buchs, Belgrade, 2015.

17 For example, Law on Business Companies states that a trade secret shall be any piece of information the disclosure of which to a third party could cause damage to a company, as well as any piece of information that may have economic value because it is not generally known. This formulation suggests

information constitute a trade secret, and the determination cannot completely be left to companies, since trade secrets on the production capacity, volume and structure constitute State and official secret. Although the state tries to provide comprehensive protection of trade secret, the provision that it may come into possession of another person, without the consent of the holder, opens the possibility for abuse by persons who are not its legal holders.[18]

3. Securing of evidence[19] - In the case of urgency, the Court may initiate the securing of evidence without previous notification or hearing of the person from whom the evidence is being collected, and may survey facilities, search the vehicles, books, documents, databases, etc. The Court decision on the securing of evidence is being handed over to the person from whom the evidence is being collected at the moment of the collecting of evidence, and the absent person is informed about it as soon as possible. The need for such drastic measure is questioned, primarily in political circles. Since this mainly concerns the interests of companies, there is an opinion that the state exceedingly engages its own resources to protect trade secret. On the other hand, the state has already let much information out of the possession of the holder, without his consent.

4. TRIPS Agreement - During a debate on the Draft Law in the House of the National Assembly, the view was set forth that the Agreement on Trade Related Aspects of Intellectual Property Rights had been hasty and inappropriately applied, and that it applied to the members of the World Trade Organization. Serbia is not a member of the WTO, and it is not known when or whether it would be.

5. Practice and "Delhaize"[20] **–** As for unfair competition and violation of the equal position of market participants, it is questionable whether the provisions of the Law have been applied to the decision of the Commission for Protection of Competition that the Belgian company "Delhaize", which bought "Delta Maxi", does not have a monopoly position on the

---

that these are two categories of information, and the disclosure of the first category could cause damage to a company, and the disclosure of the second could bring benefit to a third party. Furthermore, the Law on the Protection of Trade Secrets says that trade secret shall be any piece of information that is not generally known and is not readily available to third parties. If a piece of information is not available to third parties, it should mean that it is not generally known, and vice versa.

18Acquisition, use or disclosure of information representing a trade secret to other persons is allowed without the agreement of the owner, if it has been legally performed and in a manner which is not in opposition to the fair business practice. (Art. 7, paragraph 2, of the Law on Protection of Trade Secrets).

19 At the request of the person that makes probable to the Court that the trade secret it legally controls is violated, or is likely to be violated, as well as that there are justifiable doubt that the proof shall be destroyed, or that it will be impossible to obtain such proof later, the Court may in the case of urgency initiate the securing of evidence without previous notification or hearing of the person from whom the evidence is being collected.

Securing of evidence in the meaning of Paragraph 1 of this Article is considered to be the surveillance of facilities, vehicles, books, documents, data bases, etc. the confiscation of objects and documents, the blocking of bank accounts, confiscation of cash and stocks, the questioning of witnesses and expert witnesses, as well as the undertaking of other measures in compliance with the legislative regulation of the execution procedure.

The Court decision on the securing of evidence is being handed over to the person from whom the evidence is being collected at the moment of the collecting of evidence, and the absent person is informed about it as soon as possible. Procedure following the request from paragraph 1 of this Article is subjected to the provisions of the Law regulating executive procedure (Art. 14 of the Law on Protection of Trade Secrets).

20 Belgian company "Delhaize" bought retail chain "Delta Maxi" for almost one billion Euros in 2011, noting that it advocated open market and transparent competition, believing that healthy competition could bring numerous benefits to consumers, above all: "We are not interested in short-term profit - monthly, quarterly or yearly, rather we are interested to offer the best that Delhaize group has to offer to the consumers. Another reason why we decided to enter this market is that we are convinced that Serbia, as a European country, would join the EU, and when that happens, it will lead to market expansion and growth of the work", said the President and CEO Pierre-Olivier Beckers. Press online, 4.3.2011.

Serbian market. [21] Actually, after the purchase of "Delta Maxi", "Delhaize" took over 70% of the market in Belgrade, and more than 30% in Serbia. Recently, the Croatian "Agrokor" (together with "Delhaize"" it takes up to nearly two thirds of the market in Serbia), having taken over the shares of "Mercator", has become the majority owner of Slovenian trade chain, and it has raised the question of the effect such business decision would have on the Serbian market, i.e. suppliers, manufacturers and consumers. [22] Although formally the Commission for Protection of Competition should decide on the merger, there are several important facts apart from the possible distortion of competition.[23] The new giant could remove the smaller, domestic traders through unfair competition. In addition, in the two retail chains that are joining, private-label products made in Croatia or Slovenia make up higher percentage.[24]

6. Legal abuse - there is no doubt that the provisions of the Law can be abused. Citizens and journalists often allude to the Law on Free Access to Information of Public Importance, seeking information from public companies regarding the bidding documents and contracts for public procurement of goods and services. Often, managers circumvent the transparency in business, referring to the Law on Protection of Trade Secrets, or deny the request of the information seeker and deny him the right to a copy of the requested documents. Such actions are contrary to the provisions of the Law on Free Access to Information of Public Importance, and taking into account previous practices of the Commissioner for Information, it may be concluded that such decisions are often dismissed as illegal in stage procedures. Therefore, this Law should not make room for public companies to conceal their business or procurements whose value is measured in billions of dinars.

7. The importance of information - In the modern world it is often heard that the information is the most valuable commodity, and that the owner of timely information owns the world. In order to avoid enormous economic damage due to loss or flow of business information, the subjects of entrepreneurial activity need to develop their own system of information protection and establish the necessary level of confidentiality. Information, research, and technological procedure may have a commercial value and give a significant

21 The Commission for Protection of Competition approved the concentration of the Belgian company "Delhaize" over company "Delta Max" by the decision from 12.7.2011, stating that the concentration does not lead to a significant restriction, prevention or distortion of competition in the market of the Republic of Serbia or in its parts, and as a result of the creation or strengthening of dominant position.

22 Art 15 of the Law on Protection of Competition ("Official Gazette of RS", no. 51/2009 and 95/2013): Dominant position on a market is the position of a participant that can do business on a relevant market, independent of the actual or potential competitors, buyers, suppliers or consumers. The market power of market participants is determined in relation to economic and other relevant indicators, in particular:
1) the structure of the relevant market;
2) market share of the market participants whose dominant position is being determined, especially if it is higher than 40% in the given relevant market;
3) actual or potential competitors;
4) economic and financial power;
5) the degree of vertical integration;
6) advantages in access to supply and distribution markets;
7) legal or factual obstacles to market access by other market participants;
8) the power of the buyers;
9) technological advantages, intellectual property rights.
Two or more legally independent market participants may have a dominant position if they are linked by economic ties, so that they can act jointly in the relevant market or seem as one participant (collective dominance). The burden of proof of a dominant position in the relevant market is determined by the Commission.

23Art. 9 of the Law on Protection of Competition: Pursuant to this Law, infringements of competition are the acts or practices of market participants whose purpose or results have or can have a significant restriction, distortion or prevention of competition.

24 If "Agrokor" gets the consent of the Antimonopoly Commission to work in retail in Serbia, it will have a 30.6 % market share. It is interesting that the Belgian "Delhaize" bought "Maxi" for 932 million Euros, almost twice the price "Agrokor" paid for "Mercator".

edge over the competition. The whole meaning of the Law is to instruct businessmen, holders of significant information that has a commercial value, and people who developed it, how to commit themselves to keeping information confidential, and to establish a legal sanctioning procedure for the disclosure of information to unfair competition. Serbian legal system is criticized for having insufficiently clear procedure for classification of certain confidential information. In addition, information on the economic, commercial, technological, technical and other potentials of competitors, on business connections and weak points of persons who participate in the economy is passed on through fluctuation of personnel.[25]

8. Disclosure of trade secret - We have already pointed out that a company, through internal acts, decides on the preservation and protection of trade secret, and determines what information, data or knowledge shall constitute a trade secret. The question of remedies which would ensure the effective protection of trade secret against various acts of unauthorized acquisition, useage, or disclosure by third parties, was brought up by the Commission for Protection of Competition, in the case of the analysis of "Delta Maxi" business, which was conducted by the Institute of Economic Sciences. Namely, for the purposes of the Competition Commission, the Institute of Economic Sciences had conducted a study that showed that "Delta Maxi" did not have a dominant position on the Serbian market, and the Commission approved the "Delhaize" takeover of the largest retail chain in Serbia. However, Belgrade media published the data on the amount of trade margin from the Institute study, which were considered trade secret. Leaders of the Institute of Economic Sciences pointed out that the statements of the alleged unauthorized and unlawful disclosure of the information had been given on the basis of publicly available information, thus could not be considered as the disclosure of trade secret. Of course, the public instantly became interested whether the Serbian consumers were left to the arbitrariness of merchants, and whether they had the right to know what the real price of a product was and how much dealers earned from them. Moreover, this raised the question of the free market and monopoly market.

NONDISCLOSURE AGREEMENT

At this time of developed market economy, technological revolution and high competition, business entities tend to ensure their position, preserve specific business knowledge and information, create a sustainable competitive advantage and impose themselves to the consumers through achieving good business results.

Confidential information is autonomously protected by the general acts, such as statutes, Trade Secret Acts, rules of procedure of certain organs, business codes and the like. An important instrument for the protection of trade secret is the nondisclosure agreement.[26] It is

25 Volkswagen lost a court case and pledged to pay compensation of 100 million dollars to General Motors, with the obligation to purchase car parts for one billion dollars, after the defection of eight managers, who had taken important documents, from Opel (that belonged to General Motors) to the Volkswagen (in 1993). Famous hacker Albert Gonzales stole credit and debit card numbers from 94 million TJX credit card users, due to lack of the protection of information system. He was sentenced to 40 years in prison, and the company lost its customers. Former Ford's engineer Xiang Dong Yu who stole secret documents worth millions of dollars after 10 years in Ford, was arrested in 2009 and sentenced to 6 years imprisonment.

26 It should not be equated with the agreement on the transfer of trade secrets when the holder discloses the information that constitutes a trade secret to other party for a fee and consequently allows its application in order to achieve business benefits. Nondisclosure agreements are contracts which protect the confidential data disclosed to other party during the course of a business transaction, thus representing an accessory contract; an accessory contract is made for the purpose of assuring the performance of a principal contract; however, it is legally autonomous and independent of it. See: Graić-Stepanović, S., Trade Secret as the subject of intellectual property rights, Legal Life, no. 13/2007

best practice to conclude a nondisclosure agreement before engaging in negotiations, and in all situations where the parties hold information, which is protected as a trade secret, and are willing to exchange it under the certain circumstances. It contains conditions prohibiting the disclosure of confidential and private information on specific knowledge, customers or products, strategic plans, and other confidential information that are intellectual property of a particular business entity, and the competition could have economic gains from its use.

The agreement needs to specify what information is confidential and for what purpose it can be used, in order to protect business interests of the contracting parties and to avoid interpretation. If the contractual provisions are unclear or incomplete or prosecutors cannot prove their case, the court will reject the request, making data available to competing companies and other interested parties. The agreement must establish a time period during which confidentiality of the information is to be maintained, and in business practice it is usually from one to five years, which depends on the type, nature and importance of the protected information. Understandably, the more complex importance of information, the more complex the agreements are.

Regarding the content of the agreement, there are five basic elements: the definition of confidential information, any exclusions from the confidential information, the obligations and duties of the party receiving the confidential information, the time periods for which the NDA will be valid and enforceable, and any miscellaneous provisions (e.g. an agreement on the Law to be applied in the case of a dispute, arbitration clause, etc.). Furthermore, the parties may designate the amount of liquidated damages in case the NDA is breached. It is also recommended that the agreement includes clauses on dispute resolution through mediation or arbitration, as well as an adequate choice of national laws applicable to the agreement, in the case of international agreements.

Exceptionally, a receiving party cannot be legally bound by the agreement if the information becomes part of the public domain through no act or omission of a receiving party. Besides, the disclosing party may unilaterally rescind the contract if it allows the disclosure of the information after the agreement comes into force.

Today, the conclusion of nondisclosure agreements is the most successful method for the protection of important business information, because it is available to any natural person, stock corporation, Limited Liability Company or other business entity. The practical reason to have an intellectual property protected by the nondisclosure agreement is in the fact that such protection does not have a time limit, and an agreement can be concluded for the long period, depending on the will of the parties. On the other hand, the disclosure of the trade secret may be quite easy, especially by the parties that have somehow come into possession of it, and have not concluded a nondisclosure agreement. Then, the holder of the trade secret does not have legal power to protect it; i.e. he/she cannot achieve compensation for damages he/she may have suffered.[27]

On the occasion of the opening of a new car factory in Kragujevac, the partnership between the Italian company FCA Italy (formerly "Fiat group") and the Government of the Republic of Serbia was followed by the conclusion of a nondisclosure agreement, and the signatories committed themselves not to disclose or in any way use protected information. The company FCA Italy form Turin[28] requested that the Joint Venture Agreement between Fiat and Republic of Serbia, (signed in 2008) to invest in a car factory in Kragujevac, contained confidential provisions in order to protect the joint investment. Taking into consideration the interests of the company and its shareholders, FCA Italy did not publish confidential contract

27 Milosavljević, M., *Trade secret services and its protection in the Republic of Serbia*, Proceedings of "Law and Services", p. 626, Kragujevac, 2012
28 See: http://www.fiatsrbija.rs/fca/index.html

provisions that were key commercial and industrial secrets. Thus, the Italian partner did not want to present business plans for the next ten years to the public or competition, with the explanation that the entire agreement was in the possession of the European Investment Bank, which said the business venture was a success and approved the requested loan. Representatives of the FCA Italy pointed out that the unpublished annexes also contained a business plan of the joint venture with the data on the production dynamics, which constituted a trade secret all around the world. Namely, the business plan contained data on the volume and dynamics of vehicles production, on the markets where they would be placed, data on the usage of energy and a range of other technical details, in which only the competition would be interested.

The Commissioner for Information of Public Importance reacted to such action of the contracting parties, and pointed out that the implementation of the right to free access to information was guaranteed by the Law on Free Access to Information of Public Importance,[29] and could not be disputed by the provisions of any commercial contracts. The possibility of limitation cannot refer to information that is absolutely legitimate subject of public interest. In terms of the Joint Venture Agreement between Serbia and Fiat referring to the confidentiality and disclosure of information, it is provided that the obligation of confidentiality shall not apply if the disclosure of information is required by the applicable law, and that is the Law of the Republic of Serbia.[30]

The Anti-corruption Council reacted, raising the question why it was a secret what infrastructure the state should set for "Fiat" to do business in Serbia, what real estate Serbia invested in joint project and which subventions were given to Italian company. The general and imprecise provisions of the Law on Classified information were criticized in the media, provisions which made possible for the authorities to conceal information from commercial agreements concerning money or property of the state and citizens, under a veil of secrecy.

The contract has not been fully published to this day, however, thanks to partnership, the new factory "FCA Serbia d.o.o" was opened in 2012. It employs over 3000 workers and represents a desirable employer and socially responsible company that strives to be a good member of the community in which it operates.[31]

THE MOST EXPENSIVE SERBIAN SECRETS

Due to the loss of important business information, the signed contracts are breached or are not fulfilled, promises are broken, the request ignored, unnecessary financial resources are allocated and competitive advantage in the market is lost. The authors only want to remind you of some agreements Serbia concluded with individual counterparties under the veil of secrecy, which are still part of the public attention and whose justification is suspected. Without the intention to prejudge anyone's fault, the individual cases marked as "the most expensive Serbian secrets" are going to be summed up.

29 *Official Gazette*, nos.120/2004, 54/2007, 104/2009 and 36/2010

30 On January 16th 2012, the Commissioner for Information of Public Importance made the decision on the imposing a fine to the Ministry of Economy and Regional Development for not following the Commissioner's orders to submit annexes and appendices of the Joint Venture Agreement between Serbia and Fiat to the Anti-Corruption Council. 200 000 RSD fine was imposed to The Ministry.

31 Fiat automobile Company Serbia on the occasion of International Women's Day donated 5000 EUR to Center for Oncology and Radiology in Kragujevac; launched an internal campaign for the prevention of breast cancer; donated 30 computers to young mathematicians and computer scientists in the First Grammar School; and through the educational campaign "Smart Kid", showed the concern for the protection of the youngest traffic participants. Additionally, the Italian partner opened a kindergarten named "Autić" for employees' children.

"Satellite" Affair - Unbeknownst to the Council of Ministers of Serbia and Montenegro, the former Defence Minister Prvoslav Davinic signed a spy satellite rental contract with Israeli company ImageSat, worth 45 million euros, in a hotel room in Paris (in 2005). The Israeli side agreed to rent spy satellites like "Eros A" and "Eros B", designed for overseeing the territory of Kosovo and Metohija, to Serbia for six years period and to install a control station. Serbia failed to live up to its part of the contract, and ImageSat won the case before the International Court of Arbitration in Paris. Thus, Serbia had to pay EUR 27.85 million from the budget reserves to the Israeli company in February 2011.

"Armour" Affair - A disputable contract between the company "Mile Dragic" and the Serbia and Montenegro Forces (signed in 2005) had been discussed before the Serbian judiciary for eight years. The allegations in this case and the qualifications of the offense, for which Dragic as the company director was charged, were changed several times. The Court of Appeal upheld the acquittal of the Basic Court in Zrenjanin (2013) and Dragic was acquitted on all charges of the affair publicly known as "Armour", which was presented as a "robbery of the century" to domestic public.

The case of Miladin Kovačević is complex and unusual in many ways. Namely, Kovačević severely beat up a US citizen Bryan Steinhauer during a physical attack in the United States (2008). During the trial, he said that he had fled from the United States because he had feared for his life and his family safety, and not to avoid criminal responsibility. He pleaded guilty before the Serbian judiciary and was sentenced to 27 months prison (in 2010). It is interesting that two diplomats from the Serbian consulate in New York lost their jobs at the Ministry of Foreign Affairs and were sentenced to jail or probation because of Kovačević. In order to "improve relations" with the United States, the Government of Serbia paid the Steinhauer family $ 900 000 to help cover their son's medical costs (in early 2009).

The concession for the construction of Horgos-Pozega highway - Concessionaires for the construction of the Horgos – Pozega highway, Austrian consortium Alpine[32] and PORR broke up unilaterally the concession contract in 2008, a year after the signing because, as they claimed, the Government of Serbia did not make possible for them to close the financial construction. Due to alleged trade secret regarding technical solutions, the motorway concession contract was never fully available to the public and the European Commission aligned it in one of the "24 controversial cases" where there was serious doubt about their legality. The agreed working costs amounted to EUR 1.5 billion. The concession should have been issued for 25 years. The arbitration proceedings for broken concession Horgos-Pozega was launched before the International Chamber of Commerce in Paris and the concessionaire demanded compensation for lost revenue and investment in the concession of up to EUR 81 million. The dispute reached the decision in favor of Serbia (2013), which was obliged to allocate EUR 10 million from the budget, because it had groundlessly activated a bank guarantee in the said amount.

Sales contract for 51% of the shares of NIS to Russian company "Gazprom Neft" was a secret until its final signing (2008). The former prime ministers of the two countries contract-

32The seriousness of Alpine and the state in legal matters with the aforementioned Austrian company are often questioned before the general public. Serbian authorities have signed several "controversial" contracts with this company from 2006 until today. The first signed "controversial" contract worth RSD 2.9 billion referred to the construction of a new bridge near Beška and the reconstruction of the old one. The conceptual design of domestic company "Mostogradnja" was declared the best and cheapest offer. However, the task was entrusted to Alpine that requested fulfillment of obligations from the State, in the amount of EUR 102 million. "Roads of Serbia" accepted only EUR 62 million, and the dispute ended up in court. Later, the Austrians obtained the concession for the construction of the Horgoš -Požega highway. Meanwhile, during 2010, despite the problematic cooperation, Serbia signed another contract with Austrian Slovenian consortium "Alpina – Meteorit" to build a railway bridge over the river Velika Morava near Ćuprija, which has not been built yet.

ed the sale and state presidents took over the guarantee that contractual obligations would be fulfilled.[33] The Ministry of Interior launched an investigation to inspect the privatization of the Petroleum Industry of Serbia, in order to determine whether the selling of this company's majority shares was bad business. [34] The Anti-Corruption Council had earlier expressed doubts about the legality of this contract and warned that natural resources could not be disposed through the Contractual agreement.

NBS foreign exchange reserves – In which highly ranked foreign banks and international financial institutions National Bank of Serbia deposits foreign exchange reserves is a trade secret. According to international practice, these are banks that the world credit rating agencies rated as the safest. The Monetary Board of the National Bank manages foreign exchange reserves.[35]

CONCLUSION

- The question of the regulation and protection of trade secret is certainly extremely complicated and sensitive matter. Given that we are the part of the world where economic espionage has become common and where the success of the company depends on timely information, it is necessary to provide serious protection of the domestic economy and ensure its competitiveness on the market.

- The adoption of the Law on Protection of Trade Secret showed that certain data and information needed protection. The general concept of trade secret is regulated for the first time, along with the elements that information has to contain in order to be considered a trade secret, measures for trade secret protection, and the legal protection of trade secret against all acts of unfair competition. Merely stating that a piece of information is confidential will not automatically mean it is trade secret.

- In order to avoid enormous economic damage as a result of loss or flow of business information, business entities need to build their own system of information protection and establish the necessary level of confidentiality. The security of business information represents the most important question of security management. The act on trade secret must include provisions on the liability of persons who come into contact with most confidential documents by their function, and obligations for all employees regarding trade secret protection. Every employee is expected to cooperate in safeguarding the trade secret and to inform relevant authorities on all noticed shortcomings. Establishing a system of business security and permanent education of employees in the area of trade secret protection should be seen as the most important tasks of each company's management, and not as a business cost (See more: Milošević, M., Trade secret of the company, legal informant, no. 6 / 2005).

- Serbian legal system is criticized for having imprecise procedure for classification of certain information marked with "secret". Classification should be made according to the degree of confidentiality and secrecy.

- Regulatory provisions regulate disciplinary and criminal sanctions in case of non-compliance with the company trade secret protection policy; however, considering that due to

33 The negotiating team appointed by the Government of RS determined the transaction details in direct negotiations.

34 In political circles, the opposition believes that this investigation may affect the issue of relations with Russia, and that the initiation of the investigation is an "implicit accusation of the Russian leadership and investors".

35The public is familiar with the Russian "Euroaxis" bank affair, where the NBS once deposited the part of foreign exchange reserves. This later caused the suspicion that it was a returned favor for taking favorable loans for some influential people of the Serbian economy from the aforesaid bank.

the loss of important business information signed contracts are broken or unfulfilled, promises are violated, requests are ignored, unnecessary funds are allocated and competitive advantage in the market is lost, we come to the conclusion that the best way to safeguard the company trade secret is to act preventively.

- The most developed countries in the world are increasingly using their intelligence resources to obtain carefully guarded industrial, manufacturing or financial information, which would secure better position for the state or domestic corporation in the global market.

- There are several ways to acquire requested information that not include the use of illegal means or methods: the Internet is the easiest and most used way of finding information on economic entities. It is evident that the IT staff training regarding the Internet security is quite low. The access to social networks like Facebook, Twitter or various chat-rooms may be a great danger for every company. Anonymity, which can be achieved more easily on the Internet than in some other situations, also contributes to the popularity of using the Internet for acquisition of confidential information. The ability to access the Internet from public places, such as libraries or internet cafes, offers great opportunities for completely anonymous Economic Intelligence. The search of employees is the common method of finding information (See more: Neskovic, S., *Economic Espionage and new technologies in a globalized international community*, development work, no. 2/2013, pp. 57-76).

REFERENCES

1. Acin-Sigulinski S., Poslovna tajna-zalog kompanije za opstanak, Ekonomske teme, zbornik radova Ekonomskog fakulteta u Nišu, br. 2/1997.
2. Arsić Z., Poslovna tajna, zbornik radova Pravnog fakulteta u Novom Sadu, br. 1/3, Novi Sad 1989.
3. Berle A.; Means G.,The Modern Corporation and Private Property, Transaction Publishers, Piscataway NJ 1932
4. Bilandžić M., Poslovno-obavještajno djelovanje: Business intelligence u praksi, AGM, Zagreb 2008.
5. Bošković M.; Bošković A., „Neki aktuelni problemi od značaja za bezbednost i zaštitu korporacija", u: Naučni skup „Dani bezbjednosti" na temu: „Razvoj sistema bezbjednosti i zaštite korporacija" (Zbornik radova), Fakultet za bezbjednost i zaštitu Univerziteta Sinergija, Banja Luka 2011, str. 11–20.
6. Bošković M.; Keković Z., Bezbednost lica, imovine i poslovanja preduzeća, VŠUP, Beograd, 2003.
7. Daničić M.: Obezbeđenje lica i imovine preduzeća u Republici Srpskoj, Visoka škola unutrašnjih poslova, Banja Luka 2006.
8. Graić-Stepanović S., Poslovna tajna kao predmet prava intelektualne svojine, Pravni život, Beograd, br. 13/2007.
9. Jäger T.; Kümmel G. (eds), Private Military and Security Companies, VS Verlag für Sozialwissenschaften, Wiesbaden 2007.
10. Javorović B.; Bilandžić M., Poslovne informacije i business intelligence, Golden marketing & Tehnička knjiga, Zagreb 2007.
11. Keković Z.; Savić S.; Komazec N.; Milošević M.; Jovanović D.,Procena rizika u zaštiti lica, imovine i poslovanja, Centar za analizu rizika i upravljanje krizama, Beograd 2011.
12. Mandić G., Sistem obezbeđenja i zaštite,FCO, Beograd 2004.

13. Marković S., Poslovna tajna kao predmet ugovora o prenosu industrijske svojine, Pravni život, Beograd, br. 11-12/1993.
14. Milosavljević M., Poslovna tajna u uslugama i njena zaštita u Republici Srbiji, Pravo i usluge (zbornik radova), Kragujevac 2012.
15. Milošević M., „Normativna (ne)uređenost privatnog obezbeđenja lica i imovine u Republici Srbiji", u: Hadžić M. (prir.), Reforma sektora bezbednosti u Srbiji – Dostignuća i perspektive(Zbornik radova), Centar za civilno-vojne odnose, Beograd 2007, str. 127–140.
16. Milošević M., Poslovna tajna privrednog društva, Pravni informator, Beograd, br. 6/2005.
17. Milošević M., Propisi o poslovnoj tajni-pojmovno određenje i odgovornost za nepoštovanje, Izbor sudske prakse, br. 4/2007.
18. Nešković S., Ekonomska špijunaža i nove tehnologije u globalizovanoj medjunarodnoj zajednici, Vojno delo, br. 2/2013.
19. Semjonova N., Pravna pitanja zaštite poslovne tajne u Ukrajini, Pravo i privreda, Beograd, br. 9-10/2000.
20. Simović S., Industrijska špijunaža i zaštita poslovne tajne, Grafostil, Kragujevac 2012.
21. Trivan D., Korporativna bezbednost, Dosije studio, Beograd 2012.
22. Vukićević S., Javnost rada privrednih subjekata i poslovna tajna, Pravni život, Beograd, br. 12/2007.
23. Zabel B., Poslovna tajna, Servis Saveza udruženja pravnika Jugoslavije, Beograd 1970.
24. Zindović I.: Multinacionalne kompanije i ekonomska špijunaža, Alisa press, Kraljevo, 2008.

LEGISLATION

25. Krivični zakonik Republike Srbije, "Službeni glasnik RS", br. 85/2005, 88/2005 - ispravka, 107/2005 - ispravka, 72/2009, 111/2009 и 121/2012.
26. Zakon o privrednim društvima, "Službeni glasnik RS", br. 36/2011, 99/2011 и 83/2014-dr. zakon i 5/2015.
27. Zakon o slobodnom pristupu informacijama od javnog značaja, "Službeni glasnik RS", br. 120/2004, 54/2007, 104/2009 и 36/2010.
28. Zakon o zaštiti konkurencije, "Službeni glasnik RS", br. 51/2009 i 95/2013.
29. Zakon o zaštiti poslovne tajne, "Službeni glasnik RS", br. 72/2011.

INTERNET SOURCES

30. http://www.businessintelligence.com
31. http://www.coca-colahellenic.rs/.
32. http://www.zis.gov.rs/upload/documents/pdf_sr/pdf_tajne
33. http://www.youtube.com/watch?v=v8n8ePYA7nM
34. http://www.fiatsrbija.rs/fca/index.html

Topic VII

CYBERCRIME

UDC: 343.983:004.42

COMPARING INTEGRATED AND NON-INTEGRATED DIGITAL FORENSICS TOOLS

Dragan Randjelovic, PhD[1]
Academy of Criminalistic and Police Studies, Belgrade
Damir Delija, PhD
University College for Applied Computer Engineering, Zagreb
Dragan Stojkovic
Marko Velickovic
Ministry of the Interior of the Republic of Serbia
Dragan Erlevajn
Security Information Agency, Belgrade

Abstract: Today the security of information stored on an electronic medium is one of the biggest challenges faced by those in charge of the security and integrity of computer systems. In most countries that have a developed and modern legislation the misuse of other people's data is a criminal offense. This means that the security of the data includes not only the scope of work of safety managers, but also of law enforcement professionals and courts.

The main problem for these offenses is securing of evidence, because of its specificity in the detection of computer crime it is not possible to use the classical methods of criminal forensics. Therefore, it is necessary to have specific programs that are able to respond to new challenges and to provide data that are characteristic of evidence in judicial proceedings.

In this paper we processed the integrated and non-integrated digital forensics tools. SIFT Workstation and I3A were processed in the paper out of the integrated tools and EnCase and FTK out of the non-integrated. The function of these programs is explained in the paper and the short instructions for their use are presented. At the end of the paper there is a comparison of these tools. We compared the speed of execution of the most important functions of forensic tools which is the off-line and live image analysis.

Keywords: Internet, computer networks, digital forensics, digital evidence, integrated and non-integrated tools.

INTRODUCTION

We are witnessing a growing number of computer crimes, and it is safe to say that this trend will continue in parallel with the development of technology. It is becoming increasingly obvious that we are more often the victims of a new type of crime, the modalities and

1 E-mail: dragan.randjelovic@kpa.edu.rs.

the "modus operandi" develop with a hitherto unseen dynamics[2]. To successfully counter this type of crime, it is necessary to implement a comprehensive prevention, and if it does not produce the desired results, a key role in the discovery of the perpetrator and collection of the evidence of his guilt is now taken by a young discipline of forensics - digital forensics[3], [4],[5].

In the literature pertaining to the field of digital forensics, you may see different names for the discipline, such as computer forensics, digital forensics, cyber forensics, etc. Likewise, you may see various attempts to define this, we can say, the youngest discipline of forensics. Computer forensics: computer uses digital technology to develop and provide evidence in court and prove or disprove a claim [6][13]. A slightly different definition is given by John Vacca, and in his opinion, computer forensics involves the preservation, identification, extraction and documentation of evidence stored on digital computer[7] [20]. It is interesting that in some cases, digital forensics is also seen as a science and as an art using IT knowledge and skills to assist in the resolution of any legal process[8] [3]. Simply put, digital forensics is the process of collecting, preserving, analyzing and presenting digital evidence. In most cases, the terms "computer forensics" and "digital forensics" are regarded as synonymous, but among them there is still some difference. Unlike computer forensics relating to the collection of digital evidence stored on a computer (PC), digital forensics is a more general term and refers to all the devices that can carry digital data. In addition to the computer, it can be: digital photo cameras, digital cameras, mobile phones, smart phones, PDAs, and various other audio/video playback devices. Simply, we can say that digital forensics is computer forensics upgrade, due to the development of information technology and the emergence of various digital data carriers.

When an incident occurs, the process of digital forensic investigations starts. Digital forensics is crucial for the successful detection and prosecution of criminals in the area of computer crime. When you start this procedure, its duration must be conducted in accordance with the law, because only in this way evidence gathered in this process may be valid in court.

Also, it is very important that this process is performed by strictly determined order and not skipping any single phase. The evidence contained in a digital form is very sensitive and can easily be modified or destroyed. Every mistake that one makes in this process can be a big problem because digital forensics thus loses its fundamental meaning. If there is no credible evidence that has been collected in accordance with legal procedures, then one cannot get to punish the perpetrator.

When we talk about the process of digital forensic investigations, there is general agreement in the literature on the sequence of procedures, but there are different opinions on the number of phases. In most cases, we talk about the four stages, although there are cases where this number is three, five and even seven stages.

The process of digital forensic investigation consists of the following stages:

- Acquisition,

2 Ignjatović, Đ. (1991). Pojmovno određenje kompjuterskog kriminaliteta. Beograd: Anali Pravnog fakulteta u Beogradu

3 Milosavljević, M., & Grubor, G. (2009). Digitalna forenzika - udžbenik. Beograd: Univerzitet Singidunum

4 Milosavljević, M., & Grubor, G. (2009). Istraga kompjuterskog kriminala. Beograd: Univerzitet Singidunum

5 Petrović, R. S. (2000). Kompjuterski kriminal. Beograd: Ministarstvo unutrašnjih poslova Republike Srbije

6 Newman, C. R. (2007). Computer Forensics: Evidence, Collection and Management. New York: Auerbach Publications

7 Vacca, R. J. (2005). Computer Forensics: Computer Crime Scene Investigation, Second Edition. Massachusetts: Charles River media

8 Brown, L. T. (2010). Computer Evidence: Collection and Preservation, Second Edition. Boston: Course Technology

- Searching,
- Analysis, and
- Presentation.

The acquisition is the first phase in the process of digital forensic investigations. This phase is analogous to taking photographs, fingerprints or traces of blood in the "traditional" forensic investigation. Since the beginning does not mean that all data will be used as digital evidence, the objective of this phase is to preserve all digital values. Therefore, during the acquisitions the so-called bit-by-bit copy of data is made. In fact, it is a process where, with the help of proper forensic tools (software, hardware or a combination), a copy of the original device (HDD, CD, USB memory, etc.) is taken. This copy is called a forensic copy of the disk, a disk image, or simply images. A forensic copy is not an ordinary logical backup, because it includes not only the currently visible data on the disk but also the data that has previously been deleted.

In the searching phase, copies (images) are "start up" on a computer that is used for the analysis. After that, start the searching. It is essential to use time effectively, because sometimes it is a resource which is not available in the required quantity. It is a good first step in eliminating files that are known not to represent the potential of digital evidence (explore.exe, iexplore.exe, winword.exe, etc.).

Also, if you know what you are looking for, your search may be conducted by keyword (keyword analysis). In this way, it performs filtering files based on a given word, and it is a much easier search.

In the analysis phase, there comes the interpretation of digital evidence collected in the previous phase. The analysis aims to detect and display all the circumstances relating to particular incident. This stage requires the most skill and creativity, some of which directly depends on clarifying and verifying specific criminal activity.

Presentation of the results obtained from the previous phase, represents the last, i.e. final phase in the process of digital forensic investigations. The results of the forensic investigation are presented or given to the use of those organs who requested the investigation. The results shall be such that at any moment they could be obtained again and that someone else can get the same results.

The main objective of the investigation, when it comes to a computer incident, as in the case of classic crime, is to collect irrefutable evidence and solid evidence of guilt or release the suspect. In the case of a traditional crime such as murder, irrefutable evidence is firearms located in the hand of murderers. Or, in the case of theft, evidence may be the money that was found in a person who has committed a theft. In computer crime, such obvious and direct evidence is almost impossible to obtain, but it is possible to build solid, irrefutable digital evidence without the so-called cracks.

Also, in contrast to the classical investigations, in digital forensic investigation at the beginning it is not known where all the evidence can be found. There are no obvious places to find evidence like in classic crime, for example, a bullet hole, blood stains, messed things, etc. Also, it is very difficult to preserve a place where there is digital evidence from a variety effects that can destroy or alter evidence.

For example, if it rains on the footprints found in the dust, forensic scientist has the ability to cover the area and later continue the investigation. All this indicates that digital evidence is very sensitive and forensic experts must have enormous knowledge and experience in order to successfully carry out the process of digital forensic investigation and collect the necessary evidence.

In the literature, various definitions of digital evidence are presented. According to one of them, digital evidence is defined as any information that is stored or transmitted using a computer and that supports or refutes the theory of how the offense was performed and who was its executor[9].

Also, they can be defined as the data and information that are of relevance to the investigation, which are stored or transmitted by electronic device in digital form[10]. Simply put, digital evidence is any information in digital format (consisting of 1 and 0), which is relevant to the legal proceedings [11],[12],[13],[14]. These can be various patterns of text, images, sound clip, video clip, or combinations thereof.

DIGITAL FORENSICS TOOLS

Digital evidence is stored within a computer system, so it is impossible to see the content without the help of appropriate forensic tools. There are a number of tools. Some of them are used for one purpose, while others have a much greater range of options. The choice of tools to use depends on the specifics of the investigation. It is always desirable to choose the tool that will contribute to the most reliable way of achieving the objective for which it is used. Forensic tools can be divided into several groups, but it should be noted that, according to the functions they perform, they must not strictly belong to one particular group. In the literature, in most cases, the tools are classified into commercial and non-commercial tools, i.e. those that are licensed and those that are open source.

Commercial tools are made mainly for the Windows platform[15]. These tools have many modules integrated into a single program, so generally cover more areas of the process of digital forensic investigations. What appears as a problem with these tools is that they are paid and are costly.

Non-commercial tools are not paid, they are running on Linux, and they usually incorporate all aspects of the process of digital forensic investigations. What is important for these tools is that they can make a full investigation, i.e. provide all the features that have the expensive commercial tools. In the open source tools, source code is available for consideration and further customization. That is what makes them very functional and we can find this in literature[16].

NON COMMERCIAL TOOLS

The origins of computer forensic analysis lie not with the Windows operating systems which has achieved such popularity today but with UNIX, an operating system with its roots in the early 1970s. The developers of UNIX preferred to create a fairly large number of small programs which could be used together to perform more complex tasks rather than one program which could do everything and it is from these small programs that the sophisticated

9 Casey, E. (2004). Digital Evidence and Computer Crime, Second Edition. London: Academic Press
10 Milosavljević, M., & Grubor, G. (2009). Istraga kompjuterskog kriminala. Beograd: Univerzitet Singidunum
11 Petrović, R. S. (2000). Kompjuterski kriminal. Beograd: Ministarstvo unutrašnjih poslova Republike Srbije
12 Ranđelović, D., & Bogdanović, T. (2010). Alati za digitalnu forenziku, NBP - Žurnal za kriminalistiku i pravo, Vol. XV, No. 2, 25-47
13 Randjelović, D., Delija, D., Popović. B. (2009). EnCase forenzički alat, Bezbednost 1-2, pp. 286-312
14 Randjelović D. (2011). Poredjenje komercijalnih i nekomercijalnih alata digitalne forenzike i njihova upotreba Naucno tehnicka informacija, VojnoTehnicki Institut Beograd
15 Carvey, H. (2009). Windows Forensics Analysis. USA: Syngress Publishing, Inc
16 Altheide, C., and Carvey, H. (2011). Digital Forensics with Open Source Tools. Massachusetts: Elsevier

commercial computer forensic packages available today have grown. The small programs are still found in modern versions of the UNIX operating system and many are also available for Windows [10],[14].

In this section we consider two forensic duplication tool kits which are most popular: Autopsy with Sleuth kit and DD as a small software which is often used in other more complex as its required part.

We must also notice The Coroner's Toolkit which is a collection of (essentially) free tools designed to be used in the forensic analysis of UNIX machines. The Coroner's Toolkit is specifically designed to be of use in the investigation of a computer break-in. The tools included help to reconstruct the activities of an intruder by, amongst other things, examining the recorded times of file accesses and recovering deleted files.

MD5 is used to ensure that the copy is exactly the same as the original. This procedure results in the creation of a large number called a "message digest", or "hash", the exact value of which is determined by the layout of data found on a disk (MD5 can also be used to create message digests for files). Crucially, if the disk content is altered in any way, through deleting or changing a file for example, running the MD5 algorithm would result in a radically different message digest. This is true regardless of the extent of the alterations made; even a change to one bit of information on a large drive packed with data would result in a new message digest. md5sum is a freely available utility for creating MD5 message digests which, by comparing message digests of original disks and copies thereof, can be used in computer forensic examinations to ensure that an image made is an exact replica of the original.

The grep program allows files to be searched for a particular sequence of characters: the word "meeting" or the phrase "the meeting is at 4" for example. The real power of grep, however, lies in its ability to utilize metacharacters. Metacharacters are certain characters which have a special meaning to the grep program and allow great flexibility while searching.

For example the metacharacter "." (i.e., a full stop, without the quotation marks) means "any character" to grep, thus searching for "ca." might result in matches for "can", "cat", "cab" and so on if these sequences of characters were present in the file being searched. Grep has for a long time been one of the most useful tools for forensic investigators and as well as being a standard program on UNIX systems it is also included as a part of EnCase as well as of other known forensics tools[17].

In addition to shortly described non-commercial software for digital forensics, it is necessary and obligatory to stress out so called integrated forensics tools group, which integrate various (mentioned) non-commercial tools and their different combinations.

So, for example, SIFT workstation tool developed at the SANS Technology Institute (as a master's level graduate school in the USA) integrated among others Autopsy, Grep and Wireshark software, and iA3, developed at the Academy of Criminalistic and Police Studies, Belgrade, Serbia integrated only DD, Autopsy and Wireshark software.

COMMERCIAL TOOLS

There are a lot of commercial tools for digital forensics available in the market. Some of them are used only for creating the image and some for the analysis of images; most of commercial tools have both possibilities and more. In this part EnCase tool is described as the official tool in law enforcement in the USA and some other tools, which are the most used commercial tools, are only mentioned.

17 Forensic Focus, Jun 01, 2015, www.foren

EnCase, from Guidance Software, is a fully-featured commercial software package which enables an investigator to image and examine data from hard disks, removable media (such as floppy disks and CDs) and even Palm PDAs (Personal Digital Assistants). An investigation carried out with EnCase begins by using the software to create an image which can be analyzed later. It is possible to search the data for keywords, view picture files or examine deleted files. Many law enforcement groups throughout the world use EnCase and this can be an important factor for forensic investigators to consider where there is a possibility that an investigation may be handed over to the police or used in a court of law. EnCase is one of the more expensive commercial tools although a discount is available to the law enforcement community. EnScripts and customizable filters which allow examiners of all experience levels to quickly parse out relevant data for further review with pre-built EnScripts or by developing their own EnScript tools[18].

The Forensic Toolkit (FTK) by AccessData attempts to help the analyst by reducing large datasets to a subset of important information. FTK is a commercial product and can be purchased from AccessData. Advantage of FTK is very intuitive GUI which provides simple work for beginners[19].

Vogon International offers a range of commercial computer forensic software with a product line-up divided into imaging, processing and investigation software. The imaging software is used to create an exact replica of the data on a drive which can then be indexed by the processing software to allow fast searching by the investigation component. In broad terms Vogon's offering provides similar functionality to that of EnCase by simplifying the process of data imaging and searching for the examiner.

SafeBack is another commercial computer forensics program commonly used by law enforcement agencies throughout the world. SafeBack is used primarily for imaging the hard disks of Intel-based computer systems and restoring these images to other hard disks. It is a DOS based program which can be run from a floppy disk and is intended only for imaging, i.e. it does not include the analysis capabilities of EnCase or Vogon's forensic software.

It is necessary, beside shortly described software for digital forensics, to mention Ilook Investigator and HELIX from e-fence which is Knoppix Linux distribution.

COMPARISON OF INTEGRATED AND NON-INTEGRATED FORENSIC TOOLS

The possibilities of most integrated and non-integrated tools of digital forensics are compared in this paper. We compared integrated tools SIFT Workstation and iA3 and the non-integrated tools EnCase and FTK and in the end comparison of these two different groups of digital forensics tools will be carried out.

COMPARISON OF INTEGRATED FORENSIC TOOLS - SIFT WORKSTATION AND IA3

To find out what the possibilities of integrated digital forensics tools SIFT Workstation and iA3 tools are it is necessary to give a practical example comparing just these two tools and it will be the subject of the next part of this scientific work. For the purposes of this example

18 EnCase, Jun 05, 2015, www.encase.com
19 AccessData, Jun 05, 2015, www.accessdata.com

we used a USB memory, 512MB and therein lies the document "prazan.docx" and document "proba.docx" we previously deleted. In this particular case we compare the time which is necessary that these integrated tools of digital forensics do their bit by bit recording media.

In these examples, the timing that is needed to run some analyses or the features provided by these tools was measured. The speed start tool, the speed of acquisition of the media, evidence download speed, the speed of file analysis, the speed of search by keyword, the speed of search by file types, the speed of "live" analysis and the speed of drafting the report were measured for both integrated and non-integrated tools.

Before using a practical example to show the difference between the SIFT Workstation and iA3 tools, it is necessary to point out some quite significant differences between these tools. One of these differences is precisely that the SIFT Workstation can be started only by virtual machines which leads to that using this tool is impossible to perform live forensic analysis of data, as this causes a disruption of media. What distinguishes iA3 tool, which we designed in relation to the SIFT Workstation is that it can start live, from a USB drive or by using a "live" version of Windows To Go system where there is no access to or modification of the media or the data on them.

Another important difference between these two tools is that when taking pictures of the media "Put to death", to prepare and raise system to work SIFT Workstation certainly needs more time than it is necessary for the preparation and awareness tools iA3. From the foregoing, we conclude that these are two evident advantages of iA3 tool in relation to the SIFT Workstation.

This research was based on that and the emphasis is on measuring the time it takes to start programs. While iA3 tools start was instantly, it was much longer with the SIFT Workstation.

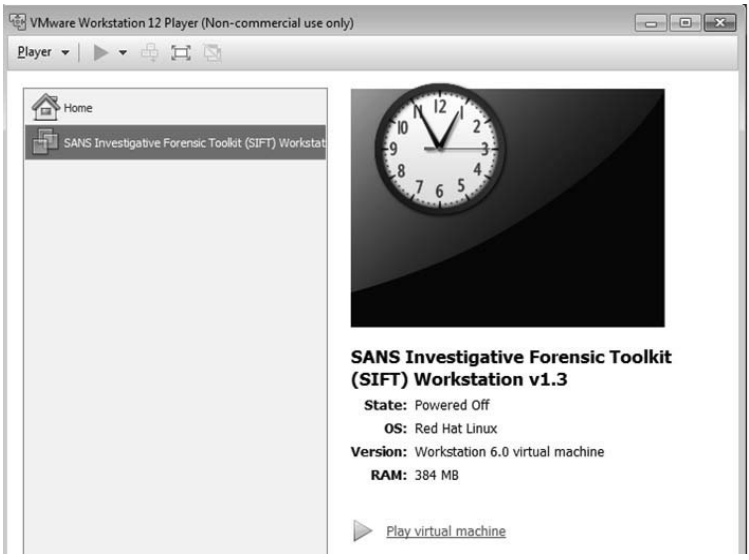


Figure 1: *Starting from the virtual machine*

Figure 2: *End of starting*

From the moment when a virtual machine started SIFTS Workstation until the moment when it was necessary to enter the username and password, it took 1 minute and 25 seconds.

Within the SIFT Workstation there is a special tool "GRAB" whose function is to record bit by bit media, the recording time of a USB drive makes the goal of this example. The recording process is initiated as indicated in the text above.

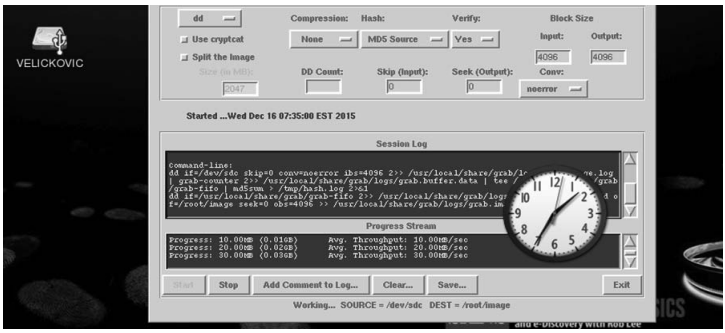


Figure 3: *Start of recording media*

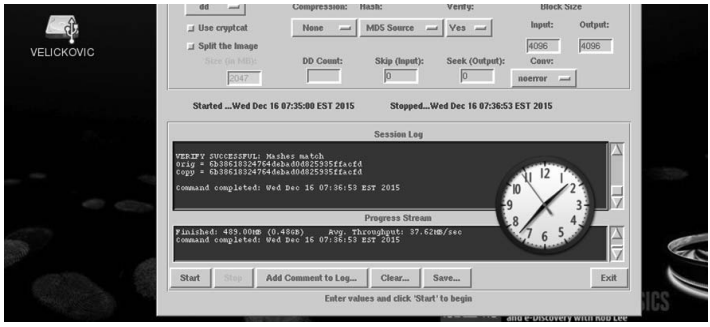


Figure 4: *End of recording media*

In iA3 the tool "DD" will be used for recording media, bit by bit. Starting the recording process is executed through the command which is explained in the previous chapter.

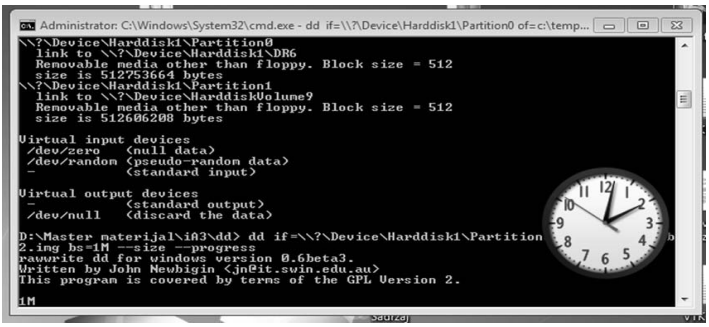


Figure 5: *Start of recording media*

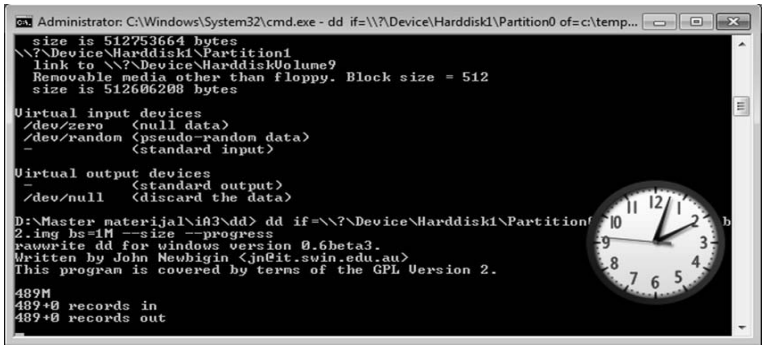


Figure 6: *End of recording media*

Because the SIFT Workstation and iA3 for the analysis of media use Autopsy, further in this paper some of the analyses will be shown and the time required to do the analysis of media in this tool using both software solutions.

The next thing that was measured is the time needed to load the files on which in a previous cas e the acquisition was made as is showed in pictures Figure 7 to Figure 16.

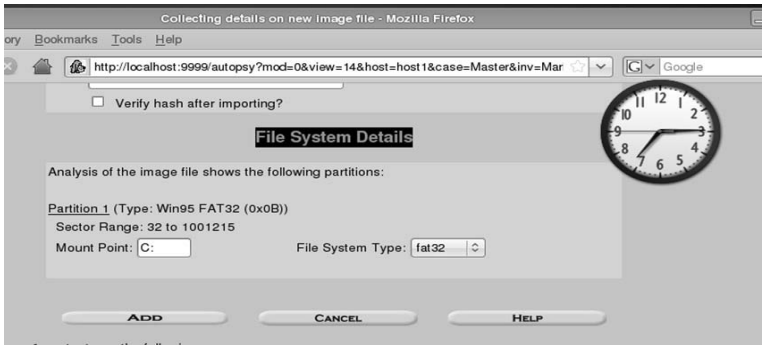


Figure 7: *Start of loading in Autopsy*

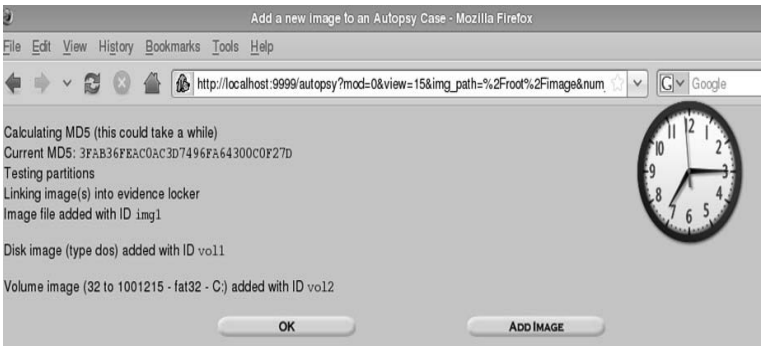


Figure 8: *Completion of loading in Autopsy*

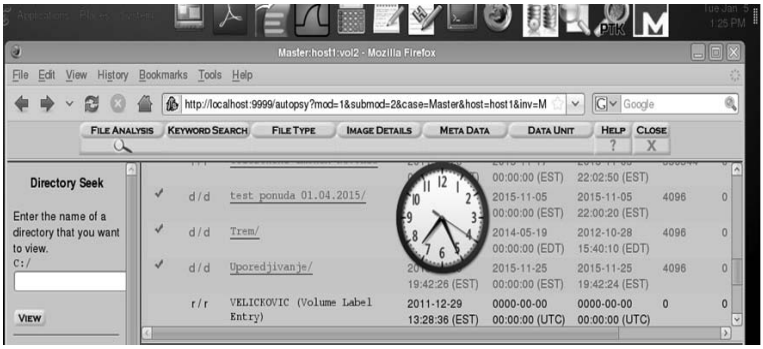


Figure 9: *Start of the analysis of the file in Autopsy*

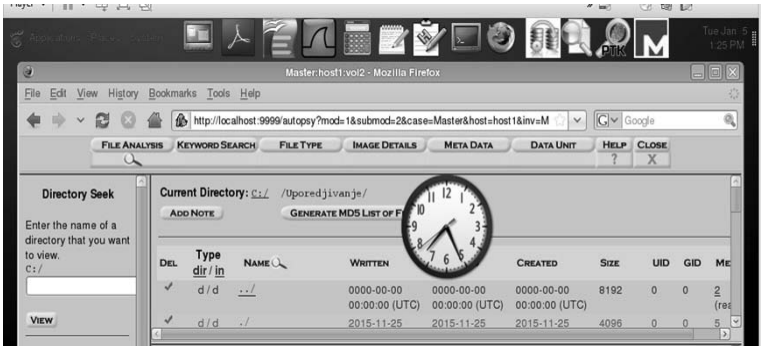


Figure 10: *Completing of the analysis of the file in Autopsy*

Figure 11: *Start of search keyword in Autopsy*

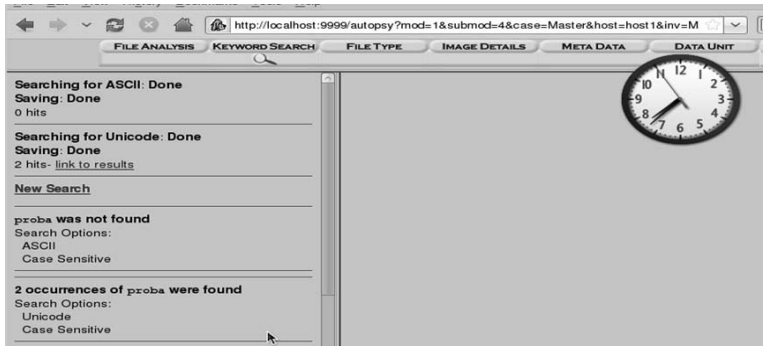


Figure 12: *Completion of search keyword in Autopsy*

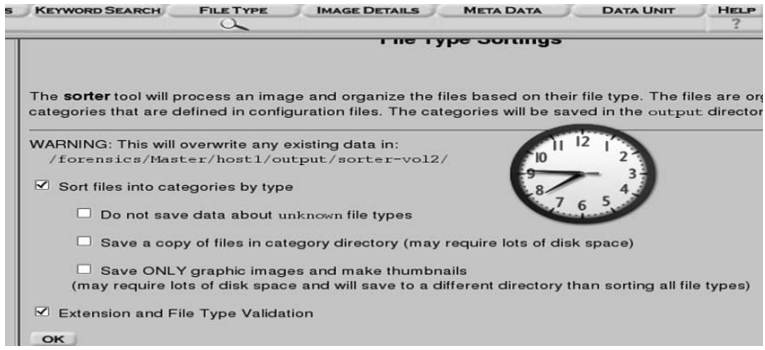


Figure 13: *Start of time per file types in Autopsy*

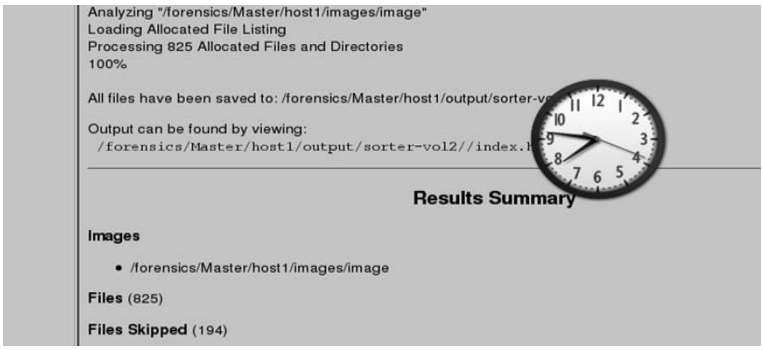


Figure 14: *Completion of searches by file types in Autopsy*

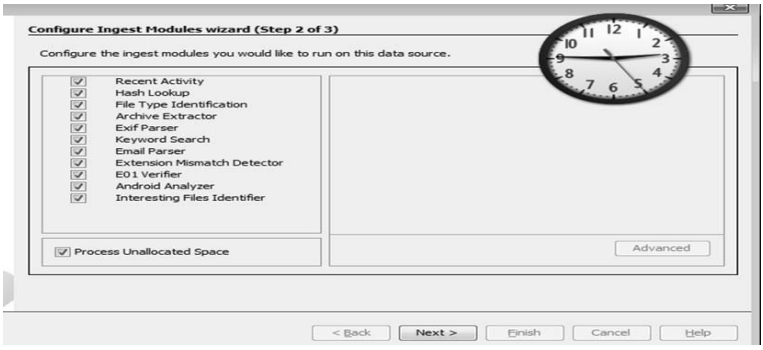


Figure 15: *Start of "live" analysis*

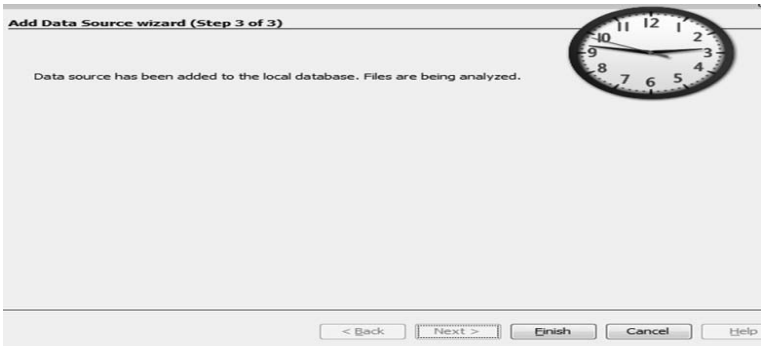


Figure 16: *Completion of "live" analysis*

Also, the time needed to produce a report in Autopsy was watched and it was immediately. The next chapter will show all the values obtained from these measurements and comparisons performed.

COMPARISON OF NON-INTEGRATED FORENSIC TOOLS – ENCASE AND FTK

One way to find out what the possibilities of digital forensics tools are is to compare them to a practical example and it is in this part of the paper where digital forensic tools EnCase and FTK are compared. For the purposes of this example a USB memory capacity 512MB was used and therein lies the document "prazan.docx" and document "proba.docx" we previously deleted.

As with comparisons of integrated tools, the measurement of the timing required to start these programs is also done here. In both programs the start was immediate.

The time needed to carry out the acquisition memory was also measured. In EnCase program after its initiation it is needed to click on Acquire in the top right corner, which opens the settings window for running analyses of USB memory.

Figure 17: *Appearance of the window EnCase and the button Acquire*

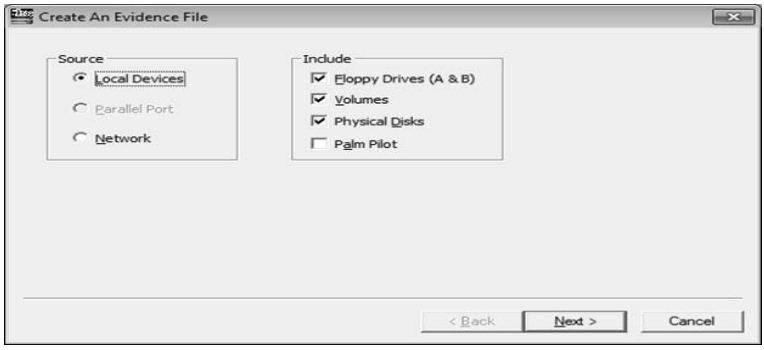


Figure 18: *Appearance of the window in which memory is selected to be analyzed*

After that it is necessary to mark the memory that will be analyzed, as in this case it was one USB stick, there was nothing more offered. This can be seen in Figure 18.

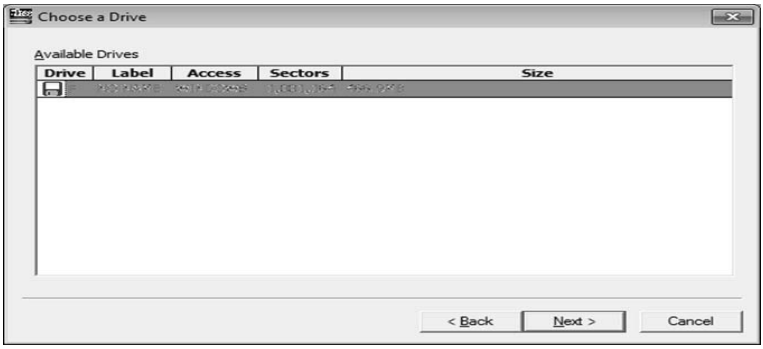


Figure 19: *Selecting the memory for analysis*

The next step is entering the number of investigation or case, who is the investigator, the number of the evidence, specific description, the exact time which is automatically entered and if necessary adding some more things that are relevant.

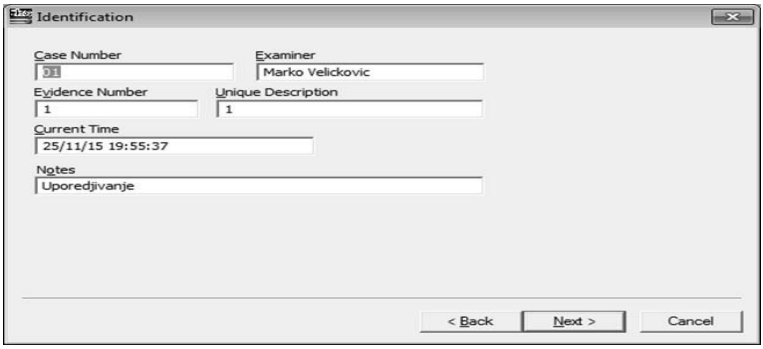


Figure 20: *Adding description*

The last step before the analysis is adjusting the options of the output file. It is necessary to choose between three modes of compression of the output file. In this case, the best option according to the program was chosen. There is also a possibility of setting up codes for greater protection, but it was not set in this case. There is also possibility to select a place where to locate the output file. All this is shown in Figure 21.

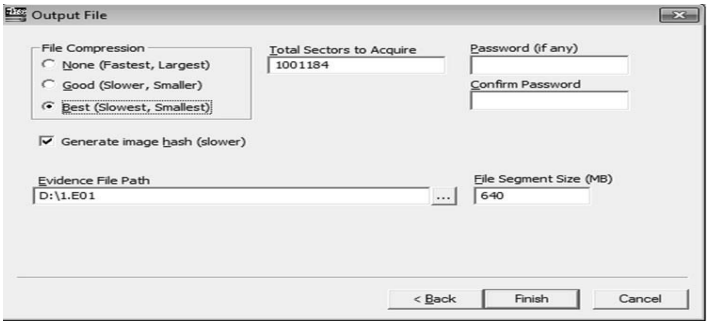


Figure 21: *Setting the output file*

When the process of the analysis of memory is completed, a new window that indicates that the memory is taken to a location we chose and that the time needed for that to be done for 1 minute and 45 seconds is opened. We can conclude that it is quite fast.

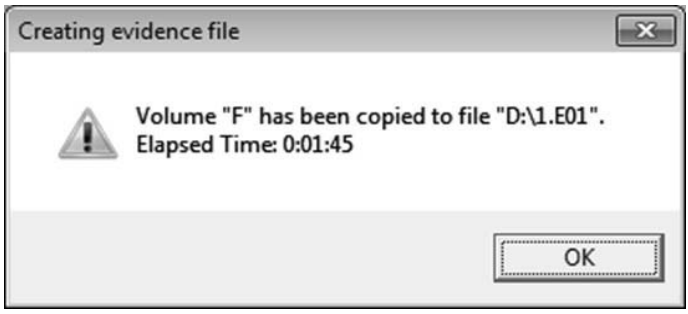


Figure 22: *Review of the information about the time of analysis.*

In the FTK program when opening tool we choose the option of a new case and then a window will be opened as shown in Figure 23. There is a form with fields to fill in who the investigator is, and information about the case as the case number, the name of the case and the place where the output file will be saved. We can also add a description of the case where we can enter everything that we think is important for the case.

Figure 23: *Filling in the case information*

After the necessary information are filled in, the window with more options that will determine what kind of analysis the file we want is opened. In these settings, we decide whether slack space, empty space, but also the filtering of files will be included in the analysis. We also decide if deleted files, encrypted files, and files with e-mail will be involved.

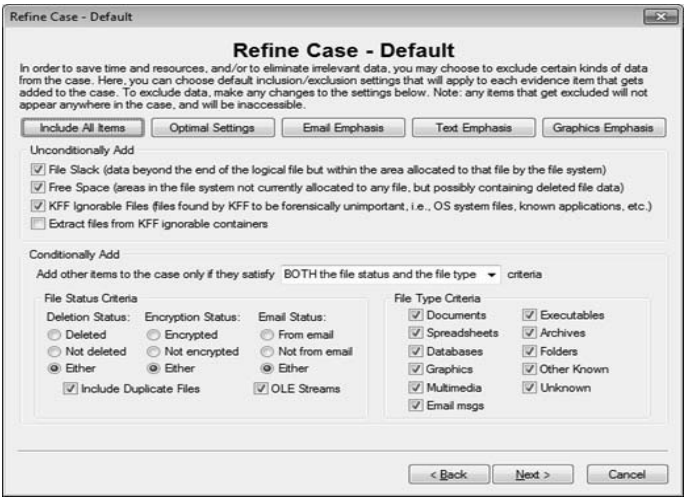


Figure 24: *Settings analyzes*

After everything needed for the analysis is set up, we access to memory adding respectively determining the location where the analysis will be done and where it will be looked for evidence. As in the previous case, in this case memory 512 was also used, and it is showed in Figure 25.

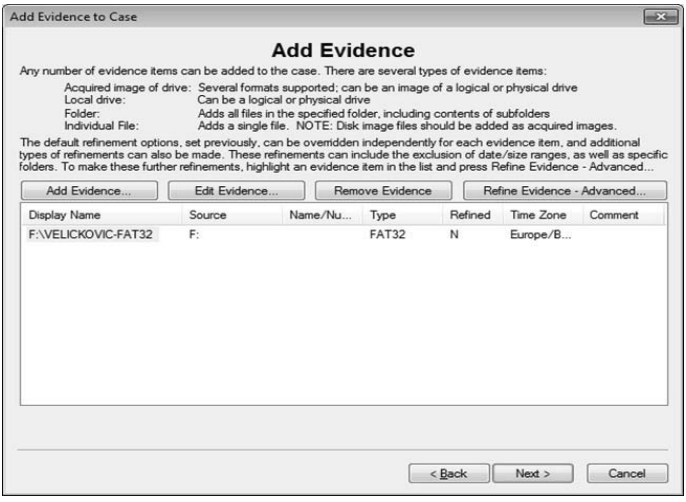


Figure 25: *Adding a location at which the analysis will be performed*

In the end of that by clicking on the "Next" button we initiate an analysis approval memory. Figure 26 shows the window where we can see how memory analysis looks. As we can see in the picture the analysis of this memory is done within 3 minutes and 45 seconds.

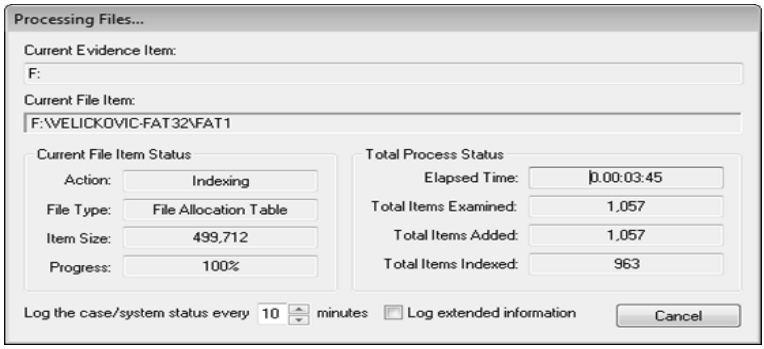


Figure 26: *Result of analysis*

Next step was to compare the time needed to load the data from media on which acquisitions are previously made and which are shown on Figures 27 to 38.

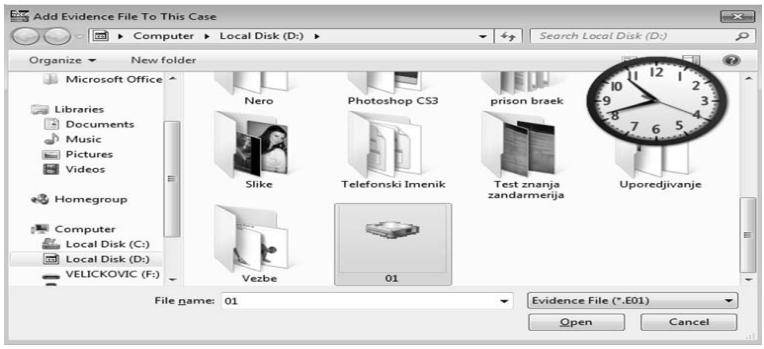


Figure 27: *Start of loading in EnCase*

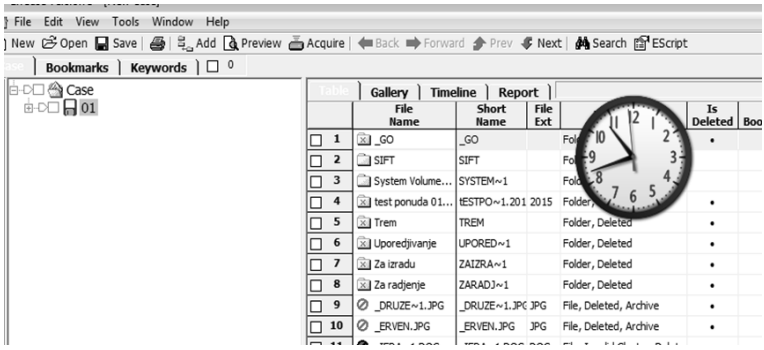


Figure 28: *Completion of loading in EnCase*

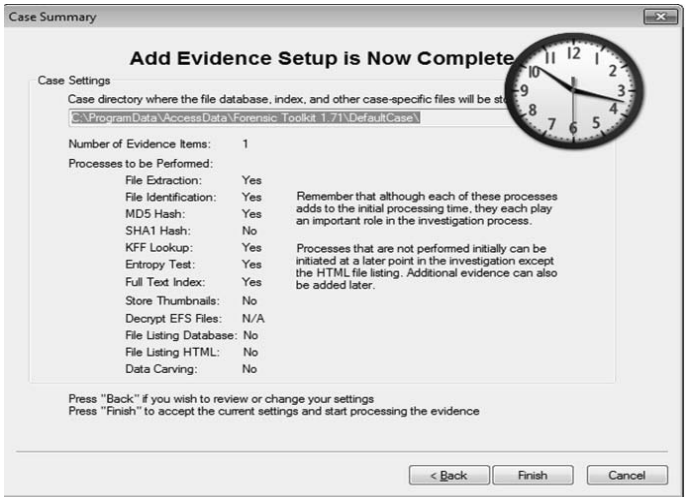


Figure 29: *Start of loading in FTK*

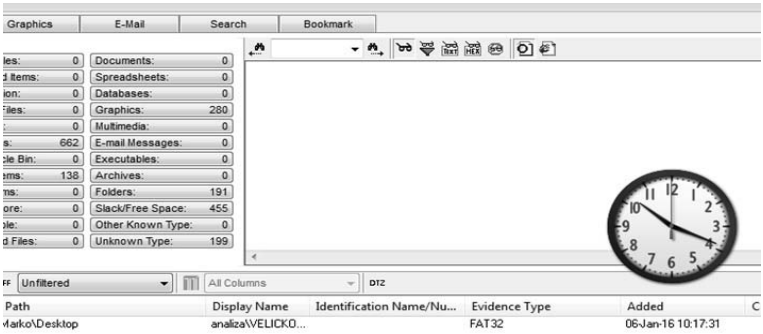


Figure 30: *Completion of loading in FTK*

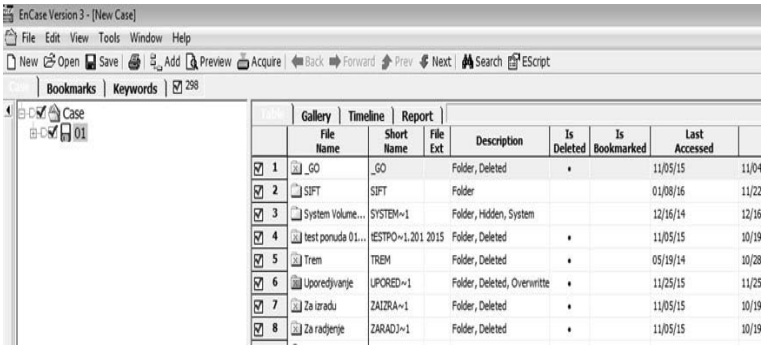


Figure 31: *Analysis of the file in EnCase*

Figure 32: *Analysis of the file in FTK*

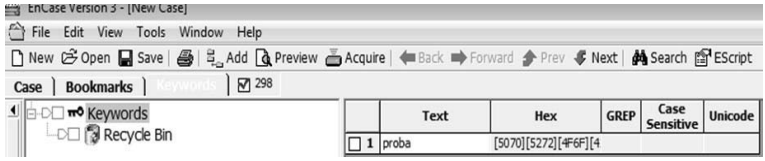


Figure 33: *Search by keyword in EnCase*

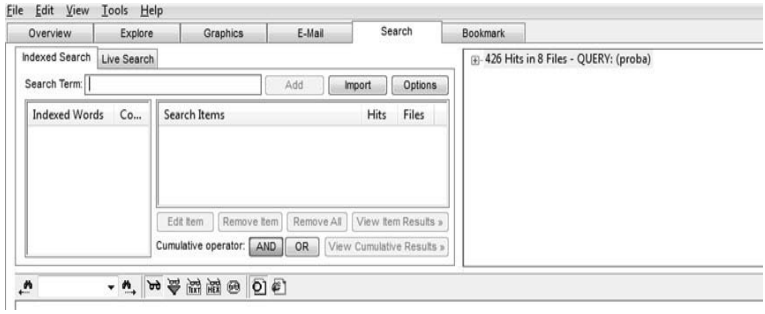


Figure 34: *Search by keyword FTK*

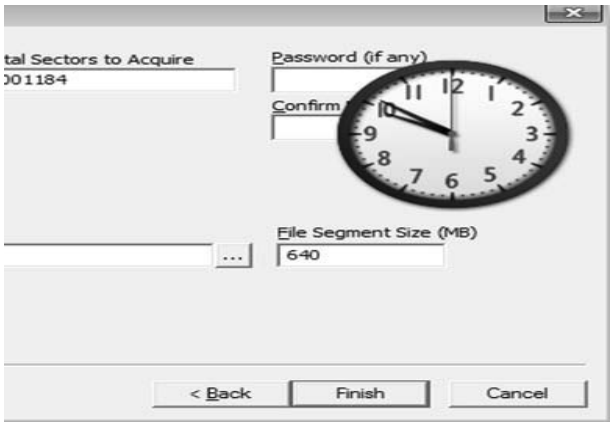


Figure 35: *Start "live" analysis in EnCase*

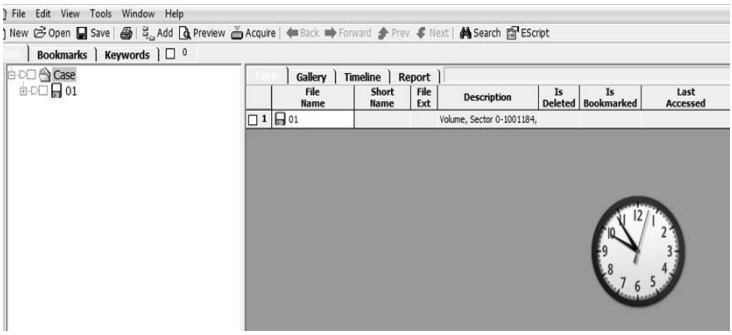


Figure 36: *Completion of "live" analysis in EnCase*

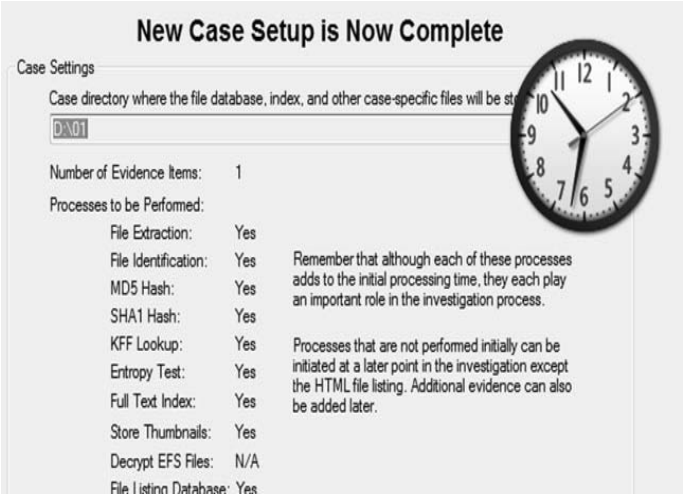


Figure 37: *Start of "live" analysis in FTK*

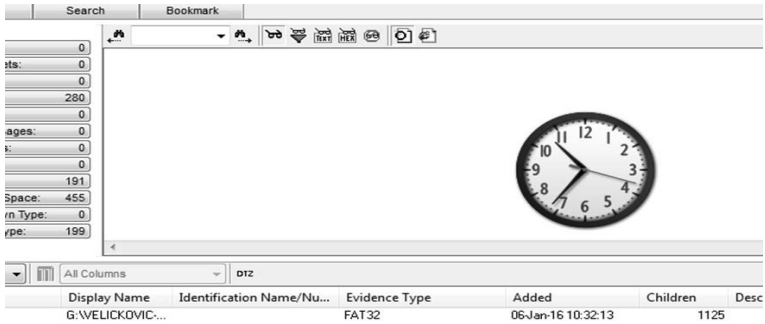


Figure 38: *Completion of "live" analysis in FTK*

In the next chapter all measurements will be shown and compared.

COMPARISON OF INTEGRATED AND NON-INTEGRATED TOOLS COMPARISON FROM THE TECHNICAL STANDPOINT

Table 1 shows the results obtained when measuring the speed that is needed to perform certain analyses. And here we see that every tool has its own advantages and disadvantages.

Table 1: *Comparison of the most important technical characteristics of integrated and non-integrated tools*

Type of analysis	iA3	SIFT	EnCase	FTK
Start	immediately	1 min 25 s	immediately	immediately
Acquisition	Seen 55 s	1 min 52 s	1 min 45 (up to)	3 min 45 s
Loading Image	14 s	14 s	39 s	1 min. 30 (up to)
Analysis of the file	19 s	19 s	immediately	immediately
Search by keyword	1 min 40 s	1 min 40 s	immediately	immediately
Search by file type	39 s	39 s	immediately	immediately
"Living" analysis	1 min 24 s	1min 24 s	3min 3 sec.	4 min 8 s
Preparing reports	immediately	immediately	immediately	immediately

As you can see, there are some differences in the speed of execution of the functions in these tools. When we talk about the difference in speed, it should be noted that this study was done on the USB memory of 512 MB, so that the differences are not manifested in a large amount. However, when analyzing the media in the tens of gigabytes, these differences would be much more expressed.

With integrated tools much more time is needed for image acquisition, but when uploading images this tool has shown better results compared to non-integrated. However, when we begin a process of analysis, we can see all the advantages of non-integrated tools, where this process is executed almost immediately, which greatly saves time which can sometimes be a resource that is not available in sufficient quantity.

On the market there are a lot of software solutions with the help of which it is possible to perform a forensic analysis of a medium. Which of the solutions users will decide to use in a particular case depends on the individual needs, values, data, technical equipment, training of personnel, resources that are available to it, etc.

In the earlier part of the article it is mentioned that the difference between integrated and non-integrated tools is that digital forensic tools are integrated collection of tools that are essential for a complete network monitoring, recording medium, detecting attacks on a network, search the Internet. Non-integrated tools do not contain more tools but only one which performs certain part of forensic analysis. It can be said that both tools have their advantages and disadvantages.

As for the integrated tools, we can say that just because we have a larger number of tools, we have better protected network, but also there is a possibility that if there is a particular attack we can investigate what happened by using a single integrated tool that in itself has all the necessary tools, while it is not possible to do so with a single non-integrated tool, but we will need more of them to achieve the same goal.

We are aware of the economic crisis that currently exists, and this aspect cannot be ignored, so we come to the conclusion that the SIFT Workstation and iA3 which are free programs are more cost-effective to use, but also because they contain all the tools required for network monitoring, and performance of forensic analysis if an attack occurs. FTK and EnCase are not free programs, and therefore are related to the high costs, and to ensure a full network require several different tools.

The advantage of iA3 and SIFT Workstation is that these programs are open source so they can constantly improve and adapt to specific customer needs.

EnCase and FTK as a non-integrated programs are more sophisticated than integrated, as they turn to training only one action that is needed to make the tool. In this way, these tools are a lot more sophisticated, but it takes a lot more knowledge of their use, economic resources, in comparison to integrated that are easy to use and quite cost effective.

This raises the question at the end, which tool should be given priority? It mostly depends on the needs and resources available. It is certainly better to use non-integrated, which are commercial tools, but in situations where the material resources are not available in sufficient quantity, the integrated tools can provide an excellent alternative.

COMPARSION OF APPLICABILITY

The tools mentioned in this paper, SIFT workstation as integrated tool and both of non-integrated tools–EnCase and FTK, are recognized and accepted by the courts of the USA on the basis of permanent positive Daubert test.[20] In order to determine whether the forensic tool

20 The Daubert standard provides a rule of evidence regarding the admissibility of expert witnesses' testimony during the United States federal legal proceedings. Pursuant to this standard, a party may raise a Daubert motion, which is a special case of motion *in limine* raised before or during trial to exclude the presentation of unqualified evidence to the jury. The Daubert trilogy refers to the three United States Supreme Court cases that articulated the Daubert standard:
I.Daubert v. Merrell Dow Pharmaceuticals, which held in 1993 that Rule 702 of the Federal Rules of Evidence did not incorporate the Frye "general acceptance" test as a basis for assessing the admissibility of scientific expert testimony, but that the rule incorporated a flexible reliability standard instead;
II.General Electric Co. v. Joiner, [1] which held that a district court judge may exclude expert testimony when there are gaps between the evidence relied on by an expert and his conclusion, and that an abuse-of-discretion standard of review is the proper standard for appellate courts to use in reviewing a trial court's decision of whether it should admit expert testimony;

iA3, which is developed at the Academy of Criminalistic and Police Studies, is acceptable to the court, or whether the evidence obtained with this tool are admissible in court Daubert test was used [21].

Daubert process identifies four general categories that were used as the main evidence in assessing acceptability of the tool in court:

1. Testing: Can it be tested and whether the procedure was tested?
2. Expectancy: Is there a known probability of error of the procedure?
3. Publications: Is the procedure public?
4. Acceptability: Are the procedures generally accepted by the relevant scientific community?

1. The software solution has been done according to the regulations of the Ministry of Education, Science and Technological Development, and the tool iA3 is tested by the Ministry of Internal Affairs (the Cybercrime Department). The tool testing started in 2015 and it is still being tested. After completion of the test the evaluation and the possibility of its admissibility in court will be given.
2. The probability of error, which refers to errors known as "bugs" in the work tools where not noticed while working with these tools and in the previous test.
3. The tool has been published in several publications:

1. Velickovic M .: Integrated digital forensics tools. Belgrade: Academy of Criminalistic and Police Studies, 2016[22].
2. Milanovic T., Kuk K., Randjelovic D., Čisar P.: Text mining techniques and identification of information by documents written (in Serbian) in High-end International Forum on Public Security Technology Informatisation, Shenyang, China, September 2015, pp. 575-583[23] .
3. Also, the tool is set up and is available on the website of the Academy of Criminalistic and Police Studies.

Based on everything mentioned above, we can say that iA3 is pretty good software solution that could be accepted in court.

ACKNOWLEDGEMENTS

This work was supported by the Ministry of Science and Technology of the Republic of Serbia under the Project no. III 44007 and TR34019.

III.Kumho Tire Co. v. Carmichael, [2] which held in 1999 that the judge's gatekeeping function identified in Daubert applies to all expert testimony, including that which is non-scientific. https://en.wikipedia.org/wiki/Daubert_standard

21 Fradella, H.F., O'Neill, L., and Fogarty, A. (2004) The Impact of Daubert on Forensic Science, 31 Pepp. L. Rev. Iss. 2

22 Velickovic, M .(2016). Integrated digital forensics tools. Belgrade: Academy of Criminalistic and Police Studies

23 Milanovic, T., Kuk, K., Randjelovic, D., Čisar, P.(2015). Text mining techniques and identification of information by documents written (in Serbian) in High-end International Forum on Public Security Technology Informatisation, Shenyang, China, September 2015, pp. 575-583

REFERENCES

1. AccessData, Jun 05, 2015, www.accessdata.com
2. Altheide, C., and Carvey, H. (2011). *Digital Forensics with Open Source Tools*. Massachusetts: Elsevier.
3. Brown, L. T. (2010). *Computer Evidence: Collection and Preservation, Second Edition*. Boston: Course Technology.
4. Casey, E. (2004). *Digital Evidence and Computer Crime, Second Edition*. London: Academic Press.
5. Carvey, H. (2009). *Windows Forensics Analysis*. USA: Syngress Publishing, Inc.
6. EnCase, Jun 05, 2015, www.encase.com
7. Forensic Focus, Jun 01, 2015, www.foren
8. Fradella, H.F., O'Neill, L., and Fogarty, A. (2004) The Impact of Daubert on Forensic Science, 31 Pepp. L. Rev. Iss. 2
9. Ignjatović, Đ. (1991). *Pojmovno određenje kompjuterskog kriminaliteta*. Beograd: Anali Pravnog fakulteta u Beogradu.
10. McClure, S., Scambray, J., Kurtz, G. (2006). *Хакерске тајне: заштита мрежних система*. (превод), Београд, Микро књига.
11. Milanovic, T., Kuk, K., Randjelovic, D., Čisar, P.(2015). *Text mining techniques and identification of information by documents written* (in Serbian) in High-end International Forum on Public Security Technology Informatisation, Shenyang, China, September 2015, pp. 575-583 .
12. Milosavljević, M., & Grubor, G. (2009). *Digitalna forenzika - udžbenik*. Beograd: Univerzitet Singidunum.
13. Milosavljević, M., & Grubor, G. (2009). Istraga kompjuterskog kriminala. Beograd: Univerzitet Singidunum.
14. Newman, C. R. (2007). *Computer Forensics: Evidence, Collection and Management*. New York: Auerbach Publications.
15. Pastore, M., & Dulaney E. (2007). Security + (prevod na hrvatski), Miš d.o.o.
16. Petrović, R. S. (2000). *Kompjuterski kriminal*. Beograd: Ministarstvo unutrašnjih poslova Republike Srbije.
17. Ranđelović, D., & Bogdanović, T. (2010). *Alati za digitalnu forenziku*, NBP - Žurnal za kriminalistiku i pravo, Vol. XV, No. 2, 25-47.
18. Randjelović, D., Delija, D., Popović. B. (2009). *EnCase forenzički alat*,
19. Bezbednost 1-2, pp. 286-312.
20. Randjelović D. (2011). *Poredjenje komercijalnih i nekomercijalnih alata digitalne forenzike i njihova upotreba* Naucno tehnicka informacija, VojnoTehnicki Institut Beograd.
21. Randjelović, D. (2013). *Visokotehnološki kriminal*. Kriminalističko-policijska akademija, Beograd.
22. Vacca, R. J. (2005). *Computer Forensics: Computer Crime Scene Investigation, Second Edition*. Massachusetts: Charles River media.
23. Velickovic, M .(2016). *Integrated digital forensics tools.* Belgrade: Academy of Criminalistic and Police Studies.

UDC: 341.456:[343.533::004(4)

EUROPEAN CYBERCRIME CENTRE

Snezana Nikodinovska-Stefanovska, PhD[1]
Faculty of Security, Skopje

Abstarct: The European Cybercrime Centre (EC3) was established under the umbrella of Europol to strengthen the law enforcement response to cybercrime in the European Union (EU) and to help protect European citizens, businesses and governments. EC3 commenced its activities in January 2013. Its establishment was a priority under the EU Internal Security Strategy. The threat from cybercrime is increasing and the EU is a key target mainly due to its advanced Internet infrastructure as well as its internet-based economies and payments systems. It is to act as the focal point in the fight against cybercrime in the European Union. Using a "shared, cross-community approach" the EC3 is concluding partnerships with member states, European agencies, international partners and the private sector.

This paper considers the main features of the new Directive on attacks against information systems. The paper also describes the coming about of EC3, its key features and its efforts to address cybercrime. Furthermore, the paper highlights how far Europol's robust data protection regime contributes to effectively fighting cybercrime while duly observing fundamental rights including the right for protection of personal data.

Keywords: cybercrime, European Cybercrime Centre, Europol, data protection regime, right to protection of personal data.

INTRODUCTION

New technologies have become an important part of the everyday lives of European Union citizens, companies, organisations and authorities. But with EU citizens' growing dependence on these technologies also comes growing opportunities for criminals. Criminals can threaten the security of nation states and/or the civil liberties of their citizens. Organised criminals exploit cyberspace to steal money or to commit fraud. They also break into computer networks in order to steal data or business secrets or simply to destroy documents. Cybercrime can damage essential infrastructure on which society depends, affecting health, safety, or security, but also infrastructure vital for economic or social well-being (such as power plants, transport networks and government networks).

The year 2001 marked a very important date in the fight against cybercrime not only at the European but also at the global level. In Budapest, on 23 November 2001, the Council of Europe Convention on Cybercrime, also known as the "Budapest Convention", was signed by 30 countries, including non-members of the Council of Europe such as Canada, United States, Japan and South Africa.[2] It defined a series of crimes such as illegal access, system and data interference, and illegal interception and set out rules concerning jurisdiction and criminal investigative measures. After fifteen years, the Council of Europe Convention on Cybercrime remains today a key instrument providing minimal legal and procedural standards for

1 E-mail: snikodinovska@gmail.com.
2 Council of Europe Convention on Cybercrime, Budapest 21.XI.2001 (ETS 185).

fighting cybercrime. The European Union acknowledged the importance of the Cybercrime Convention and has encouraged EU Member States to ratify it.

At the EU level, various attempts have been made to harmonise cybercrime legislation across the region. For the past ten years the European Union has made important efforts to develop an adequate legal framework to address the challenge of cybercrime.

The two major "hard law" legal instruments addressing this issue were adopted in mid-2000s and consisted of two EU Framework Decisions – Council Framework Decision on combating the sexual exploitation of children and child pornography[3] and the Council Framework Decision on attacks against information systems[4]. Both measures aimed at establishing minimum rules concerning the definition of criminal offences and sanctions in the areas of attacks against information systems and child pornography on the internet. However, in light of the profound changes brought by Information and Communication Technologies (ICTs), both instruments have been under intensive discussion among EU Member States. Thus, in 2011 the Directive on combating the sexual abuse and sexual exploitation of children and child pornography was adopted.[5] Also, the new Directive on attacks against information systems which repealed the 2005 Framework Decision was adopted at the end of 2015.[6] After its adoption, EU Member States have two years to bring into force the laws, regulations and administrative provisions necessary to comply with both Directives ("transposition" phase).

At operational level, the creation of the European Network and Information Security Agency (ENISA) in 2004 was followed more recently with the creation of the European Cybercrime Centre. Hosted by Europol, EC3 is intended to become the main point in the EU's fight against cybercrime, by supporting Member States and the European Union's institutions. It started its activities in January 2013.

This paper considers the main features of the new Directive on attacks against information systems, as well as establishment, performance and future perspective of the European Cybercrime Centre, particularly its outreached function. Furthermore, the paper highlights how far Europol's robust data protection regime contributes to effectively fighting cybercrime while duly observing fundamental rights including the right to protection of personal data.

THE NIS DIRECTIVE – MAIN CHARACTERISTIC

In recent years, the number of cyber-attacks against information systems has risen dramatically in Europe and around the world. Previously unknown large-scale threats to the information systems of companies, banks, and the public sector have been observed in the Member States and other countries. A particular concern was raised by the spread of malicious software creating "botnets" – networks of infected computers that can be remotely controlled to stage large-scale, coordinated attacks.[7]

3 Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography (OJ L 13 of 20 January 2004, p. 44).
4 Council Framework Decision 2005/222/JHA on attacks against information systems (OJ L 69 of 16 March 2005, p. 67).
5 Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335/1 of 17 December 2011).
6 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218/8, 14/8/2013. It was adopted in accordance with the new ordinary procedure set by the Lisbon Treaty in Article 82 that places the European Parliament on an equal footing with the Council of the EU.
7 The term botnet indicates a network of computers that have been infected by malicious software (computer virus). Such network of compromised computers ("zombies") may be activated to perform

On 24 February 2005, EU Member States agreed a Council Framework Decision that addresses the most significant forms of criminal activity against information systems, such as hacking, viruses and denial of service attacks. The Framework Decision seeks to approximate criminal law across the EU to ensure that Europe's law enforcement and judicial authorities can take action against this form of crime. It was a first step towards addressing the issue of attacks against information systems.

Technological advances and new methods employed by perpetrators call for an improvement of EU rules. In addition, the entry into force of the Lisbon Treaty on 1 December 2009 provides considerable advantages for new legislation to be adopted in the field of Justice and Home Affairs from now on[8].

The second half of the 2000s marked a decisive change of pace in the EU fight against cybercrime. After the Estonian cyber-attack in April-May 2007, the European Union started focusing on issues such as "large scale cyber-attacks" and "botnets". The Commission Communication "Towards a general strategy on the fight against cybercrime", adopted on 22 May 2007 indicated as key operational priorities an effective dialogue with industry (public/private partnership) and a coordinated financial support for training and research activities in the field of cybercrime.[9]

In the Commission's report of 14 July 2008 it was stated that several "emerging threats have been highlighted by recent attacks across Europe since adoption of the Framework Decision, in particular the emergence of large-scale simultaneous attacks against information systems and increased criminal use of so-called 'botnets'." These attacks were not the centre of attention when the Framework Decision was adopted. In response to these developments, the Commission has considered actions aimed at devising better responses to the threat.

Still, at political level, precise reference to the fight against cybercrime was made in the third multi-annual Programme in the area of freedom, security and justice, known as "the Stockholm Programme"[10], which was endorsed by the European Council in December 2009[11]. The Programme priorities were reflected in the 2010 European Commission's Action Plan setting out concrete implementing measures and actions together with a timetable for their adoption. Regarding the fight against cybercrime, as general orientations set out in the Programme, the European Commission and Europol were invited to take measures for enhancing/improving public private partnerships and to step up strategic analysis on cybercrime, while all Member States were called upon to improve judicial cooperation in cybercrime cases.[12]

---

specific actions such as attacks against information systems (cyber-attacks). These "zombies" can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This "controlling" computer is also known as the "command-and-control centre". The people who control this centre are among the offenders, as they use the compromised computers to launch attacks against information systems. It is very difficult to trace the perpetrators, as the computers that make up the botnet and carry out the attack, might be located elsewhere than the offender himself. See more at: http://europa.eu/rapid/press-release_MEMO-13-661_en.htm.

8 Legislation no longer needs to be approved unanimously by the EU Council. Instead, it is adopted by a majority of Member States at the Council together with the European Parliament. A single country is not able to block a proposal. Implementation at national level is also improved. The Commission is now able to monitor how Member States apply EU legislation. If it finds that EU countries violate the rules, it will be in a position to refer the case to the European Court of Justice.

9 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cybercrime (COM(2007)267 final).

10 The Stockholm Programme – An open and secure Europe serving and protecting the citizens. Presidency Conclusions – Brussels, 10–11 December 2009 (Council of the European Union, Brussels, 3 March 2010, doc 5731/10).

11 European Council 10–11 December 2009 – Conclusions, Brussels, 11 December 2009 (EUCO 6/09).

12 The Stockholm Programme…, *op.cit.,* p. 79.

However, cybercrime was established as serious crime with a cross-border dimension in 2009, by including "computer crime" in Article 83(2) of the new Lisbon Treaty, in the same category as similarly severe crimes: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment and organised crime.[13]

In 2010, the EU presented the Digital Agenda for Europe, the first flagship initiative adopted under the Europe 2020 strategy.[14] The Agenda recognised the need to address the rise of new forms of crime, in particular cybercrime, at European level.

The Directive on attacks against information systems (NIS Directive) also known as the Cybersecurity Directive was first proposed in February 2013 by the European Commission as a significant part of EU Cybersecurity Strategy.[15]

The aim of the proposed Directive is to ensure a high common level of network and information security (NIS). This means improving the security of the Internet and the private networks and information systems underpinning the functioning of EU's societies and economies. This will be achieved by requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures, such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc.), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

The NIS Directive, repealed the 2005 Framework Decision (FD), but retained provisions from the FD such as the penalisation of illegal access, illegal system interference and illegal data interference, but also included the following new elements:

- Penalisation of the use of tools (such as malicious software – e.g. "botnets" – or unrightfully obtained computer passwords) for committing the offences. The Directive includes provisions for use of specific software "botnets" as a method of committing cybercrimes making it a criminal offence and also increasing the maximum penalty for offenders.

- Introduction of "illegal interception" of information systems as a criminal offence. Ensuring consistent EU-wide penalisation of illegal access, system interference and data interference will strengthen the protection of personal data by reducing the ability of cybercriminals to abuse victims' rights without impunity. EU law enforcement authorities will therefore be provided with enhanced tools to fight cybercrime.

- Improvement of European criminal justice/police cooperation strengthening the existing structure of 24/7 contact points, including an obligation to answer within 8 hours to urgent request. The Directive calls for Member States to ensure that they have an operational national contact point for the purpose of exchanging information and responding to urgent requests for assistance from other Member States.

- Obligation to collect basic statistical data on cybercrimes. The Directive calls for Member States also to implement a system for gathering statistical data on cyber-attacks.

13 Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European (2010/C 83/01), OJ C 83, 30 March 2010.
14 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe (COM(2010)245, 19 May 2010).
15 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 2013/0027 (COD). Available at: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/1_directive_20130207_en.pdf (accessed 10/12/2015).

The Directive also raises the level of criminal penalties of offences committed within the framework of a criminal organisation (maximum penalty of at least five years) and adds new aggravating circumstances:

- when a significant number of information systems have been affected through the use of a tool (e.g. "botnets") (maximum penalty of at least three years);

- when causing serious damage (maximum penalty of at least five years);

- when committed against a critical infrastructure information system (maximum penalty of at least five years).[16]

Instigation, aiding, abetting and attempting those offences became penalised as well.

Incident reporting is an important requirement of the NIS Directive. Groups within the scope of the NIS Directive must notify a central authority of incidents that could significantly impact the continuity of services. Public disclosure may occur at the discretion of the controlling authority when public awareness is necessary to prevent or handle an incident. Notification of an incident must be made to authorities "without undue delay", normally expected within 24–72 hours after the breach is discovered.

NIS empowers authorities to audit private industry for suspected non-compliance. Enforcement will be combined with related regulations. This includes the European General Data Protection Regulation, which outlines security requirements and requires privacy breach reporting, subject to penalties and fines.

Recognizing that threat intelligence sharing is critical in the response to cybercrime, the NIS directive also calls for the establishment of a cooperation network to coordinate cyber defence efforts, in particular where a cross-border issue is at stake. This will include sharing early warning threat intelligence between national authorities.

Finally, entities within the scope of the NIS Directive must implement "state-of-the-art" security measures that "guarantee a level of security appropriate to the risk". This suggests that entities within the scope of NIS need to consider and adopt behavioural-based detection systems that are now the modern standard for advanced attack prevention.

The NIS Directive was adopted at the end of 2015. Each member state has 21 months to complete implementation. The states will then have another six months to identify operators of essential services that are within scope, and these operators must also comply with the Directive's security requirements. For EU governments, the NIS Directive now requires that each member state adopt a national cyber security strategy. This includes creating a policy and regulatory environment for information security and the creation of a national Computer Security Incident Response Team (CSIRT).

Directive is a significant achievement that will shape the European cybersecurity landscape. The NIS Directive provides an EU-level harmonized approach to cybersecurity, embracing every EU member state and a wide group of "operators of essential services" that are active in energy, transport, banking, financial services, healthcare and other critical industry segments. These operators must now prepare to implement the Directive's requirements to ensure compliance and avoid potential penalties. Although the NIS EU Directive cannot be seen as a panacea for all crimes committed on the Internet, it can be considered as an important tool in the fight against cybercrime.

16 European Commission MEMO Questions and Answers: Directive on attacks against information systems, Strasbourg, 4 July 2013. Available at: http://europa.eu/rapid/press-release_MEMO-13-661_en.htm (accessed on 10/12/2015)

THE ESTABLISHMENT OF EC3 – A NEW, INNOVATIVE STEP

The establishment of the European Cyber Crime Centre was a first important step on a European level to address the growing threat from cybercrime. The EC3 became a reality shortly after the European Commission's proposal to establish a European Cyber Crime Centre in 2010 as part of the EU Internal Security Strategy. Its establishment was a priority under the EU Internal Security Strategy which identifies five strategic objectives including, for 2013, the establishment of the European Cybercrime Centre.[17] Namely, the Strategy identifies a number of significant common threats such as Cybercrime "which represents a global, technical, cross-border, anonymous threat to our information systems and, because of that, it poses many additional challenges for law-enforcement agencies".

The proposal was followed by a feasibility study on the possibility of creating a Cybercrime Centre to perform a number of tasks in the fight against cybercrime. This study published in February 2012 served as the basis of the communication on a European Cyber Crime Centre recommending the establishment of a European Cyber Crime Centre to be set up within Europol.[18] Soon after, on 28 March 2012, the European Commission adopted a Communication titled: "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre".[19]

The Centre, commonly referred as "EC3" was established within the European Police Office (Europol) in The Hague. It has to be noted that the 2009 Council Decision establishing Europol already conferred to the EU Agency the competence to cover computer crime.[20] By situating the EC3 within Europol the Centre was able to not only draw on Europol's existing law enforcement capacity but also to expand significantly on other capabilities, in particular the operational and analytical support to Member States' investigations.[21] A decisive argument was that the organization is already at the present stage tasked to counter cybercrime by various methods and means in a data protection compliant manner and has considerable experience in handling sensitive information.

The main functions of the EC3 are primarily focused on three areas:

- cybercrimes committed by organised groups, particularly those generating large criminal profits such as online fraud;

- cybercrimes which cause serious harm to the victim such as online child sexual exploitation;

- cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the European Union.[22]

With regard to these three areas, Europol's EC3 five main functions are:

Data fusion

- gathering and processing information on cybercrime

- providing a cybercrime helpdesk for law enforcement in all EU States

17 Communication from the Commission to the European Parliament and the Council – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010)673, p. 9).
18 Feasibility study for a European Cybercrime Centre, Final Report, February 2012. Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre_en.pdf#page=1&zoom=100 (accessed on 15/12/2015).
19 Communication from the Commission to the Council and the European Parliament – Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM(2012) 140 final, 28/3/2012).
20 See Article 4 of Council Decision of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121 of 15 May 2009, p. 37).
21 Combating Cybercrime in a Digital Age. Available at: https://www.europol.europa.eu/ec3, accessed on 15/12/2015).
22 *Ibid*.

Operations

- supporting cybercrime investigations in EU States (e.g. against intrusion, fraud, online child sexual abuse, etc.)

- supporting joint investigations carried out by more than one EU State (technical, analytical and forensic expertise)

- facilitating law enforcement cooperation with partners outside the EU and coordinating complex transnational cases in close collaboration with Eurojust (EU agency for judicial cooperation) and Interpol[23]

Strategy

- producing threat assessments, including trend analyses and forecasts as well as new developments on the ways cybercriminals operate

- R&D (research and development) and training

- collaborating closely with CEPOL (European Police College) to develop training activities and raise awareness on cybercrime issues

- facilitating research and development and ensuring capacity building among law enforcement, judges and prosecutors

- developing forensic tools to help EU States better detect and prosecute cybercrime

Outreach

- working closely with the private sector, research community, civil society, academia and Computer Emergency Response Teams to detect and respond comprehensively to cybercriminal activity

- alignment of actions with other relevant international partners, such as EUCTF (European Union Cybercrime Taskforce), CIRCAMP (COSPOL Internet Related Child Abusive Material Project), ENISA (European Network and Information Security Agency) and ECTEG (European Cybercrime Training and Education Group).[24]

The expected impact or the results which are expected to be delivered are:

- more cybercrime networks dismantled and more suspects prosecuted;
- better detection and forensic tools for cybercrime investigators;
- specialised threat assessments for the law enforcement community;
- cooperation with the private sector and the research community;
- more focused training for law enforcement, judges and prosecutors to better handle complex cyber issues;
- a more unified voice for cybercrime investigators on the international scene,
- the Internet economy will continue to grow, with less financial losses due to cybercrime;

23 Interpol, the world's largest international police organization with 190 member countries, has set up a cybercrime centre, Interpol Global Complex for Innovation (IGCI), in Singapore. The centre started its operations in 2015 marking the transition of global policing into the digital age. This step was eventually triggered as a result of Europol's innovative effort to tackle cybercrime in a more systematic manner, the latter being first mover in the area on a European level with the establishment of the EC3. On 25 September 2013 Europol and Interpol held their first joint Cybercrime Conference with the aim of enhancing international cooperation to tackle existing and future challenges in policing cyber space. The borderless nature of cybercrime requires a global alliance in the fight against cybercrime. As stated in the first IOCTA report (Internet Organised Crime Threat Assessment, Executive Report 2014), law enforcement should concentrate on pro-active, intelligence-led approaches to combatting cybercrime through existing platforms such as the EC3 and Interpol's Global Complex for Innovation.

24 European Cybercrime Centre (EC3). Available at: http://ec.europa.eu/dgs/home-affairs/e-library/docs/infographics/cyber-crime/european_cybercrime_centre_infographics.pdf (accessed on 20/12/2015).

- EU citizens will be more secure (from fraud, intrusion, etc.) and feel more confident while conducting their lives online.[25]

Less than a year after it became operational, the EC3 was already going strong. According to the first annual report of EC3, several analytical products had been produced focusing on the dark net and deep web, including bitcoins and the digital underground economy. In addition, several knowledge products had been produced for the Member States' competent authorities, for instance, the so-called ransomware report and action plan, the strategic assessment on commercial exploitation of children online and the situation report on payment card fraud in the EU.[26]

Tackling cybercrime demands a different approach including new partners to be integrated into existing cooperation frameworks as it is the case with the EC3. The EC3 should become the European Union's focal point in the fight against cybercrime, responding to queries on specific technical issues from cybercrime investigators, prosecutors and judges, as well as the private sector, and providing operational support in concrete investigations. The EC3's added value lies in its focus on major strands of cybercrime, such as fighting online fraud generating large criminal profits, online child sexual abuse material, and cyber-attacks affecting critical infrastructure and information systems in the EU.

THE OUTREACHED FUNCTION: A SHARED CROSS-COMMUNITY APPROACH

A key novelty of the EC3 is its preparedness to exchange information with (and respond to queries from) partners that go beyond the law enforcement community. Such a shared cross-community approach, that will embrace also the know-how of other partners such as Eurojust, CEPOL, ENISA and the private sector/internet industry, to tackling cybercrime is without doubt one of the key features of the EC3.

High-tech crimes cannot be adequately investigated, prosecuted and adjudicated upon without cooperation with the private sector. Dialogue with Internet service providers and Internet industry players is a key for law enforcement authorities, judges and prosecutors to be able to prevent, detect and respond to crimes committed using information and communication technologies facilities. Therefore it is crucial to initiate such dialogue and start facing new complex issues of international relations related to national sovereignty and territoriality. According to a study from the European Parliament, "we are now dealing with a triangular diplomacy between states, companies and the inter-state system in the global regulation of the Internet".[27] It is obvious that, since cyberspace and the Internet's infrastructure are for the most part owned by the private sector, only a shared, cross-community approach could bring enduring results in the fight against cybercrime. Thus, the EC3 is in charge of a so-called "outreach function". This outreach function both develops and maintains partnerships that can contribute to the EU Member States response to cybercrime in order to facilitate such cooperation, strengthen partnerships among various sectors, including the development of forums and projects and public-private partnerships at national and international levels.

25 European Cybercrime Centre (EC3). Available at: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report (accessed on 20/12/2015).
26 See more: EC3 first year report. Available at: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report (accessed on 20/12/2015).
27 European Parliament, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Study 2012, Fighting cybercrime and protecting privacy in the cloud. Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/study_cloud_/study_cloud_en.pdf (accessed on 17/12/2015).

The outreach function further includes the "proactive identification of new partners where required and cooperation with law enforcement agencies, EU institutions, international organizations, private industry, the public sector and academia".[28] Also, this issue seems to be adequately stressed by the Communication on the establishing of the EC3 that clearly states: "Building trust and confidence between the private sector and law enforcement authorities is of utmost importance in the fight against cybercrime".[29]

Thus, the EC3 concludes cooperation agreements with key actors that can contribute to the EU Member States response to cybercrime. The EC3 has provided itself with the task of a diplomatic role ensuring that common principles and norms are created through the deployment of a shared, cross-community approach when engaging in partnerships with Member States, private parties and third countries.

As mentioned, the EC3 has been set up under the umbrella of Europol. Thus, the legal basis for the conclusion of agreements is to be found in the current 2009 Europol Council Decision (ECD), which authorizes Europol "to be able to conclude agreements and working arrangements with Union or Community institutions, bodies, offices and agencies in order to increase mutual effectiveness in combating serious forms of crime which come within the respective competence of both parties and to avoid the duplication of work".[30]

As stated in Article 23(1) on "Relations with third States and organizations", Europol may establish and maintain cooperative relations with:

(a) third States;

(b) organisations such as:

(i) international organisations and their subordinate bodies governed by public law;

(ii) other bodies governed by public law which are set up by, or on the basis of, an agreement between two or more States; and

(iii) the International Criminal Police Organisations (Interpol).

According to Article 23(2), such agreements may concern the exchange of operational, strategic or technical information including personal data and classified information.

EUROPOL'S DATA PROTECTION FRAMEWORK AS AN ASSET IN THE FIGHT AGAINST CYBERCRIME

Full compliance with data protection principles is an asset in effectively preventing and combating cybercrime. It forms the basis for the trust of Member States which provide related intelligence to Europol. In setting up the EC3, one of the key challenges is to preserve and increase security whilst paying due respect to privacy protection and other fundamental rights. There is little doubt that EC3's operations require vast processing of data which often involves risks for citizens' privacy. Also, citizens expect the EC3 to tackle the issue of cybercrime in a way which fully respects fundamental rights including the right to protection of personal data.

28 Outreach and cooperation. Available at: https://www.europol.europa.eu/ec3/outreach-and-cooperation (accessed on 20/12/2015).

29 Communication from the Commission to the Council and the European Parliament – Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM(2012)140 final, 28 March 2012, p. 7).

30 Art. 22 of the Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), OJ L121/37-66, 15.5.2009. See more: С. Никодиновска-Стефановска, Европол – нова структура и мандат, Годишник на Факултетот за безбедност – Скопје, 2007/2008; S. Nikodinovska-Stefanovska, Europol Council Decision, Kriminalističko-policijska akademija, Beograd, 2011.

Europol has a comprehensive, robust and tested regime in place, which is widely recognised as safeguarding and ensuring the highest standards of data protection in the law enforcement world. It aims at ensuring the protection of privacy of the persons whose data are processed in Europol's systems.

Europol's data protection legal framework is based on the principles contained in Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as on the Council of Europe Committee of Ministers Recommendation No. R(87) 15 regulating the use of personal data in the police sector.[31]

The Europol Council Decision contains very detailed provisions on data protection, which are further developed by a set of implementing rules such as Council Acts related to the Rules applicable to Analysis Work Files[32], Rules governing Europol's relations with partners[33], Rules on Confidentiality[34] and Conditions related to the processing of data for the purpose of determining relevance to Europol's tasks.[35] Additionally, Europol observes the principles of Regulation 45/2001[36] when it comes to the processing of staff data[37]. The application of data protection rules by Europol is supervised on various levels and throughout the entire information cycle.[38]

As of its launch in 2013, the boundaries of EC3 operations are determined by the ECD and its implementing rules. Potential operational business needs beyond the current mandate would have to be reflected in the process of the ongoing evaluation of the ECD. A future Europol Regulation is to be adopted by the European Parliament and the Council as required by Article 88 of the Treaty on the Functioning of the European Union.

THE PROPOSAL FOR A NEW REGULATION ON EUROPOL

The legal framework for Europol is about to be changed in accordance with the Treaty of Lisbon – which provides for a new legal basis for Europol. On 27 March 2013, the Commission published a proposal for a "Regulation on the European Police Office" (Europol). Article 88 and Article 87(2)(b) of the Treaty on the Functioning of the European Union are the legal bases for the proposal. The new regulation will eventually replace the current Europol decision. In the proposal for a Europol regulation, the establishment of a European Cyber Crime Centre is provided for in Article 4(1) as part of Europol's tasks which include the ambition:

(l) to develop Union centres of specialised expertise for combating certain types of crime falling under Europol's objectives, in particular the European Cybercrime Centre.[39]

31 See Art. 27 of the Europol Council Decision.
32 Council Decision of 30 November 2009 adopting the implementing rules for Europol analysis work files (2009/936/JHA), OJ L 325/14, 11/12/2009.
33 Council Decision of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information (2009/934/JHA) OJ L 325/6, 11/12/2009.
34 Council Decision of 30 November 2009 adopting the rules on the confidentiality of Europol information, (2009/968/JHA), OJ L 332/17, 17/12/2009.
35 Decision of the Management Board of Europol of 4 June 2009 on the conditions related to the processing of data on the basis of Article 10(4) of the Europol Decision, OJ L 348/1, 29/12/2009.
36 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of data.
37 Art. 39(6) of the Europol Council Decision.
38 Council Decision of 6 April 2009 …*op.cit.*, Art. 27–35.
39 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Council Decisions 2009/371/JHA, 2009/934/JHA 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

In addition, the new Europol regulation is to provide for the following:

1. to establish Europol as a hub for information exchange between law enforcement authorities in the Member States;

2. to set up a robust data protection regime.

What triggered the need for a Europol regulation was not least to impose the EU Member States the obligation to supply Europol with information. As stated in the Commission staff's working document accompanying the proposed regulation on Europol, the EU Member States do not provide Europol with all the necessary information to fight serious cross-border crime. As a result, Europol cannot be fully effective. In other words, Europol is what the states make of it.

CONCLUSION

New technologies have become an important part of the everyday lives of EU citizens, companies, organisations and authorities. But with EU citizens' growing dependence on these technologies also comes growing opportunities for criminals. As modern economies have embraced information and communication technologies, they have become vulnerable to cyber-attacks. Such attacks are mounted by a wide variety of actors, some state-affiliated or enjoying state support. The methods and tools used are however largely the same.

Cyberspace is an open environment, which poses a serious challenge to policy-makers. Its governance is shared by governments, the private sector and civil society. Cyber security efforts thus require the involvement of various stakeholders, in particular since the private sector owns the vast majority of hardware, software and information infrastructure.

Despite limits to its competence, the EU has sought to become a platform for common cyber security efforts by the Member States. It has tackled network security issues and set up procedures for the protection of critical infrastructure in Europe. Moreover, the EU has established minimum rules concerning criminal offences and facilitated law enforcement cooperation through Europol, including with the newly established European Cybercrime Centre.

The Centre marks a significant step forward in the EU's endeavour to fight cybercrime and increase cyber security, building on human rights and fundamental freedoms. The EC3 strives to be the European focal point in the fight against cybercrime, equipped with state-of-the-art technology and a strong team of highly qualified personnel. The Centre fulfils its mission by helping Member States to dismantle and disrupt more cybercrime networks. It develops detection and forensic tools for cybercrime investigators. It provides specialised threat assessments, as well as offers more focused training for law enforcement, judges and prosecutors. The Centre cannot initially focus on all sorts of cybercrime. Fraud, intrusion and Internet-related abuse of children are therefore amongst the crimes that are targeted in the initial phase. The key to success of the EC3 is cooperation, and not only within the Law Enforcement Community. The EC3 should work closely with a broad range of partners, from other EU Agencies, as well as computer emergency response teams, to private sector and the research community.

By inaugurating the EC3, EU sends a signal to the cybercriminals that 28 Member States together with the EU institutions, as well as industry, academia and civil society will come after them. Never before has the EU responded in such a strong way.

---

and 2005/681/JHA, p. 23. Available at: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/europol-cepol/docs/law_enforcement_training_scheme_proposal_en.pdf (accessed on 22/12/2015).

REFERENCES

1. An Open, Safe and Secure Cyberspace Brussels, 7.2.2013 JOIN(2013) 1 final
2. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cybercrime (COM (2007)267 final).
3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe (COM (2010)245, 19 May 2010).
4. Communication from the Commission to the European Parliament and the Council – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM (2010)673, p. 9).
5. Communication from the Commission to the Council and the European Parliament – Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM (2012) 140 final, 28.3.2012).
6. Combating Cybercrime in a Digital Age, https://www.europol.europa.eu/ec3.
7. Communication from the Commission to the Council and the European Parliament – Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM (2012)140 final, 28 March 2012.
8. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (OJ C 83, 30 March 2010).
9. Council of Europe Convention on Cybercrime, Budapest 21.XI.2001 (ETS 185).
10. Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography (OJ L 13 of 20 January 2004).
11. Council Framework Decision 2005/222/JHA on attacks against information systems (OJ L 69 of 16 March 2005).
12. Council Decision of 30 November 2009 adopting the implementing rules for Europol analysis work files (2009/936/JHA), OJ L 325/14, 11/12/2009.
13. Council Decision of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information (2009/934/JHA) OJ L 325/6, 11/12/2009.
14. Council Decision of 30 November 2009 adopting the rules on the confidentiality of Europol information, (2009/968/JHA), OJ L 332/17, 17/12/2009.
15. Cybersecurity Strategy of the European Union.
16. Decision of the Management Board of Europol of 4 June 2009 on the conditions related to the processing of data on the basis of Article 10(4) of the Europol Decision, OJ L 348/1, 29/12/2009.
17. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218/8, 14.8.2013.
18. Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335/1 of 17 December 2011).
19. European Cybercrime Centre (EC3), http://ec.europa.eu/dgs/home-affairs/e-library/docs/infographics/cyber-crime/european_cybercrime_centre_infographics.pdf.

20. EC3 first year report, https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report.
21. European Parliament, Directorate-General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Study 2012, Fighting cybercrime and protecting privacy in the cloud.
22. European Council 10–11 December 2009 – Conclusions, Brussels, 11 December 2009 (EUCO 6/09).
23. European Commission MEMO Questions and Answers: Directive on attacks against information systems, Strasbourg, 4 July 2013, http://europa.eu/rapid/press-release_MEMO-13-661_en.htm.
24. Outreach and cooperation, https://www.europol.europa.eu/ec3/outreach-and-cooperation.
25. Nikodinovska-Stefanovska, S., Europol Council Decision, Kriminalističko-policijska akademija, Beograd, 2011.
26. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM (2013) 48 final, 2013/0027 (COD), http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/docs/1_directive_20130207_en.pdf.
27. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA 2009/935/JHA, 2009/936/JHA and 2009/968/JHA and 2005/681/JHA.
28. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of data.
29. The Stockholm Programme – An open and secure Europe serving and protecting the citizens. Presidency Conclusions – Brussels, 10–11 December 2009 (Council of the European Union, Brussels, 3 March 2010, doc 5731/10).
30. Никодиновска-Стефановска С., Европол – нова структура и мандат, Годишник на Факултетот за безбедност – Скопје, 2007/2008.

UDC: 530.145:004.056.55

PHYSICAL FUNDAMENTALS OF QUANTUM CRYPTOGRAPHY

Stevo Jaćimovski, PhD[1]
Academy of Criminalistic and Police Studies, Belgrade
Jovan Šetrajčić, PhD
University of Novi Sad, Faculty of Sciences

Abstract: The end of the 20th and the beginning of the 21st century can be called the time of Information Technology (IT). IT industry that deals with creating, processing, storing and transmission of information has become an integral part of global economic system. It represents totally independent and rather important part of economy. Addiction of the modern society to information technology is so high that problems which occur in information systems lead to significant incidents. Information exchange is the most delicate area of IT technology and the most susceptible to abuses. Hence, the information protection during the information exchange is of significant importance. Cryptology as a science and particularly its part cryptography, deals precisely with this issue. Significance of cryptographic methods is in its being based on conversion of the information itself and they are not connected to material characteristics of the transmitter, which makes them the most universal and the cheapest for implementation. Quantum cryptography is relatively new area which engages in providing secure communication between the sender and the recipient of the information, using quantum-mechanical approach. The aim of this work is to get us acquainted with the principles of quantum distribution of key to information encryption and with basic problems which occur during its realisation.

Keywords: cryptography, algorithms, encryption, key, quantum mechanics, protocols.

INTRODUCTION

Cryptography can be defined in different ways, and one of them is: Cryptography is a science about secret writing (writing down), which deals with methods of preserving confidentiality of the information. Historically observed, cryptography arose from the need for transferring and delivering secret information. Along with crypto-analysis (science about the decryption of secret information) it is an integral part of the science which is called cryptology. Cryptology is nowadays a part of mathematics which has a great application in information technologies. Cryptography was for a long time associated with the elaboration of special methods of transformation of information in order to be incomprehensible to the potential adversary. With the occurrence of computer technology and its possibilities of data processing, the task of cryptography has radically changed. There are also opinions that it was cryptography and the need for decryption that stimulated the development of information technology.

According to Anglo-Saxon tradition, participants in encoding and decoding information are called Alice and Bob. The adversary, who would without authorization like to find out

1 E-mail: stevo.jacimovski@kpa.edu.rs.

information which Alice and Bob exchange is called Eve, short for *eavesdropper*. The adversary, presumably, has unlimited computational resources and fully understands the use of cryptographic methods, algorithms, protocols, etc.[2]

Classical task of cryptography is to convert the initial text (plaintext) into arbitrary string of characters which is called cryptogram. The number of characters in the plaintext and in the cryptogram can differ. The secrecy of encryption algorithms themselves cannot provide unconditional security of cryptograms, because it is assumed that Eve (the adversary) has infinitely large computational resources. Therefore, open algorithms are used nowadays. The security of contemporary cryptosystems are not based on the secrecy of algorithms, but on secrecy of a small-size information which is called the key.

The key is used to manage the encoding process and should be easy to change at any point of time. At the end of the 20th century a Dutch scientist Kerkhof[3] formulated the rule by which security of the code is provided if the adversary is aware of the entire encoding system, except the secret key, that is, except the information which manages the process of cryptographic transformation.

Claude Shannon observed encoding as copying the initial information into cryptogram

$$C = F_i(M) \tag{1}$$

where C is cryptogram, F_i - copying (function), M - initial text (message), message, *i*-index corresponding to a particularly used key. For unambiguous decoding, copying F_i must have unique inverse copying, so that it is

$$F_i \cdot F_i^{-1} = I \tag{2}$$

where *I* is –identical copying.

Whereas it follows that

$$M = F_i^{-1}(C) \tag{3}$$

It is considered that the source of the keys is a statistical process or a device which sets the copyings $F_1, F_2, ..F_{N1}$ with known probabilities $p_1, p_2, ..p_{N1}$. The number of possible information N_2 is final, and information $M_1, M_2, ..M_{N2}$ have a priori probabilities $q_1, q_2, ..q_{N2}$

The examples of physical devices which can be the source of the keys:[4]

- Coin tossing;
- Measuring time between radioactive decays;
- Time summation of Zener diode noise;
- Digitalized noise from PC audio card or of temperature sensors;
- Coincidence extracted from keystrokes on the keyboard;
- Coincidence extracted from the hard drive access times, etc.

2 Dugic (2009)
3 Килин (2009)
4 Stipčević(2003)

VERNAM CODE

If one wants to use perfectly safe cryptographic system, then Vernam code, i.e., so-called one-time pad is used. The original message is matched with a group of key characters and a group of cryptogram characters. Encoding is performed by changing the characters of the original message with cryptogram characters, depending on the ordinal character of the symbol in the key. The symbols of the key consist of random string of numbers from 0 to 37. Then the message, key and the cryptogram are represented in the shape of string of letters of the same alphabet.

$$M=(m_1,m_2,m_3,...m_n),\quad K=(k_1,k_2,k_3,...k_n),\quad C=(c_1,c_2,c_3,...c_n),\quad (N_1=N_2) \tag{4}$$

The current encoding step is given as

$$c_i=f(m_i,k_i) \tag{5}$$

Table 1: *Joining the letters of the alphabet to corresponding numbers from 00 to 36*

A	B	C	Č	Ć	...	...	...	V	Z	Ž		.	,	!	?	;
00	01	02	03	04				28	29	30	31	32	33	34	35	36

Table 2: *The example of the encoding the information KOD VERNAMA*

K	O	D		V	E	R	N	A	M	A
15	21	06	31	28	09	23	19	01	18	01
15	04	13	28	11	09	36	30	02	24	05
30	25	19	22	02	18	22	12	03	05	06

The second line in Table 2 consist S of randomly selected numbers, and the third line is the summation of the first and the second line according to the module 37.

In that way, encoding and decoding can be expressed as

$$\begin{aligned} M+k(\mathrm{mod}\,37)&=C\\ C-k(\mathrm{mod}\,37)&=M \end{aligned} \tag{6}$$

This way of encryption was invented by Gilbert Vernam.

Claude Shannon mathematically proved that one-time information is absolutely secure, if the key is really random, if it is of the same length as the message and if it is not used twice. Codes of this type are unconditionally secure.[5]

Notwithstanding the provision of unconditional security, these systems have limited application in practice. In many cases the key is long, and therefore unsuitable for sending over a secure channel.

Another disadvantage of the Vernam Code is the fact that the key can be used only once. If the key is reused Eve can decode the fragments of the message, and decode the key as well, by comparing the parts of the cryptogram.

Due to physical reasons, classic conditions of physical objects can be measured with the random precision and without perturbations of the system condition. Therefore, within the framework of classical physical ideas it is impossible to ensure the distribution of the secret

5 Shenon (1949)

key through an open channel of communication, because it is impossible to detect attempts to passive eavesdropping. Therefore, cryptograms with one-time key are not widely implemented.

Over time, the idea that encoding algorithm should not be secret has been accepted, because it can be compromised very easily, but that the security should be sought in the secrecy of the key. However, there is still one problem left - the exchange of secret keys between the person who wants to send that information (Alice) and the person who wants to receive it (Bob). Namely, there was a vicious circle, since those individuals had to exchange secret keys in a secure way, above all. In order for people who are already in communication to establish the secure communication, primarily, they had to establish the secure communication.

Diffie –Hellman's protocol

W. Diffie and M. Hellman (Stanford) published in 1976 a method for establishing the secret key between two parties which share previous secret. If Alice and Bob wish to establish the secret key it is enough to follow this protocol:[6]

- Alice generates **random number** A and calculates $P = e^A$ and sends *P* to Bob;
- Bob generates **random number** B and calculates $Q = e^B$ and sends Q to Alice.

Then Alice and Bob calculate the secret key K, as it is shown in Figure 1.

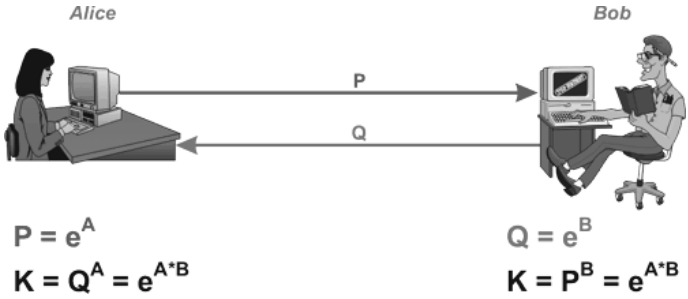


Figure 1: *DH protocol*

Let us assume that Eve possesses P and Q. Can she calculate K? In order to calculate K, Eve must calculate A or B, because even then she can repeat the calculation of the key in the same way as Alice or Bob. The idea is that calculation of A or B requires calculation of the discrete algorithm:

$$A = \ln P, \quad B = \ln Q, \tag{7}$$

and there is no efficient way for that.[7]

The existing cryptographic protocols with one-time key provide good protection, under condition of solving the problem of key distribution. However, these systems have two basic problems:

1) How to implement the key distribution through the secure channel;

2) How to accomplish secret key authentication (the so-called problem of the first contact).

Authentication implies a procedure which enables the recipient to verify that the secret key belongs to a legitimate sender. In order to understand what this is about, imagine that Eva intercepts all messages sent by Alice, introducing herself as Alice to Bob, and introducing as

6 Jakuš(2004)
7 Stipčević(2003)

Bob to Alice. It turns out that if Alice and Bob already have the secret key (which they have exchanged, for example, at the meeting), authentication of additional keys is not a problem. However, if the secret key is not exchanged, theoretically identity check is not possible, although there are some traditional methods to optimize it.

Exchange of classic information

In classical information exchange, two algorithms - symmetrical and asymmetrical are in use today. Symmetrical are based on the use of the same secret key (or keys) for encryption and decryption. Asymmetrical are based on the use of different keys for encryption and decryption, one of which is public and known to all, and the other is secret and is known only to one of the participants in the communication.[8]

Symmetric cryptography - In symmetric cryptography procedure for encoding and decoding is based on two mathematically related functions. Encoding function F (encryption) on the basis of key k and incoming message M, creates the protected message C. Decoding function (decryption) F^{-1} on the basis of the same key k and protected message C, creates the original, incoming message M. Symmetrical cryptographic algorithms provide high level of security until the key is known only to the sender and the recipient of the message. Hence, the basic security measure of symmetric algorithms is the method for keys distribution.

The best known and most widely used symmetric algorithm is DES and its upgraded version 3DES.

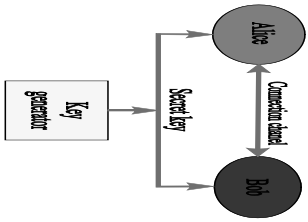


Figure 2: *Asymmetric cryptosystem generates a general secret key and distributes it to legitimate users. With the help of the same key encoding and decoding is performed.*

Asymmetric cryptography - The process of encoding and decoding in the asymmetric cryptography is also based on two related mathematical functions: encryption function F and decryption function F^{-1} manipulate the original and protected message M and C using two related but different keys, one of which is used for encryption (key f), and the other for decryption (f^{-1} key). The first one is called public (open) key, and the other key is private or secret. The public key is known to all, while private one is known only to one party. In the first case, the sender of the message (Alice) wishing to establish private communication with the recipient (Bob), uses the recipient's public key to encrypt the original message. Since the appropriate private key is the recipient's property, only he can decrypt the protected message. In that way the secrecy of communication between the sender and the recipient is established. However, the recipient is not certain who has sent him the message, because his public key is generally known - authentication request has not been satisfied. This problem was solved by introducing the digital signature.

In the second case, the sender cannot be anyone. In order to perform the protected information exchange, the sender must be identified to the recipient of the message. The sender uses his private key to protect the message, and anyone who knows the sender's public key can decrypt the message. In this case, the identity of the message sender is accomplished, as well as

8 Čisar(2015)

impossibility of his denial that he was the one who has sent the message, but the secrecy of the communication has not been accomplished, because anyone who knows the public key of the sender can decrypt the message.

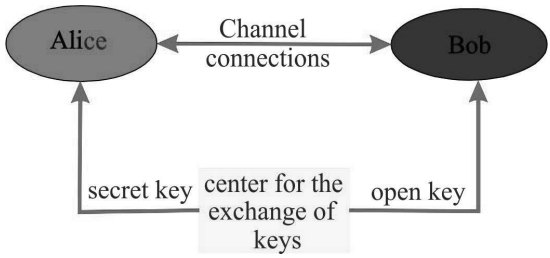


Figure 3: *Asymmetric cryptosystems operate with two keys. The first one is public, available to every user and with its help the encoding is performed. The other key is secret and should be available only to the recipient of the message.*

The best known algorithm in a group of asymmetric cryptographic methods is RSA.

Computer security is based on the amount of CPU time required for system "to break down" using the best-known computational methods.[9] We say that the system is safe, if it cannot be broken in due time by the most powerful computer resources available. It is believed that the most widely used cryptosystems with the public key (RSA, DH) as well as some with the secret key (DES, IDEA, RC5) belong to this category. Their safety is based on problems with factorizing of large numbers and calculating discrete algorithms in certain final groups. These problems are believed to be "difficult" in the sense that there is no better way for them to be solved, but to guess all possible solutions (keys), i.e. the number of steps grows exponentially along with the length of the key.

Secrecy in the contemporary world is based on the conception that something is computationally secure, i.e. that it is safe in the sense that for the breaking the code too much computing time and power would be needed.[10] For large numbers finding their factor is a difficult problem. Imagine number 100. Which are its factors? Two times 50 is 100. But that is also for 4 times 25, or 5 times 20, or 10 times 10. The number of factors is growing rapidly and finding all of them represents a great difficulty for every contemporary classic computer. An American physicist Richard Feynman was the first who realized that laws of classic physics lead to totally different limitations in information processing in relation to computing based on quantum mechanics. It turns out that quantum computer can efficiently factorize large numbers, and therefore the protection of classic cryptography ceases. The explanation for that was provided by Peter Shor,[11] who provided the algorithm by which quantum computer, since it uses quantum principle of superposition, can exist simultaneously in lots of different conditions. Imagine a single computer in superposition so that it is simultaneously in lots of different places. In each of those locations you can configure computer so that it divides your number with another number to search for factors. And that is huge, unbelievable acceleration of solving the problem with factoring, because one computer now simultaneously performs all those divisions, one by one in each spatial location. Precisely because of this the idea occurred that information protection should be searched for in, colloquially speaking, "hardware", i.e. to use the laws of quantum mechanics for the protection.

9 Čisar(2015)
10 Vedral(2014)
11 Shor(1994)

The solution was found in quantum cryptography, i.e. quantum key distribution, which enables the two parties (Alice and Bob) to communicate safely. Quantum cryptography uses natural vagueness of the quantum world. With its help, it is possible to establish the communication channel which is impossible to eavesdrop without the disturbance of the transmission, i.e. two users who communicate with each other can reveal the presence of the third party which is trying to find out the key.

Likewise, a person who eavesdrops cannot copy an unknown quantum bits called qu-bits, i.e. unknown quantum state, due to the no-cloning theorems. Quantum cryptography is used only for obtaining and distributing the key and not to transmit messages. Thus, the generated key can be used in a cryptosystem to encrypt and decrypt messages.

PHYSICAL FUNDAMENTALS OF QUANTUM MECHANICS

Quantum mechanics, whose basic ideas were formulated by Nils Bohr, Erwin Schrödinger and Werner Heisenberg, excepting mathematical apparatus that enables calculating the energy states of atoms and molecules and calculating the matrix elements of their transition, implicitly contains certain philosophical assumptions, whose interpretations until recently have not been thoroughly analysed. It is this segment of quantum mechanics that completes all the micro-world oddity. Erwin Schrödinger in his famous work from 1935 analysed one of the problems of quantum information: what can we learn about the world of quantum states of objects and what happens to objects in the process of knowledge.[12]

In his work, Schrödinger analyses "underwater rocks" to describe the quantum mechanical measurement process and he formulated the four assumptions that are confined to the fact that state of the quantum world objects has the following properties:[13]

1. Superposition - arbitrary state described by a linear superposition of the base state;

2. Interference - the measurement result depends on the relative phases of the amplitude in the superposition;

3. Hidden states - full knowledge of the state of the whole system does not mean that we have full knowledge of the conditions of parts of the system;

4. Uncertainty and impossibility of cloning - the unknown quantum state is not possible to be cloned, and also cannot be seen without being perturbed.

The system state and wave function

In quantum theory, the notion of a particle as part of a body with certain dimensions and mass is so wrong that it is not possible even principally to understand in which point of space it is.[14]

It arises from Heisenberg's uncertainty principle

$$\Delta x \cdot \Delta p_x \geq \hbar / 2; \quad \Delta E \cdot \Delta t \geq \hbar / 2 \tag{8}$$

where Δx is uncertainty of particle position, Δp_x - uncertainty of particle impulse, ΔE - uncertainty of particle energy, Δt - uncertainty of time, $\hbar$ -Dirac constant $\hbar = 1.054 \cdot 10^{-34}\ Js$.

12 Schrodinger(1935)
13 Килин(1999)
14 Hajzenberg(1974)

Although it is not possible to determine with sufficient precision the position and impulse of particles, it is possible to predict the behaviour of particles. The difficulty is in the fact that in order to explain the behaviour we have to completely give up the attempts to calculate all "traditional" physical properties of the system. It leads to the fact that the state of every elementary particle (or system of particles) must be shown with the help of so-called wave function - principally new object in our notion about the quantum world.[15] The wave function is marked by ψ and represents a time function and coordinates in the field of complex numbers.

Let us introduce the concept of a pure quantum state. Such situation is called a vector in Hilbert space **H** with unit norm. The norm means square root of scalar product.

$$\|\psi\| = \sqrt{(\psi,\psi)}, \quad \psi \in \dot{\mathrm{H}} \tag{9}$$

For physics, finite-dimensional Hilbert spaces are the most significant, their most important characteristic is the existence of scalar product. For the vector ψ the characteristics of the unitary norm corresponds to the fact that $\psi^* \psi$ =1. Each wave function corresponds to the vector ψ , whose i[th] coordinate ψ_i is equal to the probability amplitude for noticing the particle in i[th] point of space. In this way, it becomes clear that it is very important to find a space that suits the established conditions. The condition of norming the state indicates that the total probability of finding a particle is equal one. In quantum theory of information for states and operators Dirac notation is used. For state ψ mark $|\psi\rangle$ is used, called ket-vector, and for complex conjugate state ψ^* mark $\langle\psi|$ is used, called bra-vector. Scalar product of vectors φ and ψ is written as $\langle\varphi|\psi\rangle$.

For each pure quantum state $|\psi\rangle$ appropriate operator $\rho_\psi = |\psi\rangle\langle\psi|$ can be defined, which is called density operator. That operator, observed as matrix, has a rank of 1 and his spur (sum of the diagonal elements of matrix) is equal one(1) and it operates as a projector on pure state $|\psi\rangle$. With the help of density operator, the general term of quantum state is introduced. Statistical mixture of several pure states, i.e. a group of pure states with proper probabilities is called mixed quantum state:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad p_i \geq 0 \ \forall i, \sum_i p \ = 1 \tag{10}$$

Each Hermitian operator $\hat{A}$ has a spectrum development (Hermitian operator is the one whose eigenvalues are real numbers)

$$\hat{A} = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i| \tag{11}$$

where eigenvalues λ_i are real, and eigenvectors $|\lambda_i\rangle$ normed and orthogonal. Now we can define the quantum state as a positive Hermitian operator in Hilbert space **H** with spur value 1.

One of the key laws of quantum mechanics is Schrödinger equation which describes how the quantum states change with time.

$$i\hbar \frac{d|\psi\rangle}{dt} = \hat{H}|\psi\rangle \tag{12}$$

Hermitian operator $\hat{H}$ is called Hamiltonian system and it affects the evolution system.

The connection between Hermitian and unitary operators is as follows:

$$\hat{U} = e^{i\hat{H}}, \tag{13}$$

so, the Schrödinger equation can be written as

15 Bohr(1985)

$$\left|\psi'\right\rangle = \hat{U}\left|\psi\right\rangle \tag{14}$$

It is this form of Schrödinger equation which is suitable for calculating, since the arbitrary evolution of quantum system can be displayed as an effect of a unitary transformation. It should be said that unitary operators are the ones which meet the following requirement:

$$UU^{\dagger} = U^{*}U = 1, \tag{15}$$

where $U^{\dagger}$ is adjoint operator.

The simplest nontrivial quantum object is a system with two base conditions. Such a system is, for example, photon with the proper direction of polarization (vertical $\left|\updownarrow\right\rangle$ and horizontal $\left|\leftrightarrow\right\rangle$) or the direction of the spin electron (up $\left|\uparrow\right\rangle$ or down $\left|\downarrow\right\rangle$). In that case Hilbert space is two-dimensional $\mathbf{H}^2$. Usually, if the specific physical nature of two-level system is not important, its states are marked with $\left|0\right\rangle$ and $\left|1\right\rangle$ .That system is called qubit or quantum bit. Arbitrary pure qubit state can be written as:[16]

$$\left|\psi\right\rangle = \cos\alpha\left|0\right\rangle + i\sin\alpha\left|1\right\rangle \tag{16}$$

The rank of density operator is 1 (for pure state $\left|\psi\right\rangle\left\langle\psi\right|$) or 2 for mixed state which can in case of $\mathbf{H}^2$ always be written as statistical mixture of two orthogonal pure states

$$\rho = p\left|\psi\right\rangle\left\langle\psi\right| + (1-p)\left|\psi^{\perp}\right\rangle\left\langle\psi^{\perp}\right| \tag{17}$$

Measuring

The procedure of measuring the quantum states differs the quantum case from the classical one and enables the application of quantum cryptography**.** Important difference between quantum and classical mechanics is the fact that the act of measuring the quantum system changes its initial state, which is not the case with classical mechanics.[17]

The significant lawfulness of quantum mechanics which occurs during the intervention of measuring is reduction or collapse of wave function. It marks the transition of the quantum states after measurement into one of the Eigen states measurement operator. This characteristics is one of the most important for quantum cryptography. This is because an attempt of measuring the system leads to disorder, from which it follows that the attempt to gain unauthorized download of the information can always be detected by additional errors on the receiver side. The impossibility of distinguishing non-orthogonal quantum states is an important result which is the basis of quantum cryptography protocol secrecy.

Decoherence of the quantum system

In quantum mechanics, quantum decoherence represents a phenomenon of loss of coherence or ordering of phase angles among the components of (quantum) system which is in quantum superposition. Decoherence is manifested identically as wave function collapse during the process of measuring the system state, but it does not generate wave function collapse. Decoherence only gives the explanation of observation of the wave function collapse, when quantum nature of the system "leaks" into the environment. Actually, the components of wave function separate from coherent system and acquire phases from their immediate environment.

Decoherence occurs in the interaction of the system with the environment in thermodynamically irreversible manner. On this occasion, each information present in quantum system is lost in the environment. It is considered that it is a process by which information in quantum system is lost in the interaction with the environment in the way that quantum correlation of the system occurs in an unknown way, so that the system itself cannot be described without data on the state of its surroundings.[18]

16 Dugić(2009)
17 Hajzenberg(1974)
18 Ijačić(2014)

Hidden and not hidden observables

Analysis of quantum systems composed of several particles (system components) can (lead to) cause interesting properties which are not met in classic cases. Even Einstein, Podolsky and Rosen (EPR) in 1935[19] noticed unusual properties of quantum system components which contradicted the locality. From their analysis arises the fact that the effect on one quantum subsystem currently affects the other subsystem regardless of their distance. Measurement of one part of quantum state can fix the entire state as a whole. This holds true for the so-called entangled states. These are states that cannot be displayed in the form of tensor product. For states that are separable, measurement of one subsystem does not affect the state of other subsystem.

Quantum entanglement is quantum mechanical phenomenon in which quantum state of two or more objects must be described in correlation with each other, even if the objects are separated in space. As a result of that, correlation among the observed physical characteristics of objects occurs.[20] For example, it is possible to create particles in the same quantum state, so that when one particle state is noticed with spin directed upwards, the spin of other particle is directed downwards, and vice versa, despite the fact that, according to quantum mechanics, it is not possible to predict what direction of particles it would be in any case. In other words, it appears that the measurements which are performed on one system, currently affect the other system that is entangled with it.[21] However, what is meant by the information in the classic sense, still cannot be transmitted through the entanglement faster than the speed of light. Quantum entanglement is basis for technologies such as quantum computers and quantum cryptography, and, it is also used in the experiments related to quantum teleportation. This phenomenon is one of the most revolutionary characteristics of quantum theory, since the correlations which quantum mechanics predicts are incompatible with the concept, one would say, obvious locality of the real world, according to which the information about the system state can be transmitted only through the closest environment. Different views on what happens during the process of quantum-mechanics entanglement has led to different interpretations of quantum mechanics.[22]

Mathematically speaking, entanglement represents multi particulate quantum state which cannot be factorized (i.e., state which cannot be decomposed into products with several states).The simple mathematical analogy is as follows: a^2-b^2 it can be displayed as product of $(a + b)$ and $(a-b)$, while $a^2 + b^2$ cannot be factorized.

There is a way that apparently enables the successful explanation of quantum entanglement, and that is the theory of hidden parameters by which for correlations of certain but unknown microscopic parameters are responsible. However, J. S. Bell, in 1964, showed that local theory cannot be built in that way, i.e. entanglement which is predicted by quantum mechanics, we can experimentally differ from the results predicted by the theory with local hidden parameters. Additional experiments provided astounding confirmations of the regularity of quantum mechanics predictions. Entanglement leads to interesting interaction with the principle of relativity, which says that information cannot be transmitted from one place to another faster than the speed of light. Although the two systems separated by large distances can be entangled, useful information cannot be transmitted through their connection. Therefore, the principle of causality is not violated due to entanglement. That happens because of two reasons:

1. The results of measurements in quantum mechanics are fundamentally of probable character;

19 Einstein(1935)
20 Dugić(2009)
21 Marić(1986)
22 Marić(1986)

2. Theorem on the impossibility of cloning the quantum state (no-cloning theorem of quantum state) disables statistical verification of entangled states.

QUANTUM CRYPTOGRAPHY

For absolute secrecy during the exchange of information it is necessary to fulfil three conditions:[23]

- Message should be encoded with the key which is arbitrary string of characters, such as zeros and ones;
- The length of the key must not be shorter than the length of the message;
- The key is used only once.

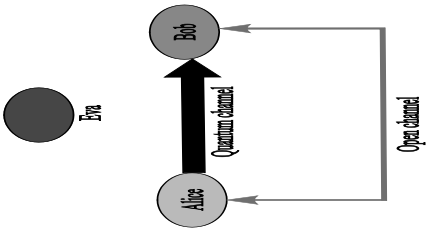


Figure 4: *Schematic representation of quantum cryptography*

Distribution of keys through the quantum state enables, in principle, ensuring their secrecy, and meets the above conditions in the exchange of confidential information. The basis for this claim is a theorem about the impossibility of copying arbitrary quantum state (no-cloning theorem), which claims that an unknown quantum state cannot be copied. Under copying, we imply the procedure during which each entry state corresponds to two identical exit states. Unitarity of evolution of quantum-mechanical systems makes this procedure possible only if copied states are deformed. Deformation of states leads to the occurrence of statistical errors which appear in the certain stage of conducting quantum-cryptographic protocol. Analysis of these errors enables the legitimate key exchange participants to verify unauthorized aces to the connection channel.

Encoding the information in quantum states was first suggested by Viesner,[24] as well as Bennett and Brassard.[25] Their idea was that passive eavesdropper Eve is not able to differ non orthogonal quantum states, (let us call them $|\psi\rangle, |\varphi\rangle$) if she does not know basis in which they are created (by state definition which are described by ket vectors $|\psi\rangle, |\varphi\rangle$ are orthogonal, if their scalar product is equal zero, $\langle\psi|\varphi\rangle = 0$).

Let us assume that Eve's measuring instrument is in state $|m\rangle$. Her aim is to differ states $|\psi\rangle, |\varphi\rangle$, whereas she must not disrupt them. Her operation can be described by the following unitary transformations over the initial state

$$|\psi\rangle|m\rangle \to |\psi\rangle|m_0\rangle \; |\varphi\rangle|m\rangle \to |\varphi\rangle|m_1\rangle \tag{18}$$

Unitary transformation preserves the scalar product, so we have

$$\langle\psi|\varphi\rangle\langle m|m\rangle = \langle\psi|\varphi\rangle\langle m_0|m_1\rangle \tag{19}$$

23 Килин(2007)
24 Wiesner(1983)
25 Bennett(1984)

where norming condition is

$$\langle\psi|\varphi\rangle\langle m_0|m_1\rangle = 1 \tag{20}$$

The last expression indicates the fact that finite state of Eve's measuring instrument is the same. Eve did not perturb quantum state, but she did not acquire any kind of information about them either.

Let us analyse more general case of measurement, when Eve during the measurement causes disorder of the initial state

$$|\psi\rangle \to |\psi'\rangle, |\varphi\rangle \to |\varphi'\rangle \tag{21}$$

As a result, we have

$$|\psi\rangle|m\rangle \to |\psi'\rangle|m_0\rangle \; |\varphi\rangle|m\rangle \to |\varphi'\rangle|m_1\rangle \tag{22}$$

Based on unitarity we get

$$\langle\psi|\varphi\rangle = \langle\psi'|\varphi'\rangle\langle m_0|m_1\rangle \tag{23}$$

The best situation for Eve is when scalar product $\langle m_0|m_1\rangle$ has minimum value. That will happen in case when it is

$$\langle\psi'|\varphi'\rangle = 1 \tag{24}$$

since $\langle\psi|\varphi\rangle = const \neq 0$. In this case she can differ two states of her instrument, however, two original non orthogonal states cannot be differentiated.[26] Thus we have arrived at the concept of attainable information of how well Bob can conclude which state Alice has sent to him.

In that way quantum cryptography enables relatively quick key exchange and registering of Eve's attempt to enter the connection channel. Let us emphasize that error occurrence during transmission and receiving quantum states does not necessarily lead to secrecy loss. For each protocol of quantum cryptography, critical error above which secrecy is not provided is defined. If the level of errors is (it is usually expressed in percent) below critical, then for creating the key protocols for error correction and later compression of remaining bits are used. After these procedures Eve has as little information about the key as Alice and Bob want.[27]

In quantum cryptography, nowadays, three forms of encoding quantum states are used: polarization state, phase state and time-shift encoding. In this study, procedure with polarization encoding of quantum states will be demonstrated, so called protocol BB84. There are other quantum cryptography protocols which are also used. We will present some protocols: B92, E91,[28] SARG04, protocol of 6 states. It is claimed that these protocols are equivalent to protocol BB84.[29]

Example of protocol BB84 without noise

Protocol BB84 is historically the first protocol of quantum key distribution, whose safety is based on principles of quantum mechanics whereas it is absolutely secure if there is no noise in quantum connection channel. The absence of noise in a given situation assumes that the quantum state of a particle is not changed along the quantum connection channel.

26 Bennett(1992)
27 Picek(2009)
28 Ekert(1994)
29 Голубчиков(2008)

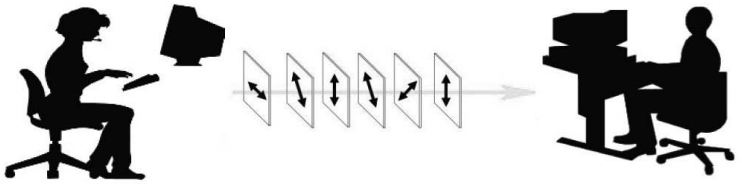


Figure 5: *Protocol BB84*[30]

Table 3: *Example of realization of the protocol BB84. States* $|\leftrightarrow\rangle$ $|\ \rangle$ *encode (0) zero, and states* $|\updownarrow\rangle$ $|\ \rangle$ *one (1). Rectangular and diagonal bases are marked with* $\oplus$ *and* $\otimes$ [31]

Stage 1	Random bits (Alice)	0	1	1	0	1	1	0	0
Stage 2	Random basis	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Stage 3	Polarization of photons which are distributed through quantum channel	⤢	⤡	⤡	↔	↔	⤡	⤢	↔
Stage 4	Random basis of reception (Bob)	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$
Stage 5	Bits which Bob received	0	0	1	1	1	0	0	0
Stage 6	Bob reports to Alice about meas. basis	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$
Stage 7	Alisa replies which are correct								
Stage 8	Sieved key			1		1			0
Stage 9	Bob reveals bits parts					1			
Stage 10	Alice confirms them								
Stage 11	Sieved key after error estimate			1					0

Protocol BB84 is formulated in language of single photons, although it can be applied on any other qubit realization. For information encoding four states of polarization are used, and they can form two mutually non orthogonal basis:

Rectangle $|\leftrightarrow\rangle$ and $|\updownarrow\rangle$ and diagonal

$$= (|\leftrightarrow\rangle + |\updownarrow\rangle)/\sqrt{2} \quad |\ \rangle\ |\ \rangle = (|\leftrightarrow\rangle + |\updownarrow\rangle)/\sqrt{2} \tag{25}$$

30 Ilievski(2009)
31 Килин(2007)

The essence of the BB84 protocol consists of the fact that one of the users (Alice) randomly selects a set of bits (stage 1) and a series of bases (stage 2), and then sends to user (Bob) a set of photons (stage 3), each of which encodes a bit of a selected string in the database which corresponds to the ordinal number of that bit wherein the states $|\leftrightarrow\rangle$ $|\nearrow\rangle$ encode (0) zero and the states $|\updownarrow\rangle$ $|\nwarrow\rangle$ encode one (1).

When obtaining a photon, Bob at random for each photon and independently of Alice, selects a base for measurement (rectangular or diagonal) (stage 4) and analogously for each photon interprets the results of his measurements in two ways as a zero or one (stage 5). According to the laws of quantum mechanics after the measurement of diagonal photons in a rectangular base, its polarization is converted into a horizontal or vertical, and vice versa, where the result is quite random. In this way, Bob obtains results that are consistent with the states of sent photons in about half of the cases (50%), i.e. when he correctly guesses the basis. The next stage of the protocol is realized by using the open channel connections, through which Alice and Bob can openly communicate classical information to each other. At this stage we assume that Eve can listen to both sides of the communications, but cannot change them or send notifications instead of them. To begin with Alice and Bob establish (by open channel) photons that are successfully received by Bob and decide which of them are measured in proper base (stages 6 and 7). After that Alice and Bob have the same bits value, encoded in these photons, regardless of the fact that this information has never been established in an open channel of communication (Stage 8). In other words, each of these photons carries one bit of random information that is known only to Alice and Bob and to no one else. Information about photons measured in the wrong base are rejected, causing Alice and Bob to obtain so called sieved key, which in the event that Eve has not intercepted information should be the same for both parties. Let us assume that Eve eavesdrops quantum channel. Because of the random selection in rectangular or diagonal bases Eve affects the information in a way that she alters sieved key bits, which should be the same for Alice and Bob, if it were not for Eve. No single measurement of photons by Eve, provides more than one half bit of information that is encoded by the photon; any such measurement provides *b* bits of information ($b < 1/2$) and is not in accordance with the probability (which is ultimately equal to *b/2*, if the measured photon or its replacement is measured in the initial base by Bob. In this way, Alice and Bob can check if someone eavesdrops openly comparing part bits (stage 9 and 10) that have the same information, although these bits, moreover, cannot be used for secret key. Bit position at the same time the comparison needs to be correctly measured random subset of bits, so that the presence of Eve must be observed. If during the comparison, all compared match, it is clear that there was no eavesdropping, and the remaining correctly measured bits can be used for the sector key of encoding (stage 11) and transmission of the data through the open channel. When that key is used, Alice and Bob repeat the procedure in order to create a new secret key.

Security of protocol BB84[32]

Protocol BB84 would be endangered if Eve could do the following interventions on the quantum channel:

1. Measure the photon polarization which Alice sends, reproduce the same one and send it to Bob;

2. Multiply photons which Alice sends.

In the first case Eve would have the same information which Alice and Bob have and at the end of the procedure she would have the same key. However, Alice uses photons from conjugate basis, i.e. there is no orientation of the polarizer by which Eve could with certainty

32 Markagić(2012)

differ the photons polarization. In the second case, Eve wants with several differently oriented polarizators, with certainty to establish the photons polarization. Nevertheless, multiplying of unknown quantum state is not possible because of the theorem about the impossibility to clone states (quantum no-clone theorem).

During the communication between Alice and Bob, it can occur that part of correctly measured photons will be wrongly detected. In addition to that, if Eve tries to measure photons which Alice sent before they came to Bob, errors will occur because of the fact that Eve is trying to measure the photon polarization data. These two situations cannot be differed: the natural (genuine) and artificial noise look the same. Due to that Alice and Bob agree on smaller cryptographic key in three stages. Those three stages are called error estimate, information levelling and privacy reinforcement.

Safety of quantum cryptography system

In order for quantum systems to be absolutely secure, the following requirements must be fulfilled:

- Eve cannot access Alice and Bob's encryption and decryption devices;
- Random numbers generator which Alice and Bob use must provide truly random numbers;
- Classical communication channel must be authenticated using absolutely secure authentication schemes.[33]

Attacks on quantum cryptographic system can be divided into:

1. Intercept and resend attack (Eve is in the middle)
2. Photon beam splitting attack
3. Hacker attack
4. DoS attack.

ADVANTAGES AND DISADVANTAGES OF QUANTUM CRYPTOGRAPHY

It is important to say that information transmission over unitary photons is still impractical method. The speed of data transmission is several hundred bits per second, so this transmission system is used only for agreement on secret key, while real communication, which should be protected, is performed through public channel, encoded with thus determined and transmitted key. There are also other obstacles for practical implementation of quantum cryptography. The range of unitary photon through optical fibre is, with contemporary technology, about hundred kilometres, which prevents the sender and the recipient of the message to be at larger distances. If they are computers, there can be a network of directly connected computers. All this requires a lot of time and computer equipment, but is still attainable.[34]

The scope of quantum cryptography problems can be perceived from the following facts:[35]

- Polarisers are imperfect, which affects both the production and detection and enlarges the possibility of wrong transmission.
- Directions of polarizer axis on transmission and receiving sides never perfectly match, which enhances errors.

33 Picek(2009)
34 Čisar(2015)
35 Jakuš(2004)

- Photon emitters do not always generate unitary photons. They mostly emit certain number of photons simultaneously, distributed according to Poisson distribution. With beam with less than 1% of admixture of multiplied photons, efficiency of emitters for launching one photon is around 10%.

- When passing through optical fibre, photos are absorbed and their polarization is changed, which enhances wrong detections.

- Photon detectors have efficiency of 10% to 30%, which implies that some photons are not detected at all.

- Photon detectors have noise, therefore, from 10 to 100 false detections happen per second.

CONCLUSION

Quantum cryptography will experience a boom, if not before, then when quantum computers become a reality. Then the algorithms in the field of classical cryptography will no longer provide reliable protection against attacks such as Shor's quantum algorithm for factorization of numbers. Of course, there will be a problem of protection of all the data, which in the past were protected by classical cryptographic systems, and there is a need for secrecy of the data over a longer period of years. At the moment quantum computers are not on the level of development that would pose a threat to the existing systems. On the other hand, quantum computing is constantly evolving problem of building a quantum computer is of technological nature, only in engineering sense and context of stability and decoherence and implication of appropriate quantum operations. Many researchers believe that it will be applicable to reach quantum computers within 10 to 15 years.[36]

The task of cryptography is to exchange secret messages. There are traditional methods that guarantee practically secure communication (between Alice and Bob), if both parties know secret decryption key, and at the same time, the key is not known to anyone else, not even a potential adversary, Eve.

It is this presumption of secrecy "of the secret key" that is the weakest link in the classical cryptography. The only task of quantum cryptography is providing the secret key. So, in quantum cryptography messages are not exchanged, only secret key via the so-called quantum channel. Today there are already commercial devices, as well as dozens of government and corporate implementations of secure communication networks that implement quantum key distribution technology. The advantage of the new technology is unconditional security that is based on the phenomena of quantum mechanics. Today it is practically possible, with unconditional security, to generate and distribute a secret key between two parties linked by optical fibres at distances up to 150 kilometres in a few seconds. Eavesdropping of communication from a third party does not lead to the discovery of the secret but only to a reduction in the speed of key generation, provided that both parties immediately know that the line is actively eavesdropped. The main disadvantages of QKD system are generating the speed limit key, which directly depends on the distance of the participants, the inability to signal amplification and transmission via a kind of relay, practical limit exclusively to communication via optical fibre, as well as the price of the system implementation.[37]

Acknowledgements: This work was done within the projects of the Ministry of Education, Science and Technological Development of Republic of Serbia, No. OI 171039 and TR34019.

36 Markagić(2012)
37 Ijačić(2014)

REFERENCES

1. Bennett C. , Brassard G., Quantum cryptography: Public key distribution and coin tossing, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Institute of Electrical and Electronics Engineers, New York, 1984), pp. 175-179.
2. Bohr N., Atomic Physics and Human Knowledge, Nolit, Belgrade, 1985.
3. C.H. Bennett, "Quantum cryptography using any two non-orthogonal states", Physical Review Letters **68**, 3121-3124 (1992).
4. Čisar P., General aspects of quantum cryptography, Info M 2 (2015)
5. Dugić M., Fundamentals of quantum informatics and quantum calculation, Faculty of Science Kragujevac (2009)
6. Einstein, A., Podolsky, B. & Rosen, N. (1935): *Can quantum-mechanical description of physical reality be considered complete?* Phys. Rev. 47 777.
7. Eckert A., Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67, 661-663 (1991).
8. Heisenberg W., Physics and Metaphysics, Nolit, Belgrade (1974)
9. Ijačić S., The application of quantum cryptography, quantum computing, and post-quantum cipher systems, Master's Thesis, Singidunum, Belgrade (2014)
10. Ilievski E., Quantum cryptorgaphy-seminar, Mathematics and Physics Faculty , Ljubljana University (2009)
11. Jakuš, M. (2004): Quantum cryptography, Faculty of Electrical Engineering and Computation, Zagreb, http://os2.zemris.fer.hr/kvant/2004_jakus/
12. Z. Maric, The experiment on the physical reality, Nolit, Belgrade (1986)
13. Markagić M., The protocols and directions of development of quantum cryptography, Military Technical Gazette, Vol. LX, No. 1, 250-265 (2012)
14. Picek, S. & Golub, M. (2009): Quantum cryptography:development and protocols, Proceedings of the Information Systems Security, MIPRO 2009, Opatija, Croatia. pp. 122-127
15. Schrodinger E., Naturwissenschaften, **23** 807, 823, 844 (1935)
16. Shannon C.E., Bell System Technical Journal **28** 657(1949)
17. Shor P.W., in Proceedings of the 35th Annual Symposium of the Foundations of Computer Science (Ed. S. Goldwasser) Los Alamos, CA:IEEE Computer Society (1994), p.124
18. Stipčević M., Quantum cryptography, http://www.irb.hr/users/stipcevi/download/fer/171203.pdf (2003)
19. Vedral V., Decoding of the reality, 180, Laguna, Belgrade (2014)
20. Wiesner S., Conjugate coding, Sigact News 15, 78-88 (1983).
21. Голубчиков Д.М., Румянцев К.Е.**,** Квантовая криптография: принципы, протоколы, системы, Таганрог, ТТИ ЮФУ, стр. 27 (2008)
22. Килин С. Я.*,* Квантовая информация , Успехи Физических Наук,Т. 169. стр. 507-527(1999)
23. Килин С.Я., Хорошко Д.Б., Низовцев А.П., Квантовая криптография:идеи и практика, Беларуская навука (2007)

UDC: 657.632:519.6

BENFORD'S LAW AND THE ANALYSIS OF THE NUMERICAL DATA[1]

Dusan Joksimovic, PhD[2]
Academy of Criminalistic and Police Studies, Belgrade
Goranka Knežević, PhD
Singidunum University, Belgrade

Abstract: In this article the contemporary generally accepted theoretical analysis and assumptions regarding the implementation of Benford's law are presented. It seems interesting to introduce the perspective to Benford's law as a consequence of the universal law of nature stating that the nature strives the maximum entropy or disorder, as well as the perspective in which Benford's law, aspire to find its place in the contemporary theory of everything in the nature.

The implementation of this law in the analysis of the anomalies in some numerical data in various scientific disciplines is also part of this article. The incorrect numerical data that describes the specific occurrence can be the consequence of the unintentional error in the formation of the numerical data (as a consequence of the bad design of the experiment, the imperfections of the detection of the numerical data, the badly set up model of some process that generates the set of numerical data etc.), but also the consequence of the intentional abuse.

The specific perspective is provided in this article regarding the implementation of this Law in the forensic analysis of the frauds, especially in the analysis of the numerical data that describes various sociological, econometrical and financial irregularities. We show how the mutual usage of Benford's law and specific laws of mathematical statistics, successfully detects potential irregularities in the numerical data and leads the forensic analyst forward in the area of the detection of the potential fraud.

Key words: Benford's law, entropy, Benford's distributions, frauds, forensic analysis, forensic accounting

THE HISTORY OF BENFORD'S LAW

In the second part of the 19th century, the astronomer Simon Newcomb, remarked that the beginning pages of the table of the logarithm are used more heavily than in the last pages. Back in that time, the table of common logarithm was used for the multiplication and divisions of big numbers. He concluded that the numbers that start with the smaller digits were used more often than the numbers with the bigger digits. In the 1881 he published the scientific article [8] describing his remarks, without getting into the assumptions and theoretical analysis of the phenomena[3]. This article was unnoticed and it was forgotten easily.

1 This paper is part of the results of the research on Projects III45003 and III44006 supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia
2 E-mail: dusan.joksimovic@kpa.edu.rs.
3 *Newcomb, S (1881). "Note on the frequency of use of the different digits in natural numbers". American Journal of Mathematics* **4** *(1): 39–40*

In the year 1938 the physicist Frenk Benford found the same conclusion as Simon Newcomb. Benford tested this hypothesis using the 20229 big data from 20 different sources and 2968 data of small numbers from 10 different sources. Sources were found in the natural and social occurrences, such as numbers used for the published journals, the length of the river, the value of some physical constant, the mortality rates, statistics in baseball etc. Differently that Newcomb, Benford in his work [3] determined the mathematical law of frequency distribution of leading digits in the numbers, that was entitled as Benford's law[4].

Starting from the second half of the 80's of the last century, this law started to be used more often in the analysis of the consistency of the numerical data expressed in various social and natural phenomena. Nowadays, the theoretical analysis of this law in the area of finding better mathematical bases and its implementation is still a current issue in contemporary scientific society [1],[2][5].

DEFINITIONS OF BENFORD'S LAW AND THEIR MUTUAL EQUIVALENCY

It is commonly understood that for any base where $B > 1$,any positive real number $(x > 0,\ \ x \in R)$, can be expressed as

$$x = M_B(x) \cdot B^k$$

Where $\in Z$, a $M_B(x) \subset [1, B)$. The number $M_B(x)$ will denote ***mantissa*** of the number x. We can conclude that the following equation is proven to be true

$$M_B(x) = \frac{x}{B^k} = \frac{x}{B^{[\log_B x]}} = \frac{B^{\log_B x}}{B^{[\log_B x]}} = B^{\log_B x - [\log_B x]}$$

where $[\log_B x]$ will denote as the whole part of the number $\log_B x$, or the greatest integer less than or equal to $\log_B x$.

In the scientific practice we can find two mutually equivalent definitions of Benford's law. Benford's law as a function of probability distributions of mantissa numerical data and Benford's Las for the joint probability distribution of representing first ***k*** digits of significant numerical data.

Definition 2.1. (Benford's law for the function of the probability distribution of mantissa)

Random variable ***X,*** whose realizations are only positive values in the base $B > 1$,is recognized under Benford's law if and only if the function of the probability distribution of random variable determined by the mantissa of the random variable ***X*** , ***M(X),***in that base is recognized under the following logarithm law

$$P(M_B(x) \leq m) = \log_B m$$

where $m \in [1, B)$.

4 Frank Benford [1938], The Law of Anomalous Numbers, Proceedings of the American Philosophical Society, Vol. 78, No. 4, p. 551-572

5 Arno Berger, Theodore P. Hill,"A Basic Theory of Benford's law", Probability Surveys,2011,Vol 8, 1-126. Drien Jamain,"Benford's law", Dissertation Report, Department of Mathematics, Imperial College, London, 2011

Definition 2.2. (Benford's law for the joint probability distribution of leading *k* digits in the numbers)

Random variable ***X***, whose realizations are only positive values in the base $B > 1$, follow Benford's law if and only if joint probability distribution first ***k*** significant digits of their realization, $(C_j)_{j=1,2,\dots,k}$, $(k \in N^*)$,satisfies the following law

$$P(C_1 = c_1, C_2 = c_2, \dots, C_k = c_k) = \log_B\left(1 + \frac{1}{\sum_{i=1}^{k} B^{k-i} c_i}\right)$$

where $c_1 \in (1,2, \dots, B-1), c_{j>1} \in (0,1,2, \dots, B-1)$.

At the first sight we can find that the **definition2.2** can be used only for the discrete random variables, but this is not correct, because the condition is that ***k*** belongs to the unlimited set of positive integers and goes to the infinity $(k \in N^*)$.

Also, we can notice that because of the continuity the following expression is valid:
$P(M_B(x) \leq m) = P(M_B(x) < m) + P(M_B(x) = m) = P(M_B(x) < m)$,
because it is $P(M_B(x) = m) = 0$.

Mutual equivalence of these definitions can be proven using the following proofs:

Proof 1.

We can prove that from **Definition 2.1.** follows **Definition 2.2.**

Let the function of probability distribution of mantissa of random variable ***X***, ***M(X)***, in the base $B > 1$, satisfy the law $P(M_B(x) \leq m) = \log_B m$, where $m \epsilon [1, B)$. Then, for the probability distribution of first ***k*** significant digits in the realization of random variable ***X***, $(C_j)_{j=1,2,\dots,k}$, $(k \in N^*)$, satisfies:

$$P(C_1 = c_1, C_2 = c_2, \dots, C_k = c_k) = P\left(\sum_{i=1}^{k} c_i B^{1-i} \leq M_B(x) < \sum_{i=1}^{k-1} c_i B^{1-i} + (c_k + 1)B^{1-k}\right) =$$
$$\log_B\left(\frac{\sum_{i=1}^{k-1} c_i B^{1-i} + (c_k+1)B^{1-k}}{\sum_{i=1}^{k} c_i B^{1-i}}\right) = \log_B\left(1 + \frac{1}{\sum_{i=1}^{k} B^{k-i} c_i}\right)$$

Let us now prove that from the **Definition 2.2.**follows the **Definition 2.1.**

So, in the base $B > 1$, probability distribution of first ***k*** significant digits the realization of random variable **X**, $(C_j)_{j=1,2,\dots,k}$, $(k \in N^*)$, satisfies the following law

$$P(C_1 = c_1, C_2 = c_2, \dots, C_k = c_k) = \log_B\left(1 + \frac{1}{\sum_{i=1}^{k} B^{k-i} c_i}\right) \quad (1)$$

where $c_1 \in (1,2, \dots, B-1), c_{j>1} \in (0,1,2, \dots, B-1)$.

Let $m \epsilon [1, B)$ be comprised of only one digit. Respectively, $m \epsilon [1,2, \dots, B-1]$.

Then, if $m = 1$, because of the infinity the following is satisfied
$P(M_B(x) \leq m) = P(M_B(x) < m) = P(M_B(x) < 1) = 0 = \log_B 1 = \log_B m$
,because $M_B(x) \subset [1, B)$.

If $m = c_1 \neq 1$, respectively $m \epsilon [2, \dots, B-1]$, then it satisfies:
$P(M_B(x) \leq m) = P(M_B(x) \leq c_1) = P(M_B(x) < c_1) = P(C_1 \leq c_1 - 1) = \sum_{l=1}^{c_1-1} P(C_1 = l)$
From (1) follows $P(C_1 = l) = \log_B\left(1 + \frac{1}{l}\right)$ that is why we have the following expression:
$P(M_B(x) \leq m) = \sum_{l=1}^{c_1-1} \log_B\left(1 + \frac{1}{l}\right) = \log_B\left(\prod_{l=1}^{c_1-1}\left(\frac{l+1}{l}\right)\right) = \log_B c_1 = \log_B m.$
Let now $m \epsilon [1, B)$ be comprised of ***k*** digits, where $(k \in N^*)$, $m = c_1 c_2 \dots . . c_k$ in the

base $B > 1$. Therefore, $m = \sum_{i=1}^{k} \frac{c_i}{B^{i-1}}$. Now it is

$$\begin{aligned}
P(M_B(x) \le m) &= P(C_1 \le c_1 - 1) + P(C_1 = c_1, C_2 \le c_2 - 1) + \cdots \\
&\quad + P(C_1 = c_1, \dots, C_{k-1} = c_{k-1}, C_k \le c_k - 1) \\
&= P(C_1 \le c_1 - 1) + \sum_{l=0}^{c_2-1} P(C_1 = c_1, C_2 = l) + \cdots + \sum_{l=0}^{c_k-1} P(C_1 = c_1, \dots, C_{k-1} = c_{k-1}, C_k = l) \\
&= \log_B c_1 + \sum_{l=0}^{c_2-1} \log_B \left(1 + \frac{1}{Bc_1 + l}\right) + \cdots + \sum_{l=0}^{c_k-1} \log_B \left(1 + \frac{1}{\left(\sum_{i=1}^{k-1} B^{k-i} c_i + l\right)}\right) \\
&= \log_B c_1 + \log_B \left(\frac{Bc_1 + c_2}{Bc_1}\right) + \cdots + \log_B \left(\frac{\sum_{i=1}^{k} B^{k-i} c_i}{\sum_{i=1}^{k-1} B^{k-i} c_i}\right) = \log_B \left(\frac{\sum_{i=1}^{k} B^{k-i} c_i}{B^{k-1}}\right) \\
&= \log_B \left(\sum_{i=1}^{k} \frac{c_i}{B^{i-1}}\right) = \log_B m
\end{aligned}$$

With this we make formal equivalency of these definitions.

SOME CHARACTERISTICS OF BENFORD'S LAW

Form the **Definition 2.2.** we can easily show that for the random variable ***X*** that satisfies Benford's law in the base $B > 1$ so the following is valid:

1.The probability of showing the first significant digit

$$P(C_1 = c_1) = \log_B \left(1 + \frac{1}{c_1}\right), c_1 \in (1,2, \dots, B-1).$$

This characteristic in the base $B = 10$, was detected in the first works of Newcomb-a [8] and Benforda [3][6].

2.Probability of showing *k*-significant digit where $k \ge 2, (k \in N^*)$ je:

For $k \ge 2, (k \in N^*)$

$$P(C_k = c_k) = \sum_{i=B^{k-1}}^{B^{k-1}-1} \log_B \left(1 + \frac{1}{i \cdot B + c_k}\right)$$

$$c_k \in (0,1,2, \dots, B-1).$$

Numerical and graphical analysis of the characteristics 1. and 2. is done in the next section (it was shown only as the distributions with the bases B= 10, 9, 6). This presents that, starting with the fourth significant digit and forward in all of the bases (digits $C_{k \ge 4}$), almost uniformly distributed, and we can say that for the probability distribution of the third digit. That is why the implementation of Benford's law in the practice is constrained on the analysis of the probability distribution first two significant numbers, and only sometimes it is the analysis of the distribution of the third significant number in the set of numerical data.

6 *Newcomb, S (1881). "Note on the frequency of use of the different digits in natural numbers". American Journal of Mathematics* **4** *(1): 39–40,* Frank Benford [1938], The Law of Anomalous Numbers, Proceedings of the American Philosophical Society, Vol. 78, No. 4, p. 551-572

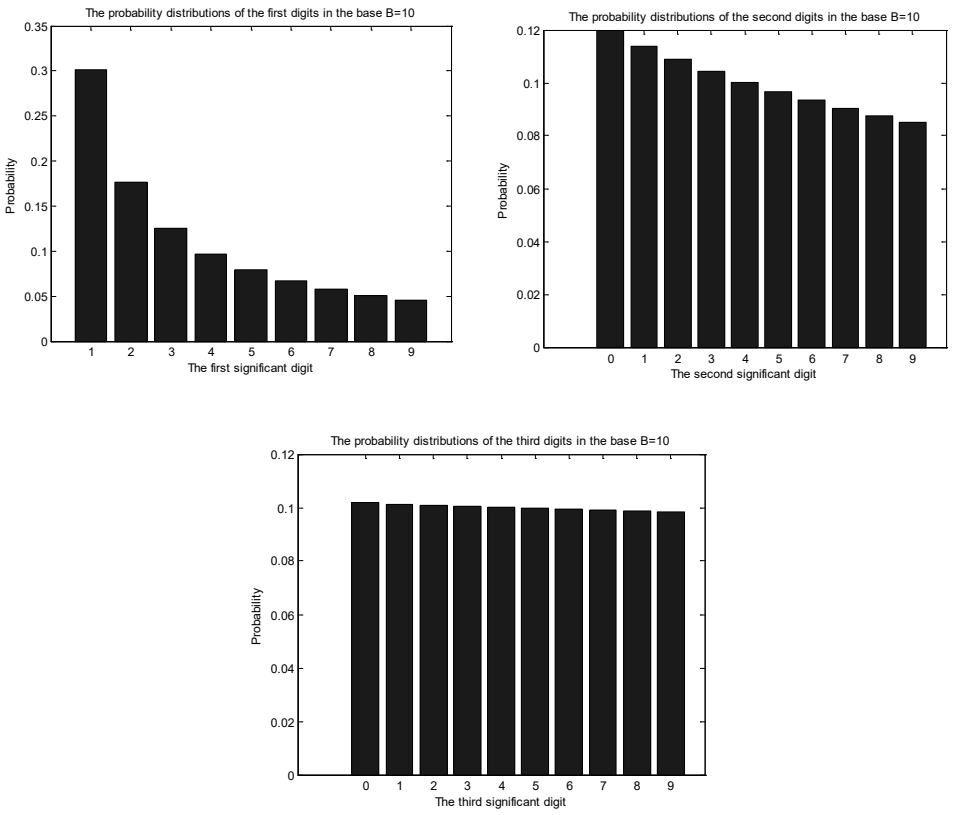


Figure 1: *The probability distributions of the first, second and third digits in the base B=10*

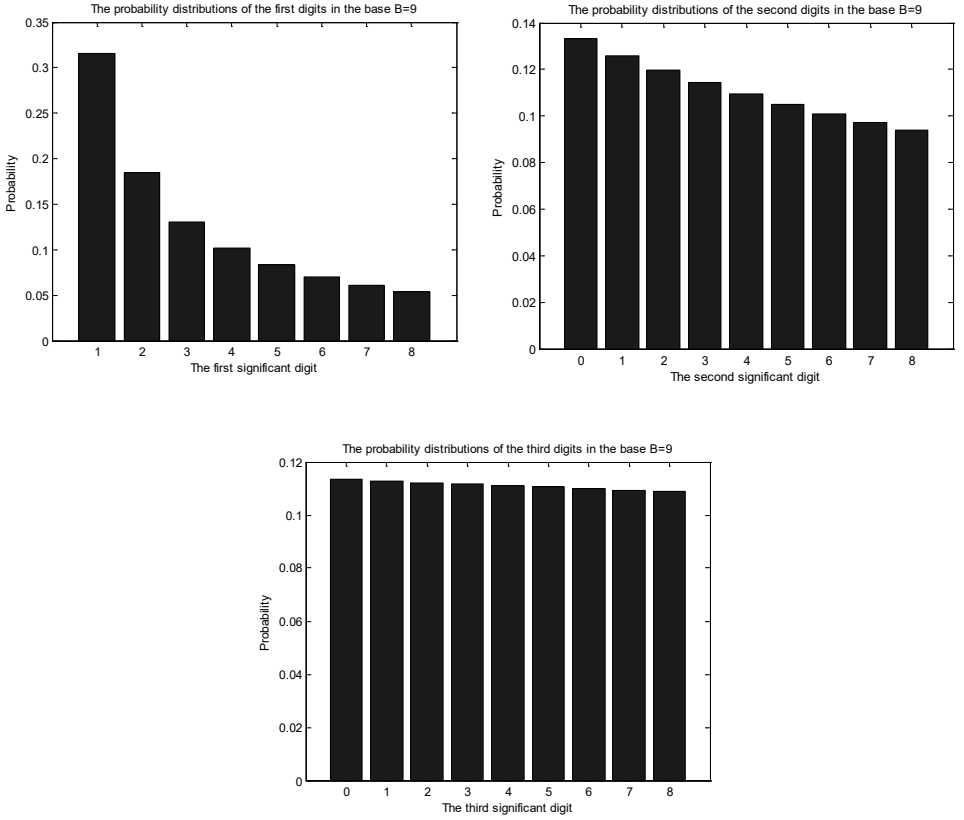
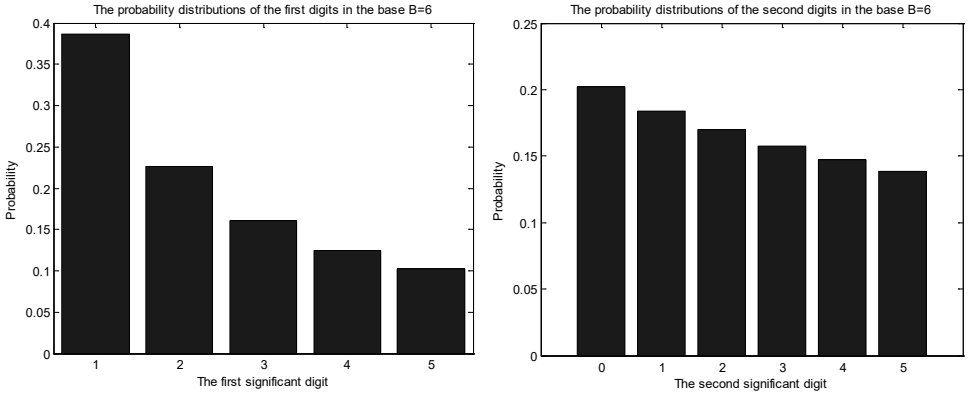


Figure 2: *The probability distributions of the first, second and third digits in the base B=9*



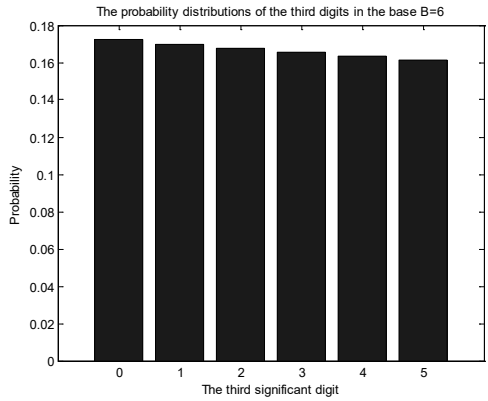


Figure 3: *The probability distributions of the first, second and third digits in the base B=6*

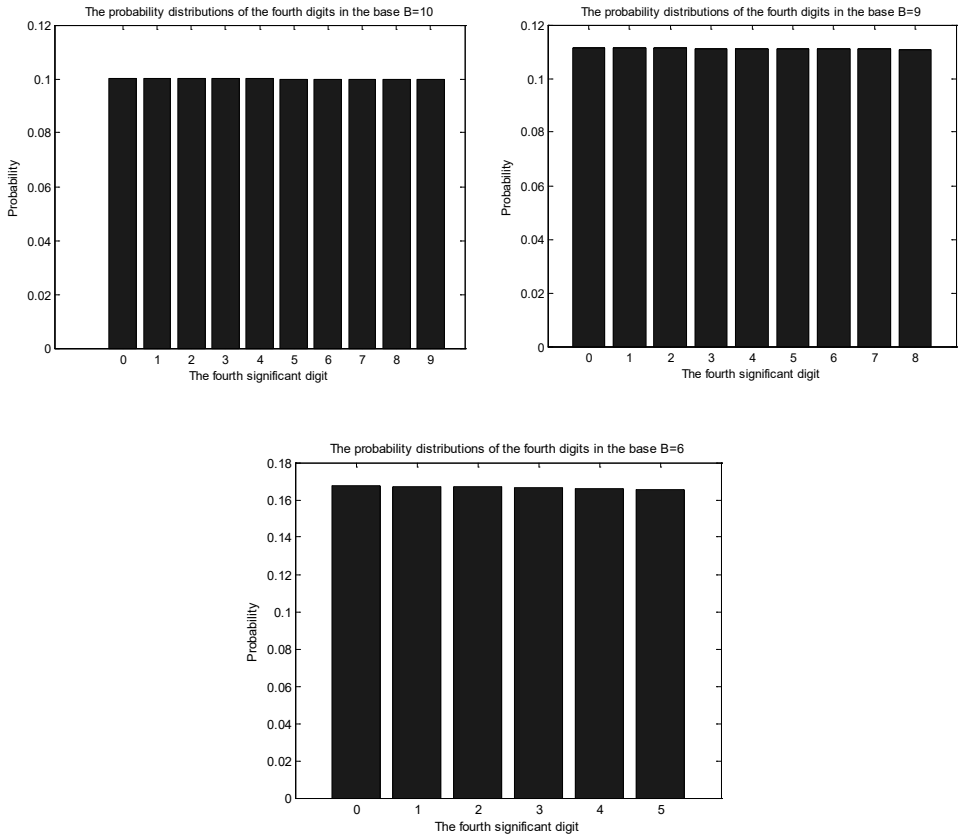


Figure 4: *The probability distributions of the fourth digit in the bases B=10,9,6*

3.The occurance of the significant digits at the realizations of the events that satisfy the Benford law are not mutually exclusive events

We can easily state that from the **Definition 2.2** for $k \geq 2, (k \in N^*)$ is valid

$$P(C_1 = c_1, C_2 = c_2, \dots, C_k = c_k) \neq \prod_{i=1}^{k} P(C_i = c_i)$$

This property shows that the appearance of the significant number within the realization of the events that satisfy Benford's law, are not mutually exclusive events. This fact opens many questions in the area of investigating these distributions and finding some universal law, which is in the essence of events that satisfy Benford's law. On the other hand, these events are from a large number of scientific disciplines and areas, and at the first sight they seem completely unrelated, some scientific and academic researchers consider that the Benford Law is one of the detectors of the existance of the theory of everything, to whom the top of the world scientists try to come closer in the last decades.

4. Theoretical possibility of generating Benford's random variable

Taking into consideration that the **(Definition 2.1.)** is valid

$P(M_B(x) \leq m) = \log_B m$, where $m \epsilon [1, B)$

We can generate the random variable mantissa $M_B(x)$, that satisfies Benford's law in the base $B > 1$, generating the $B^U \rightarrow M_B$, where the random variable U is uniformly distributed in the interval $(0,1)$, therefore , $U \sim \mathcal{U}(0,1)$.

One of the consequences of this characteristic is that the set of one digit numerical data that satisfy Benford's law can be generated using $[B^U]$, where with the $[\ ]$ we denote the whole part of the number and where the U is uniformly distributed within the interval $(0,1)$, respectively $U \sim \mathcal{U}(0,1)$.

Therefore, taking into consideration that the following is valid $M_B(x) = B^{\log_B x - [\log_B x]}$, we can conclude that the random variable X satisfies Benford's law if and only if the random variable $\log_B X - [\log_B X]$ is uniformly distributed in the interval $(0,1)$, therefore $\log_B X - [\log_B X] \sim \mathcal{U}(0,1)$, or $\log_B X \bmod 1 \sim \mathcal{U}(0,1)$. Otherwise, the number $\log_B X - [\log_B X]$ represents the fraction part of the number $\log_B X$.

Therefore, the following is valid :

$$\log_B X \bmod 1 \sim \mathcal{U}(0,1) \Leftrightarrow X \text{ satify the Benfornd's Law} \quad (2)$$

Based on Kronecker-Weyl theorem, that states that for each irrational number $\alpha \epsilon R \backslash Q$,sequence $z_n = n \cdot \alpha$, where $(n \in N^*)$ uniformely distributed based on the modul 1, therefore $n \cdot \alpha \bmod 1 \sim \mathcal{U}(0,1)$, and identity (2), is valid for all irrational number $\alpha \epsilon R \backslash Q$, sequence $B^{n\alpha}$, where $(n \in N^*)$, satisfy Benford's law in the base $B > 1$.

Sequence $\{a^n\}$ satisfy Benford's law if and only if $\log_B a$ irational number.

5. The hypothesis of the scale and base invariance for the data that satisfy Benford's law

The event space $\mathcal{M}_B$ for which the **Definition 2.1.**, in the base B > 1, is defined as

$$\mathcal{M}_B=\left\{\bigcup_{k=-\infty}^{\infty} S\cdot B^k \ , for\ all\ Borel\ \ S\subseteq[1,B)\right\}$$

The event space $\mathcal{M}_B$ we call mantissa algebra, which is , σ-algebra as a sub σ-field of the Borel.

So, for any set E it is valid:

$$E\in\mathcal{M}_B\Leftrightarrow E=\bigcup_{k=-\infty}^{\infty} S\cdot B^k, \qquad S\epsilon\mathcal{B}([1,B))$$

Where $\mathcal{B}([1,B))$ denotes Borel's set $[1,B)$.

This σ-algebra $\mathcal{M}_B$has the following properties:

Each non empty set in $\mathcal{M}_B$ is infinite with the accumulation points at 0 and $+\infty$

$\mathcal{M}_B$is closed under scalar multiplications,
$(e>0, E\epsilon\mathcal{M}_B\Rightarrow e\cdot E\ \epsilon\mathcal{M}_B)$

$\mathcal{M}_B$ is closed under integral roots, but not integral powers , e.g.

$(m\in N, E\in\mathcal{M}_B\Rightarrow E^{\frac{1}{m}}\in\mathcal{M}_B)$

$\mathcal{M}_B$ is self similar in the sense that $(E\in\mathcal{M}_B\Rightarrow B^m\cdot E\epsilon\mathcal{M}_B)$ for all $m\in Z$.

Property b) is in the essence of the scale invariance hypothesis, and the properties c) and d) are in the essence of the base invariance hypothesis for the occurrences whose realization satisfies Benford's law, and for the numerical data that has some properties of Benford's law.

The hypothesis of the scale and base invariance for the numerical data can be formulated, but not strictly mathematically, in the following way:

Scale invariance hypothesis: If some random variable ***X*** satisfy Benford's law, than the random variable $\boldsymbol{a\cdot X}$, where $a>0, a\in R$, also satisfy this law, multiplication with some positive scalar cares about Benford's properties under the numerical data that has that properties.

We can say that this hypothesis was tested theoretically and practically and it passed them all. In the year 1995 Hill found that in the base $B=10$, probability density under the field $(R^+,\mathcal{M}_{10})$ is scale invariant if and only if that probability satisfy Benford's law [11][7].

The base invariance hypothesis is much more sensitive. This one tries to answer the question if Benford's property of some random occurrence or set of numerical data which is detected in the base $B>1$, is valid on that set even when the set of data is converted into the other base. It was shown that [11][5] that Benford's properties transfer into the other base for the Borell's sets, while for the dot set we cannot be sure of that. In that case the combination of probabilities that satisfy Benford's law and Dirak's measures of the probability with the constant one, help to preserve the property of the base.

Above all it was presented that if some random variable satisfies the hypothesis of the scale invariance than that also satisfies the base invariance hypothesis, but the inverse does not hold true.

7 Theodore P. Hill,"A Statistical Derivation of the Significant-Digit Law",Statistical Science, 1995,Vol.10,No4,354-363

6. Hypothesis of the sum invariance

Random variable is sum invariant in the sense that if for any natural number $n \in N$ the expected sum of mantissae of all entries starting with the fixed *n*-tuple of significant digits is the same as that for any other n –tuple. It was presented that the random variable is sum invariant only if it satisfies Benford's law.

Sum invarianced for Benford's data is proven in the sense of ***the expected*** sums, in the real Benford's data that sum is not exactly equal, but some variance exists. The analysis of this variance leads to the certain results that assures the practical usage on the data that satisfy Benford's law.

7. Benford's law as a consequence of closed system aspiration to the maximum entropy

One of the universal law in the universe is the law on the maximum entropy that states that all isolated system in the universe have an aspiration to the maximum entropy, or disorder. This is the state in which all the possibilities are equaly possible. It shows that [7],[9],[11][8] that Benford's law is the consequence of that universal law. That is why even in the most contemporary theory of everything, Benford's law is analyzed as one of potential paths to that comprehensive solution. However, the fact that Benford's law is derived from the maximum entropy of the system in which it is used, shows us the successful implementation of this law in the large spectrum of natural and social events.

TESTING OF BENFORD'S LAW AT THE SET OF NUMERICAL

Let it be some sample set comprising of ***N*** numerical data $\bar{X} = \{\bar{x}_i | \ i = 1,2, \dots, N\}$. It was developed in the practice the specific number of tests that investigate whether the significant numbers of this set deviate from Benford's law. All of these tests are constructed under the method of statistical hypothesis where the nil hypothesis

H_0: Significant numbers of the sample satisfy Benford's law

And an alternative hypothesis that is accepted or rejected depending on the nature of the test

H_1: Significant numbers of the sample do not satisfy Benford's law.

Test significance is $\alpha = 0{,}05$, that means if the alternate hypothesis is to be accepted we can say that the significant numbers do not satisfy Benford's law.

In large number of iterations this shows the anomaly of the observed data, and the possibility of having an error (intentional and unintentional). As a matter of fact, we consider the data that are realization of events that satisfy Benford's law. If we do not accept the alternate hypothesis, this does not mean that the set of data do not satisfy Benford's law, but it can be the consequence of the fact that we do not have the adequate level of significance that the data is to satisfy Benford's law.

There are many tests developed and used for the testing of Benford's law at the numerical data (test of the absolute deviation, Pirson χ^2 test, Kuiper test, *Z*- test, Test of the sum invariance, Test of the factors of distortion, Second level test, Test of doubling the digits, Test the last two digits...).

8 Sofia B. Villas-Boas, Qiuzi Fu, George Judge, „Is Benford's law a Univerzal Behavioral Theory?", Econometrics 2015,3,698-708Oded Kafri „Entropy Princip in Direct Derivation of Benford's law",Varicom Communications Michaele Ciofalo,"Entropy, Benford's first Digit Law and The Disribution of Everything"

In this paper we are going to describe the mean absolute deviation test and Pirson χ^2.

-Test of the mean absolute deviation (MAD-Mean Absolute Deviation)

MAD is calculated for the first, second and the first two digits

$$MAD(C_1) = \frac{1}{9}\sum_{c_i=1}^{9} |P(\bar{C}_1 = c_i) - P(C_1 = c_i)|$$

$$MAD(C_2) = \frac{1}{10}\sum_{c_i=0}^{9} |P(\bar{C}_2 = c_i) - P(C_2 = c_i)|$$

$$MAD(C_1C_2) = \frac{1}{90}\sum_{c_i=1}^{9}\sum_{c_j=0}^{9} |P(\bar{C}_1 = c_i, \bar{C}_2 = c_j) - P(C_1 = c_i, C_2 = c_j)|$$

Where with the $P(\bar{C}_1 = c_i)$, $P(\bar{C}_2 = c_i)$, $P(\bar{C}_1 = c_i, \bar{C}_2 = c_j)$ we denote the probability distribution for the first, second and the first two significant digits in the sample $\bar{X} = \{\bar{x}_i | \ i = 1,2, \ldots, N\}$, a sa $P(C_1 = c_i)$, $P(C_2 = c_i)$, $P(C_1 = c_i, C_2 = c_j)$ we denote the probability for the second and the first two digits shown in Benford's law, according to the **Definition 2.2**

At this test there are no critical values that are exactly mathematically determined, but instead there are critical values got by the experience at the practical tests and they are [13][9]

Table 1: *Critical values for the mean absolute deviation test [9]*

Decisions	First digit	Second digit	First two digits
Close agreement	<0,004	<0,008	<0,0006
Accepted agreement	0,004-0,008	0,008-0,012	0,0006-0,0012
Marginal agreement	0,008-0,012	0,012-0,016	0,0012-0,0018
No agreement at all	>0,012	>0,016	>0,0018

-Pirson χ^2

Pirson χ^2 test denote $\sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i} \sim \chi^2_{k-1}$, where

O_i- sample frequency

E_i- expected frequency

The appearance of the characteristics of the set classified into k classes. In this case number of classes is equal to the number of digits for which the analysis is (k=9 for the anlysis of the first digit, , k=10 for the analysis of the second digit, k=90 for the first two digits), and this test is then:

$$N \cdot \sum_{c_i=1}^{9} \frac{(P(\bar{C}_1 = c_i) - P(C_1 = c_i))^2}{P(C_1 = c_i)} \sim \chi^2_8$$

$$N \cdot \sum_{c_i=0}^{9} \frac{(P(\bar{C}_2 = c_i) - P(C_2 = c_i))^2}{P(C_2 = c_i)} \sim \chi^2_9$$

9 Philip D. Drake, Mark J. Nigrini,"Computer Assisted Analytical Procedures Using Benford's Law", Journal of Accounting Education 18, 2000, 127-146

$$N \cdot \sum_{c_i=1}^{9} \sum_{c_j=0}^{9} \frac{\left(P(\bar{C}_1 = c_i, \bar{C}_2 = c_j) - P(C_1 = c_i, C_2 = c_j)\right)^2}{P(C_1 = c_i, C_2 = c_j)} \sim \chi^2_{89}$$

Critical values are taken from the χ^2_n tables for the level of significance $\alpha = 0{,}05$, or for some other level of significance. This test is very sensitive to the deviations of Benford's law, and it is sensitive to enlarging of the sample $\boldsymbol{N}$.

SOME EXAMPLES OF BENFORD'S LAW IMPLEMENTATION

General conditions that some of numerical data should meet in order to satisfy Benford's law were subject to the analysis of many papers and researchers [5], [6][10].

Some of these conditions are as follows:

- data must describe a similar phenomenon, i.e that they have the same nature or the same set of sources that generate them (financial transactions, the results of various measurements of length, volume, etc...)
- no need for boundaries of minimum or maximum values
- data must have an incidental nature, rather than some previously generated data using a pattern, such data are serial numbers, phone numbers, personal identification numbers, social security numbers, tax numbers, car registration, account numbers...
- data should comprise more small than large numbers, and that the average value is less than the median (positive asymmetry), the higher the ratio of the mean divided by a median, the data are more suitable for this analysis.
- data should be reported under the same units of measurement
- data should include at least two orders of magnitude.

Examples of events that generate data that satisfy Benford's law are: the price of securities on the stock exchange, financial transactions, bank cards, some processes in telecommunication and computer systems, processes that describe recurrent sequences (Fibonacci sequence, fractals). The natural demographic population growth processes of plants and animals, and many others. Subject to Benford's analysis can be also frequency of categorical data.

Some examples of the usage of this law are:

- In mathematics it seems that many dynamic systems generate data that are subject to Benford's law. Also, many recurrence relations, as well as solutions of certain classes of difference equations are associated with Benford's law. Markow chains are also associated with this law. First digit of prime numbers also follow Benford's law. In this case the observer pattern must be very large (n>10^6 prime numbers). Newton iterative procedure generates data that are subject to this law, and so on.

- In the economy we can find some famous examples of the application of Benford's law. Mark J. Nigrini analyzed tax returns. This is the beginning of the use of this law for the detection of fraud. The basic assumption is that the frequency of significant digits that do not follow the Benford's law suggests a possible irregularity in the transactions. This method was quickly adopted by some supervisory authorities and recognized as a valid audit procedure. So now there are standard software packages that use Benford's law. It has a very respectable role in detecting fraud. In the detection of scam Benford's law can be applied

10 Mark J.Nigrini,"I've Got Your Number", Journal of Accountancy, May 1999, 187, 5; 79-83
Mark J. Nigrini, Linda J.Mittermaier,"The Use of Benford's law As An Aid In Analytical Procedures", Auditing A Journal of Practice and Theory, Vol 16, No 2 1997

and this is the most widely used area for this law. This method was soon found and applied in the detection of fraud with credit cards and other forms of fraud in electronic business. Detection of fraud is not the only application of this law. Creative accounting causes many of the material misstatement in financial statements and that is why the Benford's law is needed [4][11]. It is applied in the analysis of structural deficiencies in macroeconomic data, the analysis of investment programs, accounting reports, traffic reports, forensic accounting [10][12], etc.

- In informatics and computing science it is shown, based on the law of Benford, that computer design that minimizes the storage space is based on the base B = 8. It is also used for analysis of the size of the files in the folders, as well as the duration of the analysis of various processes in multi-user environments, etc ...

- in cryptology Benford's law is used in the hidden writing (steganography) and the stylometry (analysis of linguistic styles and habits of individuals writing).

This law is also applied in a number of other problems in various fields, in almost all natural and social events and random processes such as: psychology, demographics, nuclear physics, astronomy, geology, accelerations algorithmic solutions, time series analysis, neural networks, etc.

Benford's law cannot be used in the following cases:

Data analysis where data are normalized to some process (min-max normalization, ii normalization using standards covering deviations, etc.).

- if the sample has more dimensions and if in some dimension some data are missing,

- if it is only part of the elements of the sample subject to multiplication by a number. Therefore, data must be presented in a single measuring system

CONCLUSION

Benford's law has determined the probability of occurrence of significant digits in the realization of random variables and in the analysis of numerical data, in a very wide range of events. Under certain conditions this law has a universal character. It is valid in all the various systems and it finds the application in almost all natural and social phenomena, in the analysis of the events that have some measurement system.

So far it is the most used in forensics, in the analysis of intentional fraud, especially in the various financial statements and the interpolation process analysis (Newton's iterative process), in the optimizing of computer systems, accelerating algorithms, deciphering hidden messages, and in many other analyzes. So far it is not exactly mathematically proven why numerical data under certain conditions meet Benford's distribution. For some specific events such evidence exists, but not in general. In a modeling problem of the existence of Benford's distribution, it is shown that it is a consequence of the law of universal aspirations of closed system to move to a state with maximum entropy, and it is present in all natural and social phenomena, which in a given analysis can be considered to be closed. Mathematical implications of this law are defined in a specific Borel σ-field, which is called algebra mantisa.

We believe that the implementation of this law will be more prominent, and it will be used in the practical, but also in the scientific analysis of a multitude of phenomena in many different areas.

11 G. Knežević, Mizdraković, V. Arežina, N. „Management as a cause and effect of creative accounting suppresion", Management – časopis za teoriju i praksu menadžmenta, FON, (17), 62, 5-11
12 S.Muminovic, V.Pavlovic,"Application Benford's law in Forensic Accounting", Revizor, No 61, 2013,59-69

REFERENCES

1. Arno Berger, Theodore P. Hill,"A Basic Theory of Benford's Law", Probability Surveys,2011,Vol 8, 1-126
2. Drien Jamain,"Benford's Law", Dissertation Report, Department of Mathematics, Imperial College, London, 2011
3. Frank Benford [1938], The Law of Anomalous Numbers, Proceedings of the American
4. Philosophical Society, Vol. 78, No. 4, p. 551-572
5. *G. Knežević, Mizdraković, V. Arežina, N. „Management as a cause and effect of creative accounting suppresion", Management – časopis za teoriju i praksu menadžmenta, FON, (17), 62, 5-11.*
6. *Mark J.Nigrini,"I've Got Your Number", Journal of Accountancy, May 1999, 187, 5; 79-83*
7. *Mark J. Nigrini, Linda J.Mittermaier,"The Use of Benford's Law As An Aid In Analytical Procedures", Auditing A Journal of Practice and Theory, Vol 16, No 2 1997*
8. *Michaele Ciofalo,"Entropy, Benford's first Digit Law and The Disribution of Everything"*
9. Newcomb, S (1881). "Note on the frequency of use of the different digits in natural numbers". American Journal of Mathematics ***4*** (1): 39–40
10. *Oded Kafri „Entropy Princip in Direct Derivation of Benford's Law",Varicom Communications*
11. *S.Muminovic, V.Pavlovic,"Application Benford's Law in Forensic Accounting", Revizor, No 61, 2013,59-69*
12. *Sofia B. Villas-Boas, Qiuzi Fu, George Judge, „Is Benford's Law a Univerzal Behavioral Theory?", Econometrics 2015,3,698-708*
13. *Theodore P. Hill,"A Statistical Derivation of the Significant-Digit Law",Statistical Science, 1995,Vol.10,No4,354-363*
14. *Philip D. Drake, Mark J. Nigrini,"Computer Assisted Analytical Procedures Using Benford's Law", Journal of Accounting Education 18, 2000, 127-146*

UDC: 007:35.077]:004
004.7.056:35.077

THE IMPORTANCE OF SECURE ACCESS TO E-GOVERNMENT SERVICES

Petar Milić
University of Niš, Faculty of Electronic Engineering
Kristijan Kuk, PhD[1]
Academy of Criminalistic and Police Studies, Belgrade
Turhan Civelek
Kirklareli University, Engineering Faculty,
Software Engineering Department
Brankica Popović, PhD
Academy of Criminalistic and Police Studies, Belgrade
Stefan Kartunov
Technical University of Gabrovo,
Faculty of Mechanical and Precision Engineering

Abstract: E-government services that enable businesses and citizens to easily find the information or service they need, has also brought security threats with it. These security threats may encourage cyber attackers towards activities motivated by financial gains and breaking down infrastructure that offers e-government services. Absence of policies and strategies for secure access and protection of information in offered e-services increases possibility for illegal access and altering of private data and theft of enterprise data. Ensuring higher confidence level in e-government services can be achieved through data encryption in transmission, applying of intrusion detection mechanisms, authenticating users that access sensitive information along with legal editing of all aspects of access to e-services. The aim of this paper is to give insight in the development and implementation of different security solutions in the field of e-government services, describing the importance of delivering of secure e-services to the end users. High level of confidence and trust among all users (citizens, businesses and government) will be the foundation of a successful e-government initiative.

Keywords: e-government security, e-service security, cyber attacks, cyber security.

INTRODUCTION

The concept of privacy is difficult to fully describe since it is a truly multi-dimensional notion which involves, but is not limited to, cultural, social, legal, political, economic and technical aspects. The domain of privacy partially overlaps security, which can include the concepts of appropriate use, as well as protection of information. Applying a system of ICT measures for protecting privacy and enabling secure environment in rapid technological

1 E-mail: kristijan.kuk@kpa.edu.rs.

evolution are not problem free. Growth of computerised facilities cannot be considered as 'progress' until we are sure that the drawbacks do not outweigh the benefits. Therefore, an essential responsibility of e-government is to fulfil the fundamental security properties of: availability, confidentiality, integrity, accountability and information assurance via securing access to its services, portals and platforms[2]. How privacy can be enforced, Medjahed et al.[3] describe in their work on creating comprehensive infrastructure for providing customized government services over the Web while maintaining citizens' privacy.

Trustworthiness in e-government services is related to their security, as perception of trustworthiness could also impact citizens' intention to use e-government services[4] Citizens need to be sure that they exploit e-government services in secure manner along with the guarantees that their data will not be misused and privacy diminished, because it is in this way that confidence in government is created. Also, Carter & Bélanger (2005) have showed in their research that trustworthiness is composed of two constructs: trust of the internet and trust of state government confirming empirically their hypothesis. Here we can conclude that security is a key factor in enabling reliable, transparent and efficient government. Joshi, et al., (2001)[5] claim that notion of security in e-government platform and services includes confidentiality or secrecy, integrity, availability, accountability and information assurance. Depending on the environment, the relative emphasis assigned to each of these objectives may vary. For example, for defense e-government services confidentiality may be the primary requirement, whereas in business sector information integrity is paramount.

E-government services are available through e-government platforms. These platforms are built by the use of commonly accepted state-of-the-art standards, basing it on proprietary or non-proprietary solutions. Ensuring the security in them is achieved mostly via Public Key Infrastructure (PKI) along with fine-grained access control for the definition who can do what, when, and where[6]. They can be open source or commercial. One of the pitfall with open source e-government platforms is that the support for the offered software may not be available which could lead to possible security threats as they are not maintained timely, keeping in mind at the same time ICT technologies rapid progress. When this e-government platforms are combined with the continuously increased citizen mobility, they become a source of possible security threats as allowing access to services for the users virtually anywhere leads to the dramatic expansion of the universe of ineligible people who may attempt to harm the system. Also, it is important to keep in mind that hardware and software infrastructure that support e-government portals i.e. platforms, and in that way e-services offered by them, is one of the factors that affects the security. This infrastructure introduces the risks by the inappropriateness of the hardware or software such as unreliable hardware, limited computing resources, poor communication infrastructure, unstable software, maintainability. All these factors need to be examined on a case-by-case manner.

2 Lambrinoudakis, C., Gritzalis, S., Dridi, F. & Pernul, G., 2003. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. Computer Communications, XXVI(16), pp. 1873-18893.
3 Medjahed, B., Rezgui, A., Bouguettaya, A. & Ouzzani, M., 2003. Infrastructure for E-Government Web Services. Internet Computing, IEEE, VII(1), pp. 58-65.
4 Carter, L. & Bélanger, F., 2005. The utilization of e-government services: citizen trust, innovation and acceptance factors. Information systems journal , XV(1), pp. 5-25.
5 Joshi, J., Ghafoor, A., Aref, W. G. & Spafford, E. H., 2001. Digital Government Security Infrastructure Design Challenges. Computer, XXXIV(2), pp. 66-72.
6 Kaliontzoglou, A., Sklavos, P., Karantjias, T. & Polemi, D., 2005. A secure e-Government platform architecture for small to medium sized public organizations. Electronic Commerce Research and Applications, IV(2), pp. 174-186.

SERVICE AND DATA PRIVACY

E-government offers a wide range of services to citizens and business. These services include issuing any type of personal documents, access to medical records, employment history and other. Each of these services must be accessed in a secure manner, in order to prevent misusing of personal or sensitive business data. Also, these services have their own privacy policies that specify a set of rules applicable to all users. These policies should define the purposes for which a service can use collected information, whether and how long the service can store information and specification about how, and to whom a service can reveal the information. For example, medical usage policy must declare that citizens information will not be used for purposes other than those directly related to providing health services. There are also services that exist on central e-government portals, which passed through some level of integration, from local to national level. In this case, government should ensure that all privacy and security practices are consequently displayed no matter what direction an individual is taken on the portal when requesting information[7]. The level of data collection and constituent privacy concerns increase as government services move through the stages of e-government. E-service privacy also depends on the user perception of information's sensitivity, because they expect or require different levels of privacy. Bélanger & Carter, (2008), in their research[8] on issues that affects e-government services security and privacy, claim that trust on the internet, trust of the government, disposition to trust and perceived risk have impact on the use of e-government services.

Preserving privacy and security of the data collected through e-government services and which are stored in government databases requires consideration of different aspects of their further processing. The data related to specific individuals are privacy-sensitive, whereas the statistical data are privacy-neutral. Privacy-neutral data are mostly available in anonymised form, where no one who accesses them cannot determine the identity of personal data, which are as we said earlier privacy-sensitive. To increase a level of data security especially privacy-sensitive data, they should be protected by privacy policy. These privacy policies offer a certain level of security of sensitive data, which at citizens and business, creates trust in e-government services that make them available. Privacy protection fosters the collaboration between different data owners as they may be more willing to collaborate if they do not need to reveal their data. For example, if privacy-sensitive data are needed for the purposes of data mining, in order to preserve privacy, we can:

- Distribute a limited subset of data;
- Distribute purposely distorted data records, and
- Distribute the computation instead of data.

Citizens and business have no opportunity to verify the provided data privacy, and because of that they need to accept a certain security uncertainty[9]. Additionally, data privacy has to be divided into short and long-term privacy, because short-term privacy has to ensure the privacy of the data while the task is active, e.g. transmission privacy, while on the other side, long-term privacy deals with the time after the task has been completed[10].

7 Hiller, J. S. & Bélanger, F., 2001. Privacy Strategies for Electronic Government. In M. Abramson & G. Means ed. New York: Rowman & Littlefield.
8 Bélanger, F. & Carter, L., 2008. Trust and risk in e-government adoption. The Journal of Strategic Information Systems, XVII(2), pp. 165-176.
9 Wimmer, M. & Von Bredow, B., 2002. A holistic approach for providing security solutions in e-government. Hawaii, Proceedings of the 35th Annual Hawaii International Conference on System Sciences, pp. 1715-1724.
10 Hof, S., 2002. Arguments for a Holistic and Open Approach to Secure e-Government. France, First International Conference, EGOV 2002 Aix-en-Provence, pp. 464-467.

TOOLS AND TECHNIQUES FOR PRESERVING SECURITY IN E-GOVERNMENT

In order to ensure safe use of e-government services, beside the development of awareness of the users on the need for proper use of these services, they must be equipped with the technologies that provide the appropriate level of security. This applies particularly to World Wide Web, because this is the most utilised approach for exposing government services to citizens and business. Protecting technologies can be both commercial and open source. Anonymizer[11] is a service that protects user privacy from web server where e-service is located. They deal with providing anonymity to the users from anyone watching the Internet near it.

Java Anon Proxy is a web-only anonymization tool, developed as a research project at the Technical University of Dresden[12]. Web requests and replies are divided into fixed-sized chunks, and sent through a series of mix nodes. Each such node collects a batch of these chunks, encrypts or decrypts them as appropriate, reorders them, and sends them on to the next mix node.

Protecting the content of web transactions can be done via Secure Sockets Layer (SSL) and Transport Layer Security (TLS) set of protocols. No special installation or configuration needs to be done by end users before they can benefit from e-services. Support for these protocols is built-in in most of today's browsers where they automatically encrypt/decrypt request/response to/from web server.

In some cases, e-government services may require some payment from its users such as payment of different types of taxes toward government, bills, insurance and other. The lack of adoption of electronic cash as a payment method, filling the gap of unavailability of serious electronic cash mechanisms, can be done with the set of available privacy-enhancing technologies. An alternative that gains a popularity is PayPal[13]. It enables true privacy-friendly payments online with its own payment infrastructure. Using this service requires the registration of users at PayPal, then transfer some money to PayPal accounts using a bank or credit/debit card. A recipient of PayPal transfer may request a check from PayPal, or openning PayPal account to get his money or request a transfer of funds to a bank account. PayPal is an example of a payment intermediary.

Agent-based methods of securing access to e-government services are discussed in Joshi, et al. (2001) as a solution to the publi-key infrastructure open standard with interoperable and flexible authentication for various services. This approach has begun appearing in the literature as it addresses the issue of security in a heterogeneous environment.

Role-Based Access Control (RBAC) models appear to be the most attractive solution for providing security features in multidomain e-government infrastructure. RBAC features such as policy neutrality, principle of least privilege, and ease of management make them especially suitable candidates for ensuring safety in e-government environment.

Identifying the users of e-government services is an important task which can enable signing of important documents online as well as personalization of e-government portal on which e-services are available. Today's most used way of identifying users is by digital

11 Anonymizer.com, 2016. Anonymizer - Anonymous Proxy, Anonymous Surfing & Anti Spyware. [Online] Available at: http://www.anonymizer.com [Accessed 2016].
12 Federrath, H., 2016. JAP — Anonymity & Privacy. [Online] Available at: http://anon.inf.tu-dresden.de/index_en.html [Accessed 2016].
13 PayPal, 2016. Privacy - PayPal. [Online] Available at: https://www.paypal.com/rs/webapps/mpp/paypal-safety-and-security [Accessed 2016].

certificates as one of the most secure ways which can prove identity of user online. These certificates are interoperable and can be utilized for many other purposes. Certificates are enabled by Public Key Infrastructure (PKI). The PKI is responsible for operating infrastructure services such as registration, key generation and certification for both citizens and business who participate in the secure environment. PKI fulfils the requirements on authentication of users, non-repudiation of user identity, protection from abuse of any participant by another and several legal constraints satisfying in that manner the majority of e-government security.

Encryption of communication between e-government service and its users is also an important task. Freedom software solution (https://freedom.to) that is based on at least three TCP/IP relays combined with strong encryption may be used for this purpose. Because the TCP/IP is used by every service on the Internet as a part of infrastructure who actually enables it, every service thereby can be encrypted and anonymized. They keep no logbook in such a way that even two relays put together are unable to trace back the information asked or retrieved. This is particularly important for preventing middle-attack and listening of the traffic between e-service and user computer.

While communicating with e-government platform, users via their browsers exchange different types of data, which can be privacy-sensitive. As we said in previous paragraph, encryption of data and communication solves this problem. But, we must keep in mind that some sensitive information is often stored in HTTP cookie files, which is passed openly over the Internet[14]. These cookie files are a very powerful technology for enhancing interactivity on the web which can be misused in ways that present an abuse of personal privacy. Disabling HTTP cookie files can be a remedy. There are also tools who can enable selective acceptance of cookie files that are stored on a user's computer in order to prevent damage and misusing of these files.

To demonstrate that privacy-enhancing technologies are secure software solution to protect privacy of citizens and business when they are dealing with e-government and e-commerce services the Privacy Incorporated Software Agent (PISA)[15] project was carried out. The key actions of PISA are: to develop and validate novel, scalable and interoperable technologies, mechanisms and architectures for trust and security in organizations and infrastructures and to scale up, integrate, validate and demonstrate trustful and confident privacy-enhancing technologies for e-services and everyday life.

THE APPLICATION OF MACHINE LEARNING E-TECHNOLOGIES IN E-GOVERNMENT

Nowadays there are many applications of machine learning and data mining techniques in e-technologies government tasks and domains: e-marketing, e-banking, e-learning, e-health, e-agriculture, etc.

14 Seničar, V., Jerman-Blažič, B. & Klobučar, T., 2003. Privacy-Enhancing Technologies - approaches and development. Computer Standards & Interfaces , XXV(2), pp. 147-158.
15 PISA, 2000. Building a privacy guardian for the electronic age. [Online] Available at: http://www.tno.nl/instit/fel/pisa [Accessed 2016].

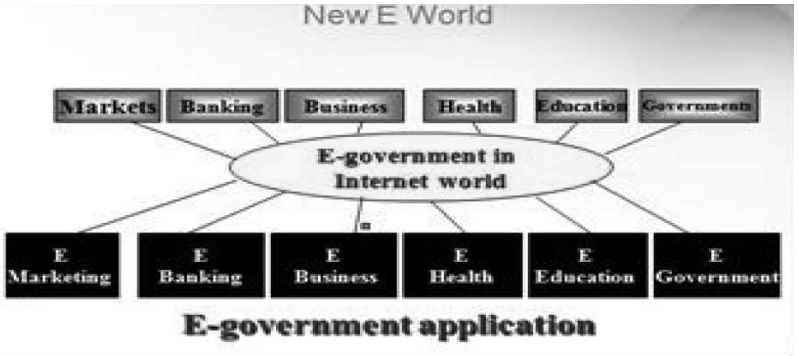


Figure 1: *E-government applications*[16]

The security in e-government system is the problem that can be related with intrusion detection[17] [18] [19] [20] [21]. The main point is to identify the users that are using e-government system without authorization. They are showing up in the form of cyber attackers, illegal access, and the use of malicious code that causes loss of individual data, denial of service, invasion of privacy and other. The behaviour of government users in the past may be viewed through the system and also analysed by different methods in order to identify illegal users. Regular users perform characteristic behaviours that are sequential and reproducible. Illegal users have anomalous behaviour as a result of emulation of regular user's actions [22].

Machine learning techniques may be used to analyse the data which is massive and complex, and their focus is on relevant information in a large quantity of data. It was reported in previous research that for the purposes of security analysis machine learning techniques may be employed, such as decision trees, information theory[23], neural networks[24], support vector machines[25], genetic algorithms[26] and artificial immune systems[27] for choosing relevant features and elimination of irrelevant features in the analysed data. Machine learning can be

16 Hanaa, M.S., Hamdy, M., Gohary E.R. & Salem M.A., 2015. Machine learning in E- Technologies. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol.4 (2), pp. 6-20.
17 Anderson, J. P., 1980. Computer security threat monitoring and surveillance, Fort Washington: James P. Anderson Company.
18 Mukherjee, B., Heberlein, L. T. & Levitt, K. N., 1994. Network intrusion detection. Network, VIII(3), pp. 26-41.
19 Blum, A. L. & Langley, P., 1997. Selection of relevant features and examples in machine learning. Artificial intelligence, XCVII(1), pp. 245-271.
20 Maheshkumar, S. & Serpen, G., 2003. Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context.. Nevada, CSREA Press, pp. 209-215.
21 Zander, S., Nguyen, T. & Armitage, G., 2005. Automated traffic classification and application identification using machine learning. Sydney, IEEE, pp. 250-257.
22 Terran, L. & Brodley, C. E., 1997. Detecting the abnormal: Machine learning in computer security, Purdue: ECE Technical Reports.
23 Lee, W. & Dong, X., 2001. Information-theoretic measures for anomaly detection. Oakland, IEEE, pp. 130-143.
24 Zhang, Z., Manikopoulos, C. N., Jorgenson, J. & Ucles, J., 2001. HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification. West Point, IEEE, pp. 85-90.
25 Wenjie, H., Liao, Y. & Vemuri, V. R., 2003. Robust anomaly detection using support vector machines. San Francisco, Proceedings of the international conference on machine learning, pp. 282-289.
26 Sinclair, C., Lyn, P. & Sara, M., 1999. An application of machine learning to network intrusion detection. Phoenix, Proceedings of the 15th Annual IEEE conference, pp. 371-377.
27 Hofmey, S. A., 1999. An immunological model of distributed detection and its application to computer security. New Mexico: PhD thesis, Department of Computer Sciences, University of New Mexico.

used to learn user profiles and to detect anomalous behaviour. E-government system may capture user profiles (user IDs, login times, login areas, login frequency, and login window size) in log file. According to the above literature, the following algorithm can be applied for detecting abnormal behaviour of users in e-government system:

1. Keep data of legitimate users in the log files in the past (such as user IDs, login times, login areas, login frequency, login window size) in the e-government system,
2. Receive the user data from user log file in e-government system,
3. Make the preparatory work on the user data,
4. Transform the data set into the appropriate format for machine learning and transmit it as input to appropriate software for analysis,
5. Analyse the data set by selected algorithms,
6. Are there misleading and inconsistent samples?
7. If the answer is *False*. go to 4,
8. If the answer is *True*, go to 6
9. Make learn and test analysis by classifier algorithms,
10. In the results of analysis determine the algorithms that give the best score values of the best learn and the best test,
11. For the most successful classifiers and for each legitimate user status, list and compare status of the legitimate user that enters the top legitimate user class and receives a set of the common intersections,
12. Take input status of the new user and compare with the previous learning results

- Is there conformity?
- If the answer is true, allow access to the system,
- If the answer is false, not allow access to the system and report to legitimate user.

STATE-OF-THE-ART IN SECURING E-GOVERNMENT

The EU GUIDES project was aimed to develop a set of guidelines at a European level for assessing the compliance of Internet-based data processing technologies to the EU Data Protection Directive (95/46/EC) —DPD. Use case study analysis of typical web information processing systems in the area of government, health and e-commerce was conducted to characterize the Internet-based data handling practices, particularly those pertinent to personal data. Its set of guidelines is advisory only. Also, the European Commission issued Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications addressing users, service providers, institutions, business, commerce, etc.

Zhao & Zhao, (2010) conducted the study[28] on assessing the U.S. state e-government sites in terms of privacy and security policies, policy implementation, and network vulnerability to cyber attacks. The data for the study were collected by web content analysis, information security auditing, and computer network security mapping. They found that privacy policy and security policy were posted on most of the e-government portals, where security measures are in place so that information will not be lost, misused or altered. Implementation of key security measures such as username and password authentication, SSL encryption, internet traffic monitoring, intrusion detection, investigation of improper activities and proper use

28 Zhao, J. J. & Zhao, S. Y., 2010. Opportunities and threats: A security assessment of state e-government websites. Government Information Quarterly, XXVII(1), pp. 49-56.

and anti-hacking statements leads to secure environment in e-government domain, along with cooperation of e-government security administrators with opportunities to learn from one another for continuously improving their e-government security.

Some e-government portals require identification of users by their logging in with username and password, and special attention should be paid to the protection from the XSS (Cross Site Scripting) and SQL injection attacks. This types of attacks in most cases cause crashes of e-government service and destroying of data. To prevent this security incidents, validation of user input is recommended, as for example, SQL injection can potentially give attacker the possibility to manipulate government database, increasing the risks of malicious data mining, identity theft and compromising the integrity of the databases[29]. As valuable data passes through the web interfaces of e-government services, these interfaces make the web a logical point of attack. One possible solution to this problem can be the existence of Single Sign-On (SSO) point on central e-government portals. In that situation, central e-government platform should undertake authentication of the users and return back the appropriate information. With SSO, authorization and privilege level of users also can be determined and propagated through different e-government services, increasing the level of security in the whole system and helping both citizens and data owners in making the process of data access simple, smooth and fast. A survey conducted by Briney & Frank (2002) showed that most information security problem[30] were caused by the negligence of people, rather by attack events. Therefore, it is important that people who manage the e-services are skilled to develop the secure environment for using of those services as well as to train and educate people who maintain them in order to keep an adequate level of security during the use of e-services. Managing the people in the context of information security assurance management requires the use of socio-technical approach to focusing on these issues[31]. Socio-technical security aspects related to e-government services may result from the lack of ethical and cultural norms, legal and contractual documents, administrative and managerial policies, operational and procedural guidelines, and/or awareness program. It must be kept in mind, that socio-technical security aspects are context specific, especially from citizen's point of view, because citizen's behaviour differs from country to country. Vroom & Von Solms, (2004)[32] asserted that the compliance with information security policies can be improved if employees integrate information security mechanisms in their daily work practicies.

In the context of utilization of e-government services by citizens, it is important to consider the quality of these services from the citizen's point of view, as their quality surely influences their security. The process of creating of secure environment for exposing government e-services to its citizen's requires the participation of citizens in assessing the quality of those e-services. This assessment includes collecting of citizen opinions on their experience, satisfaction and trust while using e-government services, as this feedback is relevant source of information for governments to improve e-services. Here we can notice mutual relation between terms such as security, quality, trust and satisfaction, which has been already verified in literature[33] [34].

29 Moen, V., Klingsheim, A., Fagerland Simonsen, K. I. & Jørgen Hole, K., 2007. Vulnerabilities in e-governments. International Journal of Electronic Security and Digital Forensics, I(1), pp. 89-100.
30 Briney, A. & Frank, P., 2002. Does Size Matter. Information Security, V(9), pp. 36-39.
31 Ihmouda, R., Mohd Alwi, N. H. & Abdullah, I., 2014. A Systematic Review on E-government Security Aspects. International Journal of Enhanced Research in Management & Computer Applications, III(6), pp. 60-67.
32 Vroom, C. & Von Solms, R., 2004. Towards information security behavioural compliance. Computers & Security, XXIII(3), pp. 191-198.
33 Welch, E. W., Hinnant, C. C. & Moon, M. J., 2004. Linking Citizen Satisfaction with E-Government and Trust in Government. Journal of Public Administration Research and Theory, XV(3), pp. 371-391.
34 Tan, C.-W., Benbasat, I. & Cenfetelli, R. T., 2008. Building Citizen Trust towards e-Government

CONCLUSION

Delivering of government e-services requires careful consideration of all aspects involved in that process, especially from security point of view. Security of e-services is extremely important for the users (citizens and business) as security creates safe environment for the consumption of those e-services. In the previous paragraphs we tried to explain these aspects and to point out the relevance of secure access to e-government services. This creates trust in government, because the opinions of citizens and business help government in improvement of its e-services and maintaining the level of confidence towards foundation of a successful e-government initiative.

Also, e-government should monitor the situation in the field of security as ICT technologies are rapidly developing and growing up. One example may be the application of biometric identification of users of e-government services as a way of unique authentication and authorization. Today's approaches based on citizen identification numbers, business tax identification number, usernames and passwords, personal certificates are subjected to theft and unauthorized use which can cause damage to their owners. Biometric identification helps in overcoming this situation as a method which guaranties that the user is a person who claim that he is. Progress of the ICT technologies is also followed up by cyber attackers who always find novel methods for provoking damage and crash of services and theft of the data related to citizens and business. Prevention and rejection of those attacks can be done by applying security patches in software, improvements of legal acts that regulate this environment, education of citizens and business how to safely use offered e-services and not less important the education of people who work in the background and maintain the infrastructure used to provide government e-services.

REFERENCES

1. Anderson, J. P., 1980. *Computer security threat monitoring and surveillance,* Fort Washington: James P. Anderson Company.
2. Anonymizer.com, 2016. *Anonymizer - Anonymous Proxy, Anonymous Surfing & Anti Spyware.* [Online] Available at: http://www.anonymizer.com [Accessed 2016].
3. Bélanger, F. & Carter, L., 2008. Trust and risk in e-government adoption. *The Journal of Strategic Information Systems,* XVII(2), pp. 165-176.
4. Blum, A. L. & Langley, P., 1997. Selection of relevant features and examples in machine learning. *Artificial intelligence,* XCVII(1), pp. 245-271.
5. Briney, A. & Frank, P., 2002. Does Size Matter. *Information Security,* V(9), pp. 36-39.
6. Carter, L. & Bélanger, F., 2005. The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information systems journal ,* XV(1), pp. 5-25.
7. Federrath, H., 2016. *JAP — Anonymity & Privacy.* [Online] Available at: http://anon.inf.tu-dresden.de/index_en.html [Accessed 2016].
8. Hiller, J. S. & Bélanger, F., 2001. *Privacy Strategies for Electronic Government.* In M. Abramson & G. Means ed. New York: Rowman & Littlefield.
9. Hofmey, S. A., 1999. *An immunological model of distributed detection and its application to computer security.* New Mexico: PhD thesis, Department of Computer Sciences, University of New Mexico.
10. Hof, S., 2002. *Arguments for a Holistic and Open Approach to Secure e-Government.* France, First International Conference, EGOV 2002 Aix-en-Provence, pp. 464-467.
11. Ihmouda, R., Mohd Alwi, N. H. & Abdullah, I., 2014. A Systematic Review on E-government Security Aspects. *International Journal of Enhanced Research in Management & Computer Applications,* III(6), pp. 60-67.

Services: Do High Quality Websites Matter?. Hawaii, In Proceedings of 41st Hawaii International Conference on System Sciences, IEEE.

12. Joshi, J., Ghafoor, A., Aref, W. G. & Spafford, E. H., 2001. Digital Government Security Infrastructure Design Challenges. *Computer,* XXXIV(2), pp. 66-72.
13. Kaliontzoglou, A., Sklavos, P., Karantjias, T. & Polemi, D., 2005. A secure e-Government platform architecture for small to medium sized public organizations. *Electronic Commerce Research and Applications,* IV(2), pp. 174-186.
14. Lambrinoudakis, C., Gritzalis, S., Dridi, F. & Pernul, G., 2003. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer Communications,* XXVI(16), pp. 1873-18893.
15. Lee, W. & Dong, X., 2001. *Information-theoretic measures for anomaly detection.* Oakland, IEEE, pp. 130-143.
16. Maheshkumar, S. & Serpen, G., 2003. *Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context.*. Nevada, CSREA Press, pp. 209-215.
17. Medjahed, B., Rezgui, A., Bouguettaya, A. & Ouzzani, M., 2003. Infrastructure for E-Government Web Services. *Internet Computing, IEEE,* VII(1), pp. 58-65.
18. Moen, V., Klingsheim, A., Fagerland Simonsen, K. I. & Jørgen Hole, K., 2007. Vulnerabilities in e-governments. *International Journal of Electronic Security and Digital Forensics,* I(1), pp. 89-100.
19. Mukherjee, B., Heberlein, L. T. & Levitt, K. N., 1994. Network intrusion detection. *Network,* VIII(3), pp. 26-41.
20. PayPal, 2016. *Privacy - PayPal.* [Online] Available at: https://www.paypal.com/rs/webapps/mpp/paypal-safety-and-security [Accessed 2016].
21. PISA, 2000. *Building a privacy guardian for the electronic age.* [Online] Available at: http://www.tno.nl/instit/fel/pisa [Accessed 2016].
22. Hanaa, M.S., Hamdy, M., Gohary E.R. & Salem M.A., 2015. Intelligence Techniques for e-government applications. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* Vol.4 (2), pp. 6-20.
23. Seničar, V., Jerman-Blažič, B. & Klobučar, T., 2003. Privacy-Enhancing Technologies - approaches and development. *Computer Standards & Interfaces ,* XXV(2), pp. 147-158.
24. Sinclair, C., Lyn, P. & Sara, M., 1999. *An application of machine learning to network intrusion detection.* Phoenix, Proceedings of the 15th Annual IEEE conference, pp. 371-377.
25. Tan, C.-W., Benbasat, I. & Cenfetelli, R. T., 2008. *Building Citizen Trust towards e-Government Services: Do High Quality Websites Matter?.* Hawaii, In Proceedings of 41st Hawaii International Conference on System Sciences, IEEE.
26. Terran, L. & Brodley, C. E., 1997. *Detecting the abnormal: Machine learning in computer security,* Purdue: ECE Technical Reports.
27. Vroom, C. & Von Solms, R., 2004. Towards information security behavioural compliance. *Computers & Security,* XXIII(3), pp. 191-198.
28. Welch, E. W., Hinnant, C. C. & Moon, M. J., 2004. Linking Citizen Satisfaction with E-Government and Trust in Government. *Journal of Public Administration Research and Theory,* XV(3), pp. 371-391.
29. Wenjie, H., Liao, Y. & Vemuri, V. R., 2003. *Robust anomaly detection using support vector machines.* San Francisco, Proceedings of the international conference on machine learning, pp. 282-289.
30. Wimmer, M. & Von Bredow, B., 2002. *A holistic approach for providing security solutions in e-government.* Hawaii, Proceedings of the 35th Annual Hawaii International Conference on System Sciences, pp. 1715-1724.
31. Zander, S., Nguyen, T. & Armitage, G., 2005. *Automated traffic classification and application identification using machine learning.* Sydney, IEEE, pp. 250-257.
32. Zhang, Z., Manikopoulos, C. N., Jorgenson, J. & Ucles, J., 2001. *HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification.* West Point, IEEE, pp. 85-90.
33. Zhao, J. J. & Zhao, S. Y., 2010. Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly,* XXVII(1), pp. 49-56.

UDC: 004.056

CVSS IN FUNCTION OF IMPROVING IT SECURITY

Petar Čisar, PhD[1]
Academy for Criminalistic and Police Studies, Belgrade
Zoltan Rajnai, PhD
Obuda University, Donat Banki Faculty, Budapest

Abstract: The Common Vulnerability Scoring System (CVSS) represents an open structure for linking the characteristics and effects of IT vulnerabilities. The National Vulnerability Database (NVD) formulated particular scores for known vulnerabilities. Government institutions can utilize the Federal Information Processing Standards (FIPS) 199 security classifications with the NVD CVSS scores to acquire impact scores that are customized to concrete environment. CVSS is comprised of three components: base, temporal and environmental. Every component generates a number going from 0 to 10 and a textual form that defines the parameters used to determine the score (called vector). The base group describes the internal characteristics of a vulnerability. The temporal component refers to the attributes of a vulnerability that change after some time. The environmental component speaks to the attributes of a vulnerability that is remarkable to any client's environment. CVSS empowers IT experts, security and application vendors and scientists to all advantage by accepting this common approach of scoring IT vulnerabilities.

Keywords: vulnerability, scoring system, metrics, vectors

INTRODUCTION

This chapter describes the main approach to the Common Vulnerability Scoring System (CVSS) and is based on NIST Interagency Report 7435[2].

Different organizations (vendors, coordinators, researchers, users) from the sphere of security have different roles, motivations, priorities, resources etc. Nowadays, IT experts must recognize and evaluate vulnerabilities crosswise over numerous specific hardware and software configurations. They have to regulate these vulnerabilities and remediate those that represent the most serious danger. The key problem is, in a situation of enormous vulnerability data, to generate appropriate actionable information. The CVSS is a vendor-independent, industry standard that evaluates vulnerability severity and helps determine urgency and priority of reaction. It tackles the issue of various, contradictory scoring frameworks and is usable and understandable by anybody. CVSS is an open structure that addresses this issue. It offers several advantages:

- Standardization of scores: At the point when an organization standardizes vulnerability scores across all of its software and hardware platforms, it can influence a single vulnerability management strategy. This strategy may be like a service level agreement (SLA) that states how rapidly a specific vulnerability must be accepted and remediated.

1 E-mail: petar.cisar@kpa.edu.rs.
2 U.S. Department of Commerce, National Institute of Standards and Technology (NIST), NIST Interagency Report 7435, The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems

- Open framework: With CVSS, anybody can see the individual characteristics used to infer a score.

- Risk priority: At the point when the environmental score is calculated, the vulnerability gets to be relevant. That is, vulnerability scores are now illustrative of the real risk to a firm. Clients know how imperative a given vulnerability is in connection to different vulnerabilities.

It is important to emphasize that CVSS is not a threat scoring system, a vulnerability database (for example, NVD - the U.S. government collection of standards based vulnerability management data) or a real-time attack scoring system.

CVSS is made out of three metric groups: base, temporal and environmental, each comprising of a set of metrics, as shown in Figure 1.

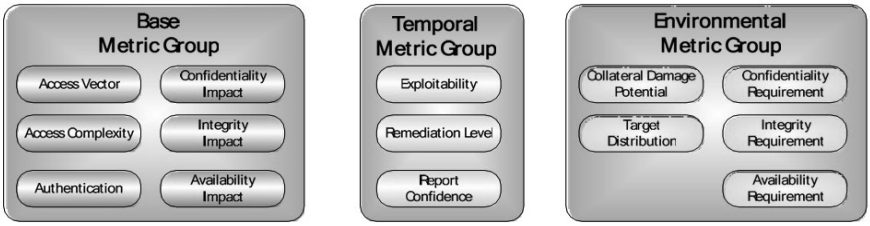


Figure 1: *CVSS Metric Groups (source: NIST Interagency Report 7435)*

The main difference between the groups is as follows:

Base - fundamental characteristics of a vulnerability that are constant over time and user environments.

Temporal - the characteristics of a vulnerability that change over time but not among user environments.

Environmental - the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

OTHER VULNERABILITY SCORING SYSTEMS

There are a number of other vulnerability scoring systems managed by commercial and non-commercial organizations. They each have their merits, but they differ by what they measure. For example, coordinator CERT/CC scoring produces a numeric value between 0 and 180 that assigns an approximate severity to the vulnerability. This number considers several factors, including[3]:

F1: Is information about the vulnerability widely available or known?

F2: Is the vulnerability being exploited in the incidents reported?

F3: Is the Internet infrastructure at risk because of this vulnerability?

F4: How many systems on the Internet are at risk from this vulnerability?

F5: What is the impact of exploiting the vulnerability?

F6: How easy is to exploit the vulnerability?

F7: What are the preconditions required to exploit the vulnerability?

The formula which is used in calculations: $3*(F1 + F2 + F3) * (F4 * F5 * F6 * F7) / 20^4$.

3 United States Computer Emergency Readiness Team (US-CERT). US-CERT Vulnerability Note Field Descriptions. 2006, http://www.kb.cert.org/vuls/html/fieldhelp.

The SANS vulnerability analysis scale considers whether the weakness is found in default configurations or client or server systems[4].

Vendor Microsoft's proprietary scoring system uses four rating categories[5]:

Table 1: *Microsoft's Vulnerability Rating*

Rating	Definition
Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity or availability of users data or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult or whose impact is minimal.

Researcher scoring: Secunia[6]

Table 2: *Secunia's Vulnerability Rating*

Rating	Definition
Extremely critical	Typically used for remotely exploitable vulnerabilities, which can lead to system compromise. Successful exploitation does not normally require any interaction and exploits are in the wild.
Highly critical	As above, no known exploits
Moderately critical	As above, but DoS only or requiring user interaction
Less critical	XSS, privilege escalation, sensitive data exposure
Not critical	Very limited privilege escalation, locally exploitable DoS, non – sensitive data exposure

THE WORKING PRINCIPLE OF CVSS

When the base metrics are assigned values, the base equation calculates a score ranging from 0 to 10, and creates a vector (Figure 2.). The vector, which has a form of text string that contains the values assigned to each metric, provides the "open" nature of the framework. It is used to communicate exactly how the score for each vulnerability is determined, with the goal that anybody can see how the score was calculated. In this way, the vector ought to be displayed with the vulnerability score.

4 SANS Institute. SANS Critical Vulnerability Analysis Archive, http://www.sans.org/newsletters/cva/.
5 Microsoft Corporation. Microsoft Security Response Center Security Bulletin Severity Rating System. November 2002, http://www.microsoft.com/technet/security/bulletin/rating.mspx.
6 https://www.first.org/cvss/cvss_basic-2.0.pdf

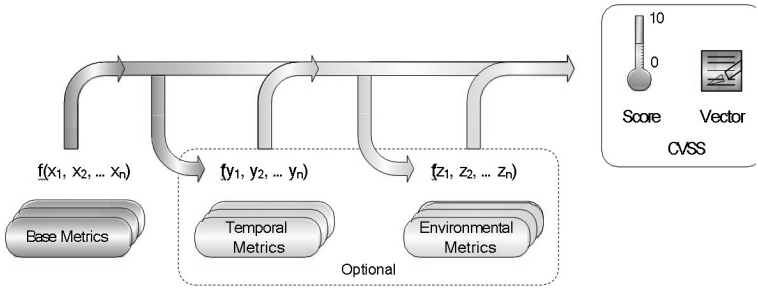


Figure 2: *CVSS Metrics and Equations (source: NIST Interagency Report 7435)*

Alternatively, the base score can be refined by assigning values to the temporal and environmental metrics. This is valuable so as to provide additional context for a vulnerability by more precisely describing the risk posed by the vulnerability to a user's environment. Depending on purpose, the base score and vector may be sufficient.

If a temporal score is required, the temporal equation will combine the temporal metrics with the base score to create a temporal score ranging from 0 to 10. Similarly, if an environmental score is required, the environmental equation will combine the environmental metrics with the temporal score to create an environmental score ranging from 0 to 10.

CVSS METRICS AND METRIC GROUPS

This section defines the metrics that comprise the CVSS version 2 and is based on (Schiffman M (2005)). These metrics are organized into three groups: base, temporal and environmental metrics.

Base Metrics

The base metric group captures the characteristics of a vulnerability that are constant with time and across user environments. The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. The three impact metrics measure how a vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability. For example, a vulnerability could cause a partial loss of integrity and availability, but no loss of confidentiality.

Access Vector (AV)

This metric reflects how the vulnerability is exploited. Measures whether a vulnerability is exploitable locally or remotely.

- Local: The vulnerability is only exploitable locally
- Remote: The vulnerability is exploitable remotely

The more remote an attacker can be to attack a host, the greater the vulnerability score.

Access Complexity (AC)

This metric measure the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. The lower the required complexity, the higher the vulnerability score.

- High - specialized access conditions exist
  - specific windows of time (a race condition)
  - specific circumstances (non-default configurations)
  - victim interaction (tainted e-mail attachment)
- Low - specialized access conditions or extenuating circumstances do not exist
- always exploitable

Authentication (AU)

This metric measures whether or not an attacker needs to be authenticated to the target system in order to exploit the vulnerability. The fewer authentication instances that are required, the higher the vulnerability score.

- Required: Authentication is required to access and exploit the vulnerability
- Not Required: Authentication is not required to access or exploit the vulnerability

Confidentiality Impact (C)

This metric measures the impact on confidentiality of a successful exploit of the vulnerability on the target system. Increased confidentiality impact increases the vulnerability score.

- None: No impact on confidentiality
- Partial: There is considerable informational disclosure
- Complete: A total compromise of critical system information

Integrity Impact (I)

This metric measures the impact on integrity of a successful exploit of the vulnerability on the target system. Increased integrity impact increases the vulnerability score.

- None: No impact on integrity
- Partial: Considerable breach in integrity
- Complete: A total compromise of system integrity

Availability Impact (A)

This metric measures the impact on Availability of a successful exploit of the vulnerability on the target system. Increased availability impact increases the vulnerability score.

- None: No impact on availability
- Partial: Considerable lag in or interruptions in resource availability
- Complete: Total shutdown of the affected resource

Temporal Metrics

This metrics describe time dependent qualities of a vulnerability (the threat posed by a vulnerability may change over time): exploitability, remediation status and report confidence. Since temporal metrics are optional they each include a metric value that has no effect on the score. This quality is utilized when the user feels the specific metric does not make a difference and wishes to bypass it.

Exploitability (E)

This metric measures how complex the process is to exploit the vulnerability in the target system once it has been accessed. The more easily a vulnerability can be exploited, the higher the vulnerability score.

- Unproven: No exploit code is yet available

- Proof of Concept: Proof of concept exploit code is available
- Functional: Functional exploit code is available
- High: Exploitable by functional mobile autonomous code or no exploit required (manual trigger)

Remediation Level (RL)

This metric measures the level of solution available. The less official and permanent a fix, the higher the vulnerability score is.

- Official Fix: Complete vendor solution available
- Temporary Fix: There is an official temporary fix available
- Workaround: There is an unofficial non-vendor solution available
- Unavailable: There is either no solution available or it is impossible to apply

Report Confidence (RC)

This metric measures the degree of confidence in the existence of the vulnerability and the credibility of its report. The urgency of a vulnerability is higher when a vulnerability is known to exist with certainty. The more a vulnerability is validated by the vendor or other reputable sources, the higher the score.

- Unconfirmed: A single unconfirmed source or possibly several conflicting reports
- Uncorroborated: Multiple non-official sources; possibly including independent security companies or research organizations
- Confirmed: Vendor has reported/confirmed a problem with its own product

Environmental Metrics

This metric is related to implementation and environment specific qualities of a vulnerability. Since environmental metrics are optional they each include a metric value that has no effect on the score. This quality is utilized when the user feels the specific metric does not make a difference and wishes to bypass it.

Collateral Damage Potential (CDP)

This metric measures the potential for a loss in physical equipment, property damage or loss of life or limb. Naturally, the greater the damage potential, the higher the vulnerability score.

- None: There is no potential for property damage.
- Low: A successful exploit of this vulnerability may result in light property damage or loss
- Medium: A successful exploit of this vulnerability may result in significant property damage or loss
- High: A successful exploit of this vulnerability may result in catastrophic property damage and loss

Target Distribution (TD)

This metric measures the relative size of the field of target systems susceptible to the vulnerability. The greater the proportion of vulnerable systems, the higher the score.

- None: No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting (0%)
- Low: Targets exist inside the environment, but on a small scale (1% - 15%)
- Medium: Targets exist inside the environment, but on a medium scale (16% - 49%)
- High: Targets exist inside the environment on a considerable scale (50% - 100%)

Base, Temporal, Environmental Vectors

Each metric in the vector consists of the abbreviated metric name, followed by a ":" (colon), then the abbreviated metric value. The vector lists these metrics in a predetermined order, using the "/" (slash) character to separate the metrics. If a temporal or environmental metric is not to be used, it is given a value of "ND" (not defined). The base, temporal, and environmental vectors are shown below in Table 3.

Table 3: *Base, Temporal and Environmental Vectors*

Metric Group	Vector
Base	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Temporal	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Environmental	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

For example, a vulnerability with base metric values of "Access Vector: Low, Access Complexity: Medium, Authentication: None, Confidentiality Impact: None, Integrity Impact: Partial, Availability Impact: Complete" would have the following base vector: "AV:L/AC:M/Au:N/C:N/I:P/A:C."

SCORING

Scoring is the process of combining metric values. It defines the equations used for base, temporal, and environmental score generation.

- Base score is the "foundation" - modified by temporal and environmental metrics
- Base and temporal scores are computed by vendors and coordinators with the intent of being published
- Environmental score is optionally computed by end-user /organization

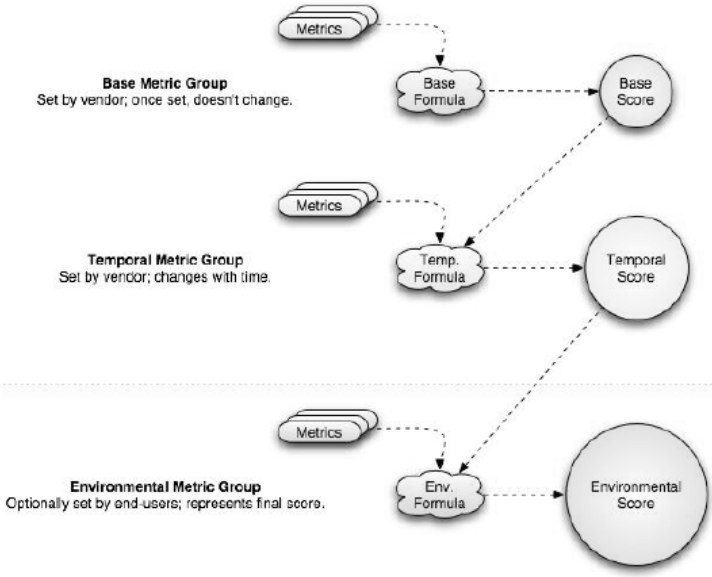


Figure 3: *CVSS – Scoring view*

Base Scoring

Base score is computed by vendors and coordinators. It combines innate characteristics of the vulnerability.The base score has the largest bearing on the final score - computed primarily from the Impact Metrics. Represents vulnerability severity.

The base equation is the foundation of CVSS scoring. The base equation is (NIST Interagency Report 7435):

Temporal Scoring

Temporal score is computed by vendors and coordinators. It modifies the base score. It allows for the introduction of mitigating factors to reduce the score of a vulnerability. It is designed to be re-evaluated at specific intervals as a vulnerability ages. It represents urgency at specific points in time. The temporal equation will produce a temporal score no higher than the base score, and no less than 33% lower than the base score. The temporal equation is (NIST Interagency Report 7435):

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))

Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))

Exploitability = 20* AccessVector*AccessComplexity*Authentication

f(impact)= 0 if Impact=0, 1.176 otherwise

AccessVector     = case AccessVector of
                        requires local access: 0.395
                        adjacent network accessible: 0.646
                        network accessible: 1.0

AccessComplexity = case AccessComplexity of
                        high: 0.35
                        medium: 0.61
                        low: 0.71

Authentication   = case Authentication of
                        requires multiple instances of authentication: 0.45
                        requires single instance of authentication: 0.56
                        requires no authentication: 0.704

ConfImpact       = case ConfidentialityImpact of
                        none:               0.0
                        partial:            0.275
                        complete:           0.660

IntegImpact      = case IntegrityImpact of
                        none:               0.0
                        partial:            0.275
                        complete:           0.660

AvailImpact      = case AvailabilityImpact of
                        none:               0.0
                        partial:            0.275
                        complete:           0.660
```

```
TemporalScore = round_to_1_decimal(BaseScore*Exploitability
                *RemediationLevel*ReportCon idence)

Exploitability    = case Exploitability of
                         unproven:              0.85
                         proof-of-concept:      0.9
                         functional:            0.95
                         high:                  1.00
                         not defined:           1.00

RemediationLevel = case RemediationLevel of
                         official-fix:          0.87
                         temporary-fix:         0.90
                         workaround:            0.95
                         unavailable:           1.00
                         not defined:           1.00

ReportConfidence = case ReportConfidence of
                         unconfirmed:           0.90
                         uncorroborated:        0.95
                         confirmed:             1.00
                         not defined:           1.00
```

Environmental Scoring

Environmental score is computed by end users. It adjusts combined base-temporal score and should be considered the final score. It represents a snapshot in time, tailored an environment. User organizations will use this to prioritize responses within their own environments. Environmental equation will produce a score no higher than the temporal score. The environmental equation is (NIST Interagency Report 7435):

```
EnvironmentalScore = round_to_1_decimal((AdjustedTemporal+
(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)

AdjustedTemporal = TemporalScore recomputed with the BaseScore's Impact sub-
equation replaced with the AdjustedImpact equation

AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)
                 *(1-AvailImpact*AvailReq)))
```

```
CollateralDamagePotential = case CollateralDama gePotential
                                 none:            of 0
                                 low:             0.1
                                 low-medium:      0.3
                                 medium-high:     0.4
                                 high:            0.5
                                 not defined:     0

TargetDistribution        = case TargetDistribu tion
                                 none:             of
                                 low:              0
                                 medium:           0.25
                                 high:             0.75
                                 not defined:      1.00
                                                   1.00
ConfReq          = case ConfReq of
                        low:              0.5
                        medium:           1.0
                        high:             1.51
                        not defined:      1.0

IntegReq         = case IntegReq of
                        low:              0.5
                        medium:           1.0
                        high:             1.51
                        not defined:      1.0

AvailReq         = case AvailReq of
                        low:              0.5
                        medium:           1.0
                        high:             1.51
                        not defined:      1.0
```

EXAMPLES

1. CVSS score distribution for all vulnerabilities[7]**:**

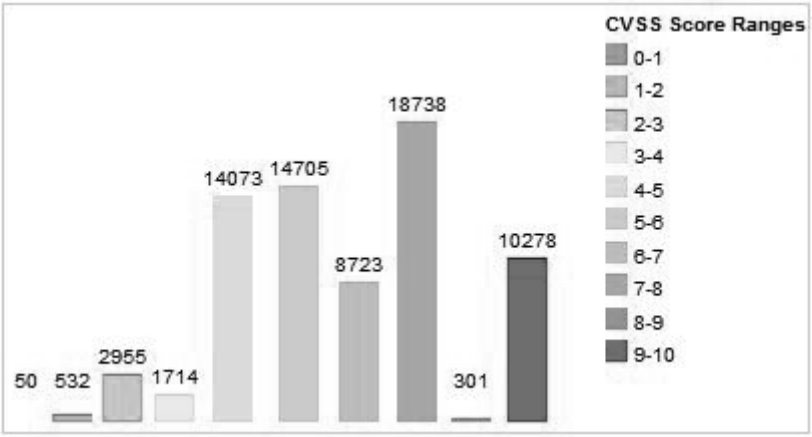


Figure 4: *Vulnerability distribution by CVSS score (source: CVE Details)*

2. Consider vulnerability CVE-2015-1337: Simple Streams does not properly verify the GPG (Gnu Privacy Guard) signatures of disk image files, which allows remote mirror servers to spoof disk images and have unspecified other impact via a 403 response.

The base vector for this vulnerability is[8]: AV:N/AC:M/Au:N/C:P/I:P/A:P.

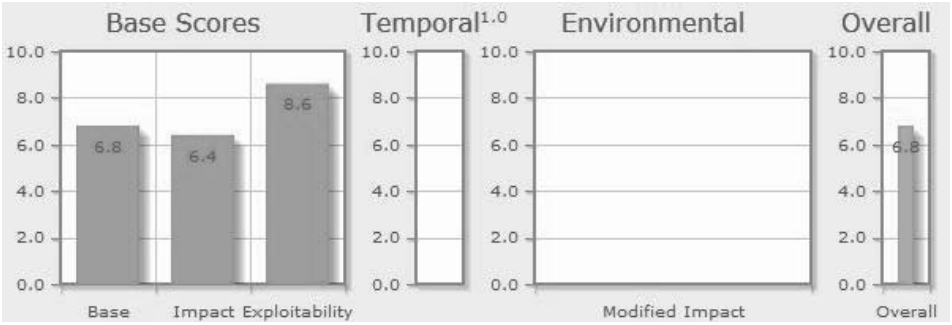


Figure 5: *Base scores and overall score for CVE-2015-1337*
(source: National Vulnerability Database)

CVSS version 3

CVSS v2 has been used by many organizations over the past years to rate vulnerabilities, but experts say this version has many faults and shortcomings. "While CVSSv2 saw improvements over CVSSv1, the scheme is still not adequately supporting real life usage, as it suffers from being too theoretical in certain aspects. Specific vulnerability types and vectors are not properly supported while others are not properly described, leading to subjective and incon-

7 CVE Details, https://www.cvedetails.com/cvss-score-distribution.php
8 National Vulnerability Database (NVD), https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1337

sistent scoring, which CVSS was designed to prevent." (Eiram C & Martin B (2013)).

On June 10, 2015, after three years in which it received input from the representatives of a broad range of industries, FIRST announced the availability of CVSS v3, which aims to provide a more robust and useful scoring system for vulnerabilities.[9]

The updated version includes enhancements such as: the promotion of consistency in scoring, the replacement of scoring tips in order to guide end users of CVSS more clearly, and consideration of the system in order to make it more applicable to modern concerns.[10]

Seth Hanford, co-chair of the FIRST CVSSv3 working group said "We hope that CVSS version 3 is clear, consistent and repeatable, and able to support the work of those who seek to understand, describe, compare, or evaluate IT vulnerabilities via a common scoring system."

CVSS v2.0 and v3.0[11]

The differences between two versions of CVSS are shown in the following table.

Table 4: *CVSS v.2 and v.3*

Version 2	Version 3
Vulnerabilities are scored relative to the overall impact to the host platform.	Vulnerabilities now scored relative to the impact to the impacted component.
No awareness of situations in which a vulnerability in one application impacted other applications on the same system.	A new metric, Scope, now accommodates vulnerabilities where the *thing suffering the impact* (the impacted component) is different from *the thing that is vulnerable* (the vulnerable component).
Access Vector may conflate attacks that require local system access and physical hardware attacks.	Local and Physical values are now separated in the Attack Vector metric.
In some cases, Access Complexity conflated system configuration and user interaction.	This metric has been separated into Attack Complexity (accounting for system complexity), and User Interaction (accounting for user involvement in a successful attack).
In practice, the Authentication metric scores were biased toward two of three possible outcomes, and not effectively capturing the intended aspect of a vulnerability.	A new metric, Privileges Required, replaces Authentication, and now reflects the greatest privileges required by an attacker, rather than the number of times the attacker must authenticate.
Impact metrics reflected percentage of impact caused to a vulnerable application.	Impact metric values now reflect the degree of impact, and are renamed to None, Low and High.
The Environmental metrics of Target Distribution and Collateral Damage potential were not found to be useful.	Target Distribution and Collateral Damage potential have been replaced with Mitigating Factors.
CVSS v2.0 could not accommodate scoring multiple vulnerabilities used in the same attack.	While not a formal metric, guidance on scoring multiple vulnerabilities is provided with Vulnerability Chaining.
No formal qualitative scoring guidelines were provided.	Numerical ranges have been mapped to a 5-point qualitative rating scale.

Several practical examples of numerical differences between version 2 and 3:[12]

9 SecurityWeek, FIRST Releases CVSS Version 3, http://www.securityweek.com/first-releases-cvss-version-3
10 FIRST, https://www.first.org/cvss
11 FIRST, https://www.first.org/cvss/user-guide
12 FIRST, https://www.first.org/cvss/examples

Table 5: *Examples of Numerical Differences Between CVSS v2 and v3*

Vulnerability	CVSS v2 Base Score	CVSS v3 Base Score
SSL/TLS MITM (CVE-2014-0224)	6.8	7.4
DokuWiki Reflected Cross-site Scripting Attack (CVE-2014-9253)	4.3	5.4
SearchBlox Cross-Site Request Forgery (CVE-2015-0970)	6.8	7.8
Apple iWork Denial of Service (CVE-2015-1098)	6.8	8.8

CONCLUSION

The Common Vulnerability Scoring System gives a standard technique to government institutions and different organizations to rate the seriousness of vulnerabilities inside of their frameworks. The National Vulnerability Database gives a standard set of approved scores. When implemented into security items, NVD and CVSS empower organizations to comprehend the vulnerabilities' effect on their environments. Besides, the effect evaluations will be the same notwithstanding when the vulnerabilities are detected by various security tools utilized as a part of different subjects. This empowers logical correlation of the seriousness of vulnerabilities between government frameworks, and even organizations. Viewing the scores of found vulnerabilities after some time can help in identifying security trends. In that case, with a successful security strategy, organizations will see upgradings in their vulnerability status over time.

REFERENCES

1. Schiffman M (2005). The Common Vulnerability Scoring System. *The RSA conference*. http://packetfactory.openwall.net/papers/CVSS/cvss-ppt.pdf
2. Eiram C & Martin B (2013). The CVSSv2 Shortcomings, Faults, and Failures Formulation, An Open Letter to FIRST, https://www.riskbasedsecurity.com/reports/CVSS-ShortcomingsFaultsandFailures.pdf
3. Chambers J & Thompson J (2004). Common Vulnerability Scoring System. Final Report and Recommendations by the Council. *National Infrastructure Advisory Council*. https://www.dhs.gov/sites/default/files/publications/niac-common-vulnerability-scoring-final-report-10-12-04-508.pdf
4. Frühwirth C & Männistö T (2009). Improving CVSS-based vulnerability prioritization and response with context information. *MetriSec09*. Helsinki University of Technology. http://www.securitymetrics.org/attachments/Metricon-4.5-Fruwirth-Improving-CVSS.pdf

UDC: 347.78:004
343.533::004

USING COMPUTER DEVICES TO INFRINGE COPYRIGHT AND RELATED RIGHTS - SOME CRIMINAL LAW ISSUES

Vladan Joldzic, PhD[1]
Institute for Criminological and Sociological Researches, Belgrade

Abstract: In actual time we are witnessing a growing variety of crimes including cyber crimes, as well as of crimes at earlier times committed in various ways but in actual time as well by computers and computer lines as instruments for crime assessments. For example, for the attacks on copyright and its holders. Aim of our text is to point at such problems, starting from the relevant elements of international law, being hierarchically the most important for the protection of copyright, and then moving to the adequate examples from the reality of Serbia and its legislature. In such effort we strongly use our explorative results from the General Project 47011 – Prevention of crimes and the other social deviations, especially project State reaction on criminality in developing and growth – highly technological and ecological, project we are working on more than five years.

Key words: copyright, computer instruments as devices for assessments of crimes.

INSTEAD OF INTRODUCTION – A RESEARCH APPROACH TO DEFINING THE TOPIC

Crime is a historical, this means developmental phenomenon, observed by:

1. Dimension,

2. Affected region(s) and, of course,

3. Forms of expression. To be precise:

1. Expressions of the logical beings of socially negative acts, from such a reason

2. Unwanted and dangerous,

2. Proscribed, clearly incriminated and sanctioned forms of events.

We remind you that constant development of reality at the same time produces:

- New forms of crimes as the elements of specific mosaic as well as
- New logical beings of offences as building components of such mosaics.

Some of such phenomena need special precaution and/or object of action, but very often also acts of execution, and in some situations specific performers too. This is the main reason why modern states in actual time, parallel to the classical crimes, incriminate and treat some forms of offences unknown only a century or even a few decades ago. Good examples are:

1. Financial criminality in actual time mostly immanent at the field of financial potentials[2],

1 vladanj@EUnet.rs

2 See, for example: 1. George Robb (2002): *White-Collar Crime in Modern England: Financial Fraud and Business Morality*, Cambridge University Press, Cambridge, UK. 2. Laura L. Hansen, (2009): Corporate financial crime: social diagnosis and treatment, *Journal of Financial Crime*, Vol. 16, Iss: 1, pp. 28 – 40, and 3. Petter Gottschalk (2010): Categories of financial crime, *Journal of Financial Crime*, Vol. 17, Iss: 4, pp. 441 – 458.

2. Crimes that attack postal systems, infrastructures and users[3], as well as

3. Computer crimes[4].

In the last few decades we are the witnesses of more and more registered computer crimes expressed at many different ways. Some forms of computer crimes unknown, or not adequately known to public and professions, are hidden in such multitude. Among them are forms of crimes that attack the copyright and related rights, which means their holders too. The task that we have formulated and took upon us to fulfill is to present to you some of our research results, which means some knowledge acquired about the mentioned matter through the synoptic text, presented. In the first place:

What is really protected (which right), as well as

Who is attacked, and

Who can be a possible perpetrator of such crime:

- Physical entity (person), or
- Artificial entity (machine)?

Of course, we form our deliberation with the strong use of the science of law methods[5], starting from the formally normative and normative hierarchical methods[6], *in principio* in our research work:

1. Beginning our deliberation by analyzing the international law elements, then

2. Analyzing the European Union legislature,

3. Working our way from the more general toward narrower segments, also defined by the space and time,

4. Analyzing, finally, the elements of the legislature of Republic of Serbia.

Such approach is understandable and acceptable for the simple reason that Criminal law and legislature do not define what the copyright is and to what extent it is regulated. Answers at those questions have been defined by special parts of law science and legislature:

1. Copyright law, and

2. Copyright legislature, hierarchically formed, at such a way that possess its principles and norms, norms mostly of complex structure connected with the precisely defined parts of special annexes that completed logical beings of observed norms. To say at another word, such annexes have been and are needed to form, in any real case, a complete picture as well as correct conclusion: Is it what we see as being a copyright crime act - infringement of protected copyright (or related rights) or is not being such an act?

---

3 See, for example: 1. A Law Enforcement Guide to Postal Crimes (June 2004). Publication 146. *US Postal Inspection Service, National Headquarters*, Washington, USA, and *2. U.S. Postal Inspection Service - A Guide for the U.S. Congress* (*Publication 278*) (February 2008), United States Postal Inspection Service, Washington, USA.

4 See, for example: 1. Moore, R. (2005): *Cyber crime: Investigating High-Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing, 2. Joldžić Vladan (2007.): Kompjuterski kao deo elektronskog kriminaliteta – neka razmišljanja, *Pravni život*, br. 10, Tom 2, Beograd, Srbija, str.: 165.-174, 3. Stefan Fafinski (2008): *UK Cybercrime Report*, Publisher: 1871 Ltd, UK, 4. David S. Wall (June, 2008): *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge, UK, and 5.Rizgar Mohammed Kadir (2010): The Scope and the Nature of Computer Crimes Statutes A Critical Comparative Study, *German Law Journal*, Vol. 11, No 6, pp. 609. - 632.

5 Joldžić Vladan (2008): *Ekološka politika. Od ideje do izgradnje međunarodnog ekološkog prava*, Chapter 7: Metodi potrebni za celovito sagledavanje ekološko-pravnog odnosa kao predmeta naučnog izučavanja i praktičkog tretmana, publisher: Institute for Criminological and Sociological Researches, Belgrade, pp.: 39. – 61.

6 Joldzic Vladan: Chapter: 3.2. Methods of Law Sciences, from the book: *Ecology law - general part. Or on the Elements necessary for the establishing and existing of the Independent Law Discipline* (*Personal Observations*), Publisher: *Revista Mestrado em Direito*, Osasco, Brasil, Ano 9, n. 1, pp. 156-158.

Our approach leads us to observe many possible and present elements of valid laws and sub-law acts as material-formal base for logical being (or beings) forming in any concrete case, between them also in cases treated by our research of cyber crime. Such scientific approach guides us through three phases of researching:

1. Throughout the previously expressed phase of the research theme defining,

2. Logical phase of the substantial elements of copyright defining, elements needed as formal and material base for our research, and

3. Phase of analyzing elements needed for the approach to copyright and related rights protection by the criminal law and the actual legislatures, having in mind that criminal laws hold in estimation mentioned formal and material base for such criminal acts forming and threatening.

We form our analysis, and present it to you, not only on the base of specific knowledge but also by using adequate practical examples, having in mind that law is not only a logical but also practical discipline, the discipline of science and legislatures that is valid in the measure in which it is really included in reality; the measure that is at this moment, not only in Republic of Serbia, in the elementary process of developing and applying.

ABOUT THE CRUCIAL ELEMENTS OF THE COPYRIGHT AND RELATED RIGHTS ESTABLISHMENT

Regulating the authors' copyright as well as the related rights, had been initialized, more than a hundred years ago, at the level of International law, by the Berne Convention for the Protection of Literary and Artistic Works[7], but latter appearance of new types of media brought on demands for:

1. The Berne Convention updating, and

2. Forming of a number of new regulative texts:

1.1. starting with the Universal Copyright Convention[8], through

1.2. Convention Establishing the World Intellectual Property Organization[9],

1.3. Followed at the domestic terrain by the Act of Ratification[10], to the

1.4. Convention on the Use of Electronic Communications in International Contracts[11].

The elements of the European Union legislation connected with the mentioned problems and themes are also of utmost importance for Republic of Serbia. This, for the simple reason of the current process of aligning with the European Union.

---

7 Berne Convention for the Protection of Literary and Artistic Works, of September 9th, 1886, completed at Paris on May 4th, 1896, revised at Berlin on November 13th, 1908, completed at Berne on March 20th, 1914, revised at Rome on June 2nd, 1928, at Brussels on June 26th, 1948, at Stockholm on July 14th, 1967, and at Paris on July 24th, 1971, and amended on September 28th, 1979.

8 Universal Copyright Convention, Signed at Geneva on 6th September 1952, United Nations - Treaty Series, No 2937, Year 1955.

9 Convention Establishing the World Intellectual Property Organization, Signed at Stockholm on July 14, 1967 and as amended on September 28, 1979.

10 Uredba o ratifikaciji Konvencije o osnivanju Svetske organizacije za intelektualnu svojinu, *Službeni list SFRJ - Međunarodni ugovori i drugi sporazumi*", br.: 31/1972, and *Službeni list SFRJ - Međunarodni ugovori*, br. 4/1986, - dr. uredba.

11 Convention on the Use of Electronic Communications in International Contracts, United Nations, General Assembly, New York, 23 11 2005. *United Nations Publication Sales*, No.: E.07.V.2. ISBN: 978-92-1-133756-3.

All the mentioned documents can be observed as specific links of chain that string one after the other refilling the field of copyright regulating and protection. Although most of the mentioned legal documents have not been formulated in digital era all are adequately applicable at the intellectual products of authors formed either by:

1. A computer, or

2. For the computer using,threatening the right of the author as the exclusive right to authorize the products of their intellectual work, at the state as well at the international level, also identifying such products as the enterprise products the author can commercially place at the market, or to say it in another way, to profit by such intellectual products.

Starting from the conventions listed in our text the European Union has been developing (for a long time) stratified elements of legislature:

1. As the EU legal acts that regulate many issues connected with the copyright, and, of course,

2. Through the process of establishing the copyright protection by the adequate elements of criminal law and legislature of EU Member States.

European Union bases such process on the Article 288 of the Treaty on the Functioning of the European Union[12], formulating more than 10 directives over time by which the EU specifies a number of requirements and obligations for the Member States to develop and mutually synchronize adequate formal elements of their legislatures, necessary for the copyright and related rights protection. Such documents have to be analyzed relative to their form as well as chronologically.

It the presented text the starting point of our analyze belongs to the EU Council Directive on the legal protection of computer programs,[13] by which legal act have been established imposing an obligation upon the Member States to create and start an efficient legal protection of the computer programs as intellectual products. This goal and purpose can be seen at the beginning of the text (passage 16) where it is clearly said that this Directive also treats interconnections and interoperability aimed for exchange of the computer programs (which also includes: ways, resources and facilities of stratified marketing and sale), programs available for the rental use for a limited period of time and for profit-making purposes[14]. States have the obligation (regulated by Article 1, Section 1, Subsection 1) to protect all kinds of computer programs as the written works in accordance with the Berne Convention for the Protection of Literary and Artistic Works, including all the preparatory materials and products. Also that "programs" have to be protected as the intellectual creation of the author[15]. Of course, author can be: a.) natural person, or b.) legal person. Legal protection of the intellectual products has to be established "under national copyright legislation as applied to literary works[16]". Moreover, by the Directive 91/250 also have been established obligations for the special protection[17]; to be precise:

1. EU Member States are obliged to provide, in accordance with their national legislation, appropriate remedies against a person committing:

(a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;

12 See: Consolidated versions of the Treaty on European Union, *Official Journal of the European Union*, C 326, 26/10/2012, pp. 13-47, and The Treaty on the Functioning of the European Union, *Official Journal of the European Union*, C 326, 26/10/2012, pp. 47-201.
13 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal of the European Union*, L, 122, 17/05/1991, pp. 0042 – 0046.
14 See passage 20th of the introductory part of the Directive 91/250/EEC.
15 Directive 91/250/EEC, Article 1, Paragraph 1, point 3.
16 Directive 91/250/EEC, Article 3.
17 By the Article 7 of the Directive 91/250/EEC.

(b) the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;

(c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.

2. Any infringing copy of a computer program shall be liable to seizure in accordance with the legislation of the Member State concerned.

3. Member States may provide (legal ways, comm. V.J.) for the seizure of any means referred to in paragraph 1 (c).

In the year 1993, the Directive 93/98 is established that obliges Member States of the European Union to harmonize the term of protection of copyright and certain related rights by appropriate legal acts[18]. This Directive, alluding at Article 2 of the Berne Convention for the Protection of Literary and Artistic Works, obliges Member States (by Article 1, Section 1) to protect the rights of authors through their life and 70 years after their death! Also, to form such legal protection uniformly from state to state as well as to enable this protection at the territory of third states[19].

In the year 1996, Parliament and the Council of the European Union bring on the Directive 96/9/EC on the legal protection of databases[20], starting from the fact that such protection had not been uniform, to establish uniform an qualitative protection of the rights of all the kinds of databases and services based on them[21], indeed intellectual products[22], products that go to marketing through the on-line way, which means also by the internet. Text precisely defines that non-authorized extracting or applying of intellectual products produce "can have serious economic and technical consequences[23]", which, of course, also means financial and other damages for the authors! Introductory part of this Directive clearly accentuate that the protection is established for the various forms of the intellectual products, between them also all the electronically, electromagnetically or electro-optically produced or stored[24], and that the selection or the arrangement of the contents of such database is the author's own intellectual creation, legally protected[25], protected at a such a way that:

- anyone can individually access to it[26], but not to change anything into the product, which also means not to change esthetically or in quality, a

- only the author possesses the right to approve using of his product or not to approve[27].

The introductory part of the Directive 96/9/EC [under (22)] emphasizes that "electronic databases within the meaning of this Directive may also include devices such as CD-ROM and CD. It is clearly defined that it is only the right of the author:

To determine:

a) The way in which his work is exploited, and

b) By whom his work can be exploited[28],

18 Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, *Official Journal of the European Union*, L 290 , 24/11/1993, pp. 0009 – 0013.
19 Directive 93/98, Article 7 – Protection vis-à-vis third countries.
20 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *Official Journal of the European Communities*, No L 77/20 EN.
21 Introductory part of Directive 96/9/EC, under (2).
22 Introductory part of Directive 96/9/EC, under (4).
23 Introductory part of Directive 96/9/EC, under (8).
24 Introductory part of Directive 96/9/EC, under (13).
25 Introductory part of Directive 96/9/EC, under (15).
26 Introductory part of Directive 96/9/EC, under (17).
27 Introductory part of Directive 96/9/EC, under (18).
28 Introductory part of Directive 96/9/EC, under (30).

1. To control the distribution of his work to unauthorized persons[29], and

2. To prevent "the unauthorized extraction and/or re-utilization of all or a substantial part of the contents of that database[30]"

3. To prevent unauthorized extraction and/or re-utilization by the user which go beyond his legitimate rights, whereas the right to prohibit extraction and/or re-utilization of all or a substantial part of the contents relates not only to the manufacture of a parasitical competing product but also to any user[31],

4. To determine the relationship toward the right on transmission of product by a line or lines[32].

The Directive 96/9/EC on the legal protection of databases, starting from the elements of introductory part of text, establishes the protection for databases expressed:

- In any form (Article 1, Paragraph 1), and

- "As independent works… arranged in a systematic or methodical way and individually accessible by electronic or other means (Article 1, Paragraph 2)".

Moreover this text obliges EU Member States to provide support to the:

1. Legal protection of such products [Article 2, under (a)],

2. Rental and other rights related to copyright in the field of intellectual property [Article 2, under (b)], and

3. Term of protection of copyright and certain related rights [Article 2, under (c)].

Directive 96/9 also obliged EU Member States to protect intellectual products by copyright (Article 3). Directive clearly that only the author possesses the right:

1. To authorize his work (Article 5, Paragraph 1), and

2. Authorize the "temporary or permanent reproduction by any means and in any form, in whole or in part [Article 5, Paragraph 1, under (a)],

3. To translate or arrange his product [Article 5, Paragraph 1, under (b)],

4. "On any form of distribution to the public of the database or of copies thereof. The first sale in the Community of a copy of the database by the right holder, or with his consent, shall exhaust the right to control resale of that copy within the Community [Article 5, Paragraph 1, under (c)]", and

5. To display or performance to the public [Article 5, Paragraph 1, under (d)],

6. On "any reproduction, distribution, communication, display or performance to the public of the results of the acts referred to in (b)".

The state has the obligation to protect all the mentioned rights from the day of completion of the observed intellectual product. Protection shall expire fifteen years from the first of January of the year following the date of completion[33], if the product has not been, in the meantime, modified by the author. If the product was modified the period of 15 years has to be applied again. Such long time protection also provided by the Directive 2006/116 on the term of protection of copyright and certain related rights (codified version)[34], as well as by the Directive from the year 2011, that amended it[35].

29 Also Introductory part of the Directive 96/9/EC, under (30).
30 Introductory part of Directive 96/9/EC, under (41).
31 Introductory part of Directive 96/9/EC, under (42).
32 Introductory part of Directive 96/9/EC, under (43).
33 See: Directive 96/9/EC, Article 10, Paragraphs: 1 and 3.
34 Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version), *Official Journal of the European Communities,* L 372, 27.12.2006, pp. 12–18.
35 Directive 2011/77/EU of the European Parliament and of the Council of 27 September 2011 amending

In the year 2001, the Directive 2001/29 is passed on the harmonization of certain aspects of copyright and related rights in the information society.[36] This may be the most important document for the topic of our work. It is the text that regulates in detail some issues treated in previous documents, at the same time changing a number of their elements[37]. Directive 2001/29/EC:

1. Obliges the states to provide the legal protection of copyright an related rights, with particular emphasis on the information society (Art. 1, under 1),

2. Regulates protection of:

a) computer programs [Art. 1., paragraph 2, under (a)],

b) rental and rights related to copyright in the field of intellectual property [Art. 1, paragraph 2, under (b)],

c) copyright and related rights applicable to broadcasting [Art. 1, paragraph 2, under (c)],

d) the legal protection of databases [Art. 1, Paragraph 2, under (e)],

1. Obliges the states (by the Article 3, Paragraph 1, Point 1) to:

- protect the right of the authors to authorize their products, or

- protect the right of the authors to prohibit any communication to the public of their works,

- provide protection to author to approve or prohibit access to his intellectual product from any, including public, place,

2. Prescribes that author can "authorize or prohibit any form of distribution to the public by sale or otherwise (Article 4 - Distribution right)" of his product,

3. Obliges the EU Member States to provide additional protection:

a) of any technological measure that can hurt rights of the author, at the first place that can hurt his intellectual product (Article 6, paragraph 1),

b) of illegal possessing of intellectual product for any commercial purpose (Article 6, paragraph 2),

c) to respect and apply *mutatis mutandis* the elements of Directive 92/100/EEC[38] and Directive 96/9, also aimed for the protection of copyright and connected rights (by the Article 6, Paragraph 4, Point 4),

4. Also obliges the EU Member States to provide for adequate legal protection against any person knowingly performing without authority:

a) the removal or alteration of any electronic rights management information [Article 7, Paragraph 1, under (a)], and

b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive [Article 7, Paragraph 1, under (b)] or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority,

Directive 2006/116/EC on the term of protection of copyright and certain related rights, *Official Journal of the European Union*, L 265, 11, 10, 2011.

36 See: Title and the Article 1, Paragraph, 1 Point 1 of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, *Official Journal of the European Union*, L 167 , 22/06/2001, pp.: 0010 – 0019.

37 See: Articles 11 and 12 of the Directive 2001/29/EC.

38 Council Directive 92/ 100/EEC of 19 November 1992nd on rental right and lending right and on certain rights related to copyright in the field of intellectual property, *Official Journal of the European Communities*, No L 346/61, 27th November 1992.

5. Obliges the states to establish adequate and proportional sanctions for the infringements of copyright and the obligations with such rights connected (Article 8, Paragraph 1), as well as to undertake necessary measures to confiscate illegally obtained and/or used intellectual products (Article 8, Paragraph 2).

As can be seen from the text, it is clear that the Directive 2001/29 treats all kinds of intellectual products of importance for IT society, which means WEB products also, all their elements which were defined by the Convention on the Use of Electronic Communications in International Contracts[39] and in detail explained through law science[40].

Our attention is also paid to the European Union Directive 2004/48 on the enforcement of intellectual property rights[41] by which the text relating rights of authors, at the by the Directive 2004/48 same time are defining intellectual products as goods that also have to be obligatorily treated by the contracting rules in force[42]. The Actually, at the beginning of the text, the Directive points that the author possesses all rights for the protection of their intellectual property, which means that "the inventor or creator (has the right) to derive a legitimate profit from his invention or creation. It should also allows the widest possible dissemination of works, ideas and new know-how[43]" and that the Member States have the obligation to precisely and at a qualitative way protect such rights and products, fully respecting the legislature of the European Union[44], especially the Directive 2000/31[45], which, among other things, treats electronic commerce[46].

The Directive 2000/31 establishes many obligations to the EU Member States, especially the ones regulating the issues of: general obligations[47], evidence[48], right of information[49], measures[50], injunctions from the judicial authorities and the right holders against the infringers of copyright and related rights[51], infringers to paying damages[52] and that, starting from the Berne Convention for the Protection of Literary and Artistic Works, to enable authors to request protection if they possess only the minimal testimonial elements[53]. Also that states have to make possible, by legislation, the protection of any possible: threatening, violation of rights and further producing of damages before the formal ending of any legal proceeding[54].

39 United Nations Convention on the Use of Electronic Communications in International Contracts, United Nations General Assembly Resolution A/RES/60/21, 9th December 2005.
40 See, for example: Polanski, Paul, Przemyslaw (June 5-7, 2006): Convention of E-Contracting: The Rise of International Law of Electronic Commerce? 19th Blend e Conference, eValues, Slovenia.
41 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, *Official Journal of the European Union*, L 157 of 30 April 2004.
42 Having in mind contracting rules see especially:
94/800/EC: Council Decision (of 22 December 1994) concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994), *Official Journal of the European Union of the European Union*, L 336 , 23/12/1994, pp. 0001 – 0002.
43 Regulated precisely by the Introductory part of the Directive 2004/48/EC, under (2) and Articles: 1, and 2 (Paragraph 1).
44 See Directive 2004/48/EC: introductory part of the text, under (3), and Article 3.
45 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *Official Journal of the European Communities*, L 178, 17.7.2000 EN.
46 Directive 2000/31/EC, introductory part of text, under (15).
47 By the Articles: 1, 2 and especially 3.
48 By the Articles 6 and 7.
49 Article 8 of the Directive 2000/31/EC.
50 See Directive 2000/31/EC, Articles: 9, 10 and 12.
51 Article 11 of the Directive 2000/31/EC.
52 Ibid, Article 13.
53 See: Introductory part of the Directive2000/31/EC, under (19) and Article 5, Paragraph 1, point under (b).
54 See: Introductory part of the Directive2000/31/EC, under (24) and Article 13.

CRIMINAL LAW PROTECTION OF COPYRIGHT AND RELATED RIGHTS

Penal protection of copyright and related rights in the legislature of the European Union Member States is located in: 1. Basic criminal legislations, or 2. Secondary criminal legislations, but mostly at the levels of national criminal legislations, basic and secondary, formed before the time of the European Union establishing.

To the first group belong the states that, in the first place and over the time, developed legislative acts that treat (regulate) some of the copyright and related rights issues, and, in the second place, developed penal protection of such by legal acts regulating copyright and the related rights. Such protection had been developed through forming and putting in force a number of norms, locating them in the so cold:

a.) basic, and

b.) secondary penal legislation,

which means:

1. By penal law elements, primarily the elements of criminal law, as the elements (norms) of Criminal Laws (and Codes) and

2.Legislative acts that primarily treat (regulate) some of the copyright and related rights issues but also formulate and put in force penal protection of regulated rights.

Good examples of such states are: Denmark[55], Netherlands[56] and Finland[57].

To the second group belong the states that regulated the copyright and related rights, thus protecting them, with the number of *lex specialist*, at the same time providing penal protection of the regulated rights by the specific elements of relatively new criminal codes. Examples of such states such are: Bulgaria[58], Czech Republic[59], Estonia[60] and Hungary[61], in essence the "young" Member States of the European Union that had the obligation to harmonize their legislations, criminal legislature also, with the legislature of the EU.

To the third group belong the states that the criminal protection of the copyright and related rights regulated, in essence, by special legal acts aimed for the regulation of all the issues of the copyright and related rights regulation, to mention some of them: Austria[62], Germany[63], and Italy[64].

55 See: Danish Penal Code, Consolidated Act no. 1068 of 6 November 2008 as amended by Act no. 1404 of 27 December 2008, Act no. 319 of 28 April 2009 and Act no. 501 of 12 June 2009, Section 299b, Danish Trademark Act, Consolidated Act no. 90 of 28 January 2009, Section 42, i Danish Copyright Act, Consolidated Act no. 587 of 20 June 2008. Sections: 76, 77, 80.

56 See: The Dutch Penal Code, Adopted at 3rd March 1881, updated by amendments up to the 1994, Article: 23(3), (4) i (7) and Dutch Copyright Act of 23 September 1912, Articles: 31, 31A, 31B, 32 and 33.

57 See: Criminal Code of Finland (39/1889, amendments up to 927/2012 included), Chapter 49, Section 1, and Copyright Act of Finland (Act No. 404 of July 8th 1961, as amended up to April 30th, 2010), Chapter 7, Section 56a.

58 See: Criminal Code (Republic of Bulgaria), *State Gazette*, No. 26/1968, amended by the *State Gazette*, No. 32/2010, Articles: 172a and 172b; in force from the 28th. 05. 2010.

59 Czech Republic Criminal Code, Act No. 140/1961, Article. 152.

60 Penal Code of Estonia, originally named: RT1 I 2001, last amendments at the year 2007. (RT I 2007), Chapter 14, criminal acts defined by the Articles: 219, 222, 2221, 223, 224, 225 and 225.

61 See: Act C of 2012 on the Criminal Code of Hungary, 13 July 2012, Section 329/A.

62 See: Republic of Austria Federal Law on Copyright in Works of Literature and Art and on Related Rights (BGBl. No. 111/1936, as last amended BGBl. I No. 25/1998), Section 91, and Austrian Design Law 1990, *Federal Law Gazette*: 1990/497 as amended by 1992/772, I 2001/143, I 2003/81, I 2004/149, I 2005/131 and I 2005/151, Section 35.

63 Act on Copyright and Related Rights (Copyright Act of Germany). Full citation: Copyright Act of 9 September 1965 (Federal Law Gazette Part I, p. 1273), as last amended by Article 8 of the Act of 1 October 2013 (Federal Law Gazette Part I, p. 3714), Article: 106-111a.

64 Law No. 633 of April 22, 1941, for the Protection of Copyright and Neighboring Rights (as last amended by Legislative Decree No. 154 of May 26, 1997), Article: 171 *bis*, 171 *ter*, 171 *quater*.

What we can conclude based on fast analyses is that the European Union Member States have not harmonized their legislatures regarding the issues of incriminations and sanctions, this means: They have not yet provided all the necessary and requested elements for the required criminal law protection of the copyright and related rights, nor that such existing elements have really been harmonized between states, as the Directive 2004/48 claims., , A proposal for the European Union Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights to supplement the Directive 2004/48/EC on the enforcement of intellectual property rights[65], was drafted for this reason practically ten years ago, but has not yet been finalized and put in force.

What has been done in the same field of the copyright and related rights regulation and penal protection inside the state Republic of Serbia? We remind you that on more than one occasion we designed legal acts analogous to the actual Copyright and Related Rights Act[66]. Until the year 2005, those previous legal acts contained criminal norms aimed at the protection of the rights of authors, but such protection, by the Criminal Code having been enacted and endorsed[67], was dislocated to its Chapter 20 (Articles: 198-202), for the reason of more practical approach to the copyright and related rights criminal law protection. Unfortunately such step does not automatically produce more frequent and efficient persecutions of such criminal acts and their perpetrators. We have formed such conclusion on the basis of our scientific research by which we recognize the most frequent modes of attacks at the copyright and related rights of the authors. We shall try to explain problems, starting from the cognition of the necessary elements of law and legislature, perceiving the elements of intriguing cases.

Subjects of economies more and more often hire experts to design for them intellectual products by which they can, in many ways, increase their profits. Engaged are:

a.) physical persons, as well as

b.) physical persons, as owners of specialized firms that can do precisely defined jobs.

Paying for such engagements can be determined:

a.) as a defined sum of money,

b.) as percentage of the earnings achieved by such intellectual products, or

c.) in both ways.

The time in which the purchaser has the right to use such product has to be precisely defined in the contract. This automatically obligates the purchaser to stop using this intellectual product after the expiring of the time defined by the text of contract. It is also an important fact that authors authorize their intellectual products more often than in earlier times[68], in the first place at the level of the State institution: Office for Intellectual Propriety of Republic of Serbia. The act of authorization, although not obligatory, is indeed the decisive element for the consideration whether the act of criminal injury is or is not present in a concrete case.

When considering some concrete cases it is imperative not to overlook the substantial fact of *dolus*. We remind you that in the perception of the Serbian citizens there is a widespread notion that intellectual products falling within the categories of:

65 The European Union (EU) (proposed) directive on criminal measures aimed at ensuring the enforcement of intellectual property rights (2005/0127/COD), proposal from the European Commission for a directive aimed "to supplement Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights (Civil enforcement)". Resource: Justification for the proposal, COM (2005) 276 final, July 12, 2005.

66 Originally named: Zakon o autorskom i srodnim pravima. See: *Official Gazette of the Republic of Serbia*, No.: 104/2009, 99/2011 and 119/2012.

67 Criminal Code, *Official Gazette of the Republic of Serbia*, No.: 85/2005, 88/2005 – emendation 107/2005, - emendation 72/2009, 111/2009, 121/2012, 104/2013 and 108/2014.

68 In accordance with the Articles: 1 – 5 of the Law on copyright and related rights, *Official Gazette of the Republic of Serbia*, No: 104/2009, 99/2011 and 119/2012.

a) computer program,
b) products designed by computers, or
c) products suited for placement by computers or computer lines,

can be illegally found and used, although another person, such as the author(s), regularly earns by such products. This, in a really obvious way, confirms clear criminal intention (*dolus*). Intention expressed not only by the use of complete product but also by:

1. Extracting the parts of such product,
2. Any modification,
3. Trans border using, or
4. Using in another state, or states, that had not been covered by any contract element, and
5. Many other possible ways.

For this reason, in practice there is almost no act of only one criminal offence, for example that from Chapter 20 of the Serbian Criminal Code, but a number of such acts in ideal or/and real accumulation(s).

In the case that we came across in our research one legal person from Belgrade, with really low turnover of capital until some 8 years ago, had engaged an expert (holder of a special firm) to design for them a product with the help of which they can increase profit of their school in the year of such engagement. They closed contract and précised:

a) what is to be done, and
b) the span of time in which the orderer has the right to use this intellectual product.

The engaged expert authorized officially his product at the State Office for Intellectual Propriety of Republic of Serbia, accordingly to legislation in force, and after that installed his complete product at the computer system of the orderer to be used in limited time, in accordance with the contract. The author of this legally protected product subsequently, after six years of his contractual engagement, finds out that the other contracting party illegally and continually used and still uses his intellectual product in the Republic of Serbia and abroad, in a number of other states, as well as that for such illegal doings the other party uses parallel and in the organized way computer systems in possession of foreign providers (in the German Democratic Republic) for illegal doing at the territories of a number of foreign states, thus violating many norms of national Law on Copyright and Related Rights (Articles: 3, 5, 8, 14, 15, 16, 17, 19, 20, 21, 22, 30, 31, 34, 42 and 70), for which reason this (and the mentioned norms) has to be observed and treated as the formal an material base for the logical beings forming, logical beings of criminal acts, in the first place from Chapter 20 of the Republic of Serbia Criminal Code. Furthermore in this case it is clear that the observed acts belong to the organized crime, offenses in concurrence (Article 60 of the Criminal Code) as well as to the extended offences (Article 61.), a number of them (more than six year of continual doing).

To be precise, the firm which is the performer of incriminated acts, its owner and general manager, directly act contra obligations from the Serbian Law on Copyright and Related Rights that provides complete protection to the moral and material rights of authors, including the rights connected with the products produced by computers, for this reason clearly contra elements of the actual Criminal Code Act, having in mind that the actors:

1. Agree to illegally use intellectual product of another person (Article 61 of the Criminal Code Act of Serbia), at the same time

2. Organized a team for criminal acts doing (Article 346.: Associating for criminal offence committing), to be precise: the team of six members of different professions needed for such organized criminal acts performing,

3. Engaged a computer operator for the execution of the criminal act from the first section of "Article 198 – Placing under personal name of product", product that cannot be legally copyrighted for the reason that this product of a known author was previously legally and completely copyrighted,

4. Point 3 connected with point 1 of the Article 199 (Unauthorized use of the author's product or the subject of the connected rights), expressed through the use without the approval of the author and an adequate contract of his clearly legally authorized and protected intellectual product,

5. Organizing a group of persons technically necessary for the above mentioned as well as a number of another doings at the aim of their illegal goals, for this reason criminal acts, clearly accessing to the criminal acts doings through:

- section 3 in connection with section 1 of Article 298 (Damage of the computer data and programs), for the reason that is:

illegally changed the elements of the author's intellectual product, originally expressed in the Serbian language, by translating genuine text to the Romanian as well as the Russian language, which is two times done the same criminal act of illegally changing the elements of products of noteworthy values [in this case more than RSD 3,000,000 per year of illegal use], by which acts the perpetrators of crimes adjust this intellectual product for use at the IT addresses, lines and booklets not covered by any contract between the parties, which is, in the Criminal Code of the Republic of Serbia Section 3 in connection with Section 1 of Article 298.

The described events occurred and still occur as follows, that:

1. Minimally one physical person from this legal entity presented himself as the group organizer – group for criminal acts doing,

2. Engaged translators to 3 foreign languages as the assistants to the computer administrator,

3. Engaged an administrator able of illegal changing a copyrighted product that is not his, or his legal propriety, or in the rightful possession of legal entity that engaged him,

4. Also engaged minimally one professional able of text manipulating as well as person in charge for computer design (in reality extraneous design), as well as

5. The present person is responsible in the legal entity that business under the mother firm in the territory of a foreign state (Romania),

6. The present person is responsible in the legal entity that business under the mother firm at the territory of foreign state (Bosnia and Herzegovina) and

7. The present person is responsible in the legal entity that business under the mother firm at the territory of foreign state (Ukraine),

by such doings, continual activities of criminal acts are performed from Articles 298 and 301 of the Criminal Code of the Republic of Serbia, clearly and illegally violating the protected rights of the author, rights that are protected by the norms of Criminal Code, from which reason the organizer, and the members of his criminal team, have to be treated as criminally liable, prosecuted and punished.

INSTEAD OF A CONCLUSION - WHAT WE CAN ADJOURN ON THE BASE OF REALITY RESEARCHING

What has been confirmed by the research and by the example illustrated and explained, is telling us:

1. In the first place, about the real weight of such criminal acts against the copyright and related rights, not only in the presented examples but for all alike, that a long period time, usually of a few years or more, is necessary for the creation of such intellectual products that can be attacked by criminal doing(s). For this reason it is understandable why such products

have been and are rigorously protected in the territory of the European Union by a series of legal acts - Directives (1991/250, 1993/98, 2001/29, 2004/48, but also 2009/24, 1996/9 1998/84, 2006/116 and 2011/77) as well that their most important elements have been also included in the legislature of Republic of Serbia, in the first place as elements of national laws on copyright and related rights, which has to be observed as the material and formal legal base necessary for the logical beings forming, logical beings of the norms, in the example of Republic of Serbia, placed into the Criminal Code Act, Chapter 20.

2. Our scientific research shows that there exists a really big difference between the European Union Member States on the level of formal and practical approach to the problems of copyright and related rights protection, especially the protection of intellectual products designed by computers. This was, at the level of the European Union, the prime reason to formulate a series of Directives that continue one after another, protecting intellectual products in many ways.

3. Although European Union possesses a long series of directives aimed at the protection of copyright and related rights, the Member States have not yet responded to the request of the Directive 2004/48 to mutually harmonize their criminal law norms that protect intellectual products and proprieties.

4. Although it is obvious that, year by year, the criminal prosecution of the acts that attack "computer programs" as the products of authors increases, until now no adequate attitude has been expressed toward the necessity for the criminal law protection of the all other intellectual products of authors, among them also the products designed by computers as adequate technical instruments.

5. Although Republic of Serbia, possesses relatively good elements of legislature necessary for the protection of copyright and related rights, among them those aimed at protection of intellectual products produced by using computers, in reality the criminal prosecution of such incriminated acts is poor.

6. The xpressed low quality of criminal prosecution mostly comes from the fact that such criminal acts are relatively new forms of unwanted and incriminating doings.

7. Our research confirms that in the territory of Serbia legal entities have not yet been prosecuted for the criminal acts explained in this paper. They also have to be prosecuted and adequately punished for the observed criminal acts. Elements of the Law on the Legal Persons Penal Responsibility[69] have to be respected and this is an obligation at which we pointed in our earlier works[70].

REFERENCES

1. Act C of 2012 on the Criminal Code of Hungary, 13 July 2012.
2. A Law Enforcement Guide to Postal Crimes. Publication 146. June 2004. Publisher: *National Headquarters*, *US Postal Inspection Service*, Washington DC, 20260-2169.
3. Act on Copyright and Related Rights (Copyright Act of Germany). Full citation: Copyright Act of 9 September 1965 (Federal Law Gazette Part I, p. 1273), as last amended by Article 8 of the Act of 1 October 2013 (Federal Law Gazette Part I, p. 3714).
4. Austrian Design Law 1990, *Federal Law Gazette*: 1990/497 as amended by 1992/772, I 2001/143, I 2003/81, I 2004/149, I 2005/131 and I 2005/151, Section 35.

69 Law on the Legal Persons Penal Responsibility, *Official Gazette of the Republic of Serbia*, No 97/2008.
70 Joldžić Vladan (2007): Kompjuterski kao deo elektronskog kriminaliteta – neka razmišljanja. *Pravni život*, br. 10, Tom 2, Beograd, Srbija.

5. Berne Convention for the Protection of Literary and Artistic Works, of September 9th, 1886, completed at Paris on May 4th, 1896, revised at Berlin on November 13th, 1908, completed at Berne on March 20th, 1914, revised at Rome on June 2nd, 1928, at Brussels on June 26th, 1948, at Stockholm on July 14th, 1967, and at Paris on July 24th, 1971, and amended on September 28th, 1979.
6. Consolidated versions of the Treaty on European Union, *Official Journal of the European Union*, C 326, 26/10/2012, pp. 13.-.47.
7. Council Decision 94/800/EC: (of 22 December 1994) concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994), *Official Journal of the European Union of the European Union*, L 336 , 23/12/1994, pp. 0001 – 0002.
8. Convention Establishing the World Intellectual Property Organization, Signed at Stockholm on July 14, 1967 and as amended on September 28th, 1979.
9. Convention on the Use of Electronic Communications in International Contracts, United Nations, General Assembly, New York, 23. 11. 2005. *United Nations Publication Sales*, No.: E.07.V.2. ISBN: 978-92-1-133756-3.
10. Copyright Act of Finland [(Copyright Act) Act No. 404 of July 8, 1961, as amended up to April 30, 2010)].
11. Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights, *Official Journal of the European Union*, L 290 , 24/11/1993, pp. 0009 – 0013.
12. Council Directive 92/ 100/EEC of 19 November 1992nd on rental right and lending right and on certain rights related to copyright in the field of intellectual property, *Official Journal of the European Communities*, No L 346/61, 27. 11. 1992.
13. Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *Official Journal of the European Union*, L, 122, 17/05/1991, pp. 0042 – 0046.
14. Criminal Code (Republic of Bulgaria), *State Gazette*, No. 26/1968, amended by the *State Gazette*, No. 32/2010, Articles: 172a and 172b; in force from the 28th. 05. 2010.
15. Criminal Code of Finland (39/1889, amendments up to 927/2012 included).
16. Criminal Code, *Official Gazette of the Republic of Serbia*, No. 85/2005, 88/2005 – emendation 107/2005, - emendation 72/2009, 111/2009, 121/2012, 104/2013 and 108/2014.
17. Czech Republic Criminal Code, Act No. 140/1961, as amended by Acts No. 120/1962 - No. 103/1997.
18. Danish Copyright Act, Consolidated Act No. 587 of 20 June 2008.
19. Danish Penal Code, Consolidated Act No. 1068 of 6 November 2008 as amended by Act no. 1404 of 27 December 2008, Act no. 319 of 28 April 2009 and Act No. 501 of 12 June 2009.
20. Danish Trademark Act, Consolidated Act No. 90 of 28 January 2009.
21. David S. Wall (June, 2008): Cybercrime: The Transformation of Crime in the Information Age, *Polity Press*, Cambridge, UK.
22. Directive 96/9/EC of the European Parliament and of the Council on the legal protection of databases, *Official Journal of the European Communities*, No L 77/20 EN, of 11th March 1996.
23. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), *Official Journal of the European Communities*, L 178, 17.7.2000 EN.
24. Directive 2011/77/EU of the European Parliament and of the Council of 27 September 2011 amending Directive 2006/116/EC on the term of protection of copyright and certain related rights, *Official Journal of the European Union*, L 265, 11th October 2011.
25. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, *Official Journal of the European Union*, L 157 of 30 April 2004.

26. Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version), *Official Journal of the European Communities,* L 372, 27.12.2006, pp. 12 – 18.
27. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, *Official Journal of the European Union*, L 167 , 22/06/2001, pp. 0010 – 0019.
28. Dutch Copyright Act, of 23 September 1912.
29. Dutch Penal Code, Adopted at 3rd March 1881, updated by amendments up to the 1994.
30. Fafinski, Stefan (2008): *UK Cyber-crime Report*. Publisher: 1871 Ltd, UK.
31. Gottschalk, Petter (2010): Categories of financial crime, *Journal of Financial Crime*, Vol. 17, Iss: 4, pp. 441 – 458.
32. Hansen, Laura L. (2009): Corporate financial crime: social diagnosis and treatment, *Journal of Financial Crime*, Vol. 16, Iss: 1, pp. 28 – 40.
33. Joldzic, Vladan (2008): Ecology Law - General Part. Or on the Elements Necessary for the Establishing and Existing of the Independent Law Discipline (Personal Observations). Publisher: *Revista Mestrado em Direito*, Osasco, Brasil, Ano 9, n. 1.
34. Joldžić, Vladan (2008): *Ekološka politika. Od ideje do izgradnje međunarodnog ekološkog prava, Chapter 7: Metodi potrebni za celovito sagledavanje ekološko-pravnog odnosa kao predmeta naučnog izučavanja i praktičkog tretmana*. Publisher: Institute for Criminological and Sociological Researches, Belgrade.
35. Joldžić, Vladan (2007.): Kompjuterski kao deo elektronskog kriminaliteta – neka razmišljanja, *Pravni život*, br. 10, Tom 2, Beograd, Srbija, pp. 165 - 174.
36. Law No. 633 of April 22, 1941, for the Protection of Copyright and Neighboring Rights (as last amended by Legislative Decree No. 154 of May 26, 1997) (Italy).
37. Law on Copyright and Related Rights, *Official Gazette of the Republic of Serbia*, No: 104/2009, 99/2011 and 119/2012.
38. Law on the Legal Persons Penal Responsibility, *Official Gazette of the Republic of Serbia*, No 97/2008.
39. Moore, R. (2005): Cyber Crime: Investigating High-Technology Computer Crime, *Anderson Publishing*, Cleveland, Mississippi, USA.
40. Penal Code of Estonia, originally named: RT1 I 2001, last amendments at the year 2007. (RT I 2007).
41. Polanski, Paul, Przemyslaw (June 5-7, 2006): Convention of E-Contracting: The Rise of International Law of Electronic Commerce? *19th Bled eConference, eValues*, June 5 - 7, 2006, Slovenia.
42. Republic of Austria Federal Law on Copyright in Works of Literature and Art and on Related Rights,
43. BGBl. No. 111/1936, as last amended *BGBl.* I No. 25/1998.
44. Rizgar Mohammed, Kadir (2010): The Scope and the Nature of Computer Crimes Statutes, A Critical Comparative Study, *German Law Journal*, Vol. 11, No 6, pp. 609. - 632.
45. Robb, George (2002): White-Collar Crime in Modern England: Financial Fraud and Business Morality, *Cambridge University Press*, Cambridge, GB.
46. The European Union (EU) (proposed) directive on criminal measures aimed at ensuring the enforcement of intellectual property rights (2005/0127/COD), proposal from the European Commission for a directive aimed "to supplement Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights (Civil enforcement)". Source: Justification for the proposal, COM (2005) 276 final, July 12, 2005.

47. The Treaty on the Functioning of the European Union, *Official Journal of the European Union*, C 326, 26/10/2012, pp. 47. - 201.
48. U.S. Postal Inspection Service - A Guide for the U.S. Congress. *United States Postal Service*, Publication 278. February 2008, PSN 7610-08-000-4312.
49. United Nations Convention on the Use of Electronic Communications in International Contracts, United Nations General Assembly Resolution A/RES/60/21, 9th December 2005.
50. Universal Copyright Convention, Signed at Geneva on 6th September 1952, United Nations - Treaty Series, No 2937, Year 1955.
51. Uredba o ratifikaciji Konvencije o osnivanju Svetske organizacije za intelektualnu svojinu, *Službeni list SFRJ - Međunarodni ugovori i drugi sporazumi*, No 31/1972, and *Službeni list SFRJ - Međunarodni ugovori*, No 4/1986, - dr. uredba.

UDC: 343.533::004
343.53:336.741.1
343.9.024:336.7

CYBERCRIME AND MONEY LAUNDERING

Miguel Abel Souto, PhD[1]
University of Santiago de Compostela

Abstract: An offense that has benefited most from the internet is money laundering thanks to the potential provided via internet and electronic transfers for executing this crime.

These new technologies are appealing to money launderers mainly because of the anonymity provided, high marketability and usefulness of funds and global access to ATM network. To these factors one should add the problems of persecution, which requires new investigation methods that must maintain the delicate balance between security and fundamental rights.

In any case, to avoid misuse of legal insufficiencies in new technologies by organized crime, internet cannot be an area outside the law, but must be regulated.

Undoubtedly, the new payment systems facilitate money launderers' criminal activity. These systems are better than cash for moving large sums of money, non-face to face business relationships favour the use of straw buyers and false identities, the absence of credit risk, as there is usually a prepaid, discourages service providers from obtaining a complete and accurate customer information, and the nature of the trade and the speed of transactions make it difficult to control property or freezing.

However, the development of technologies, including the internet, has unquestionable advantages involved and even provides, through online resources, verification of identity or other duty of surveillance for the prevention of money laundering

Keywords: money laundering, cybercrime, security and fundamental rights.

INTERNET AND MONEY LAUNDERING

Money laundering is a "crime of globalization"[2]. Its importance nowadays is transcendental because of the economic crisis we are suffering.

Indeed, it was noted that "an offense that has benefited most from the internet is money laundering"[3], "generalised and radicalized"[4] by the new electronic media, with a "spectacular"[5] development thanks to the potential provided via internet and electronic transfers[6] for executing this crime[7].

---

1 **Corresponding author:** Miguel Abel Souto is Professor of Criminal Law, University of Santiago de Compostela, Spain, and Director of the *Revista Cuatrimestral Europea sobre Prevención y Represión del Blanqueo de Dinero* (European Quarterly Review for Prevention and Repression of Money Laundering). Email: miguel.abel@usc.es.
2 Levi, 2012, p. 107.
3 Velasco San Martín, 2012, p. 75.
4 Sandywell, 2010, p. 46.
5 Pérez Estrada, 2010, p. 306.
6 Fernández Teruelo, 2011, pp. 231 and 234.
7 Abel Souto, 2012a, pp. 1–45; 2012b, pp. 220–247; 2013a, pp. 266–284; 2013b, pp. 1–53; 2013c, pp. 1–7; 2014a, pp. 80–91.

NEW PAYMENT METHODS AND PROBLEMS OF PERSECUTION

The increasing use of new payment methods, such as transactions and movements of funds, resulted in an increase in the detection of cases of money laundering committed using telematic media[8]. These new technologies are appealing to money launderers mainly because of the anonymity[9] provided, high marketability and usefulness of funds and global access to ATM network[10]. To these factors one should add: the problems of persecution[11], which requires new investigation methods that must maintain the delicate balance between security and fundamental rights[12].

In any case, to avoid misuse of legal insufficiencies in new technologies by organized crime[13], internet cannot be an "area outside the law"[14], but must be regulated[15].

ADVANTAGES AND DISADVANTAGES OF NEW TECHNOLOGIES

Undoubtedly, the new payment systems facilitate money launderers' criminal activity. These systems are better than cash for moving large sums of money, non-face to face business relationships favour the use of straw buyers and false identities, the absence of credit risk, as there is usually a prepaid, discourages service providers from obtaining a complete and accurate customer information, and the nature of the trade and the speed of transactions make it difficult to control property or freezing[16].

However, the development of technologies, including the internet, has unquestionable advantages involved and even provides, through online resources, verification of identity or other duty of surveillance for the prevention of money laundering[17]. The new payment methods are the result of the need to both offer commercial alternatives to traditional financial services and to include everyone in the system irrespective of poor credit rating, age or residence in areas of low bank offer. These methods can also have a positive effect on the economy, given their efficiency in terms of speed of transactions, technological security, low costs compared to payment instruments based on paper, and accessibility, especially for prepaid cards and payment services with mobile phones, identified as a possible tool to integrate excluded individuals because of poverty[18].

For example, a total of four million people in the United States receive Social Security benefits without actually being bank accounts holders. To reduce their dependence on cheques, which force spending between 50 and 60 dollars a month in check cashing, bill payment or sending money to their families, benefits were provided with prepaid cards with which one could buy goods or get cash. Moreover, in 2009, the war displaced in Pakistan more than a million people, and their government distributed prepaid cards with a maximum value of 25,000

8 FATF, 2010, p. 7.
9 Mata Barranco, 2010, p. 19; Miró Llinares, 2011, pp. 12, 13, 25 and 26.
10 FATF, 2010, p. 7.
11 Gless, 2012, pp. 3–22.
12 Pérez Estrada, 2010, pp. 307, 309 and 311–317.
13 Angelini and Gibson, 2007, pp. 65–73.
14 Gless, 2012, p. 22.
15 Gómez Tomillo, 2006, p. 189.
16 FATF, 2010, p. 21.
17 The money laundering, 2011, pp. 37–39 and 54.
18 FATF, 2010, p. 12.

rupees, about $300, for the immediate assistance of 300,000 families. Similarly, in Afghanistan, the police salary is paid via mobile phones, so that policemen do not have to leave their job in order to collect their salary. This also reduces the possibility of corruption or bribery[19].

In 1996, the Financial Action Task Force (FATF) was specifically concerned in the recommendation number 13 with new technologies and the danger they pose for potential money laundering by allowing the realization of huge transactions instantly from remote locations, while keeping the anonymity of the transgressor and without the involvement of traditional financial institutions. The absence of financial intermediation makes it difficult to identify customers and to keep a record of relevant information. In addition, traditional investigation techniques become ineffective or obsolete to new technologies: the problem of physical volume of money posed for launderers[20] – to the point of leaving the paper money because of slow movement – is minimized with "electronic money", its rapid mobility, especially on the internet, difficult to trace the funds transferred and the unusual volume of data to analyse make it almost impossible to detect any suspicious activity.

Please note that 30 years ago there was no internet. However, a decade and a half later the closure of the "European Union Bank"[21] was agreed in Antigua, the bank that became famous for being the first bank to operate through the internet and for advertising explicitly on the web, which made it the right bank for tax evaders and money launderers[22]. Today nearly three-quarters of households in the European Union have internet access and over a third of the population makes banking online[23].

Precisely for this reason the FATF developed, in October 2010, a report regarding the use of new payment methods for money laundering[24] which focused on prepaid cards, payment services on the internet[25], steady growth, and its misuse for the implementation of the so-called "cyber laundering"[26] as well as on payments with mobile phones. Notably, with regard to this latter issue, it is estimated that 1,400,000,000 people used payments via mobile phones for their financial transactions in 2015[27].

Also the FATF has provided revised recommendations on February 16, 2012, of which recommendation number 15 indicates that countries and financial institutions should identify and assess the risks for money laundering relating to new technologies, while recommendation number 16 discusses electronic transfers and identifying both their originators and beneficiaries[28].

As for the detection and monitoring of transboundary movements of cash, and despite being one of the oldest techniques of money laundering, it still continues to increase its volume significantly[29]. Thus, the study of the framework of the Mafia published by VARESE, showed that criminal goods arrived in Italy by a large network of individuals who travelled from Russia with cash[30]. There are also new "money mules" recruited by email with the excuse of having an opportunity to work at home through internet. Sometimes the only payment they receive is criminal prosecution for money laundering[31].

19 FATF, 2010, pp. 12, 13, 15 and 20.
20 Abel Souto, 2013b, pp. 2–6; Vidales Rodríguez, 2015a, pp. 91 and 92, note 6, and 2015b, p. 16.
21 Schudelaro, 2006, pp. 47–72.
22 Blum *et al.,* 1999, pp. 52–57, with reproduction of the advertisements that the "European Union Bank" made available in internet; Martin, 1997, pp. 38 and 39.
23 Bruselas, 2012, p. 1; Comisión, 2012, p. 1.
24 Baldwin and Fletcher, 2004, pp. 125–158.
25 Philippsohn, 2001, pp. 485–490; Ping, 2004, 48-55; Yan *et al.,* 2011, pp. 93–101.
26 Filipkowski, 2008, pp. 15–27.
27 FATF, 2010, p. 18.
28 FATF, 2010, p. 17.
29 FATF, 2010, pp. 46 and 47.
30 Varese, 2012, p. 242.
31 Clough, 2010, pp. 187 and 188.

BETWEEN CHARYBDIS AND SCYLLA

Finally the 32nd recommendation urges countries to ensure that their authorities impede or restrict the movement of cash which is potentially related to money laundering[32] and Article 14.2 of the United Nations Convention against corruption provides that "States Parties shall considerer implementing feasible measures to detect and monitor the movement of cash and appropriate negotiable instruments across their borders", but "without impeding in any way the movement of legitimate capital". It has been said that the cash is the common medium of exchange in criminal transactions[33]. In similar vein, the Spanish government, having more closely in mind its tax collection purposes, approved in the council of ministers of 22 June 2012 a bill to combat tax fraud, given the legislative experience of other EU countries like France and Italy, limited to 2,500 euro cash payments for operations involving businessmen or professionals[34]. However, in order to escape the Charybdis of paper money we will find the Scylla of "electronic money", as new payment technologies are not without risks that may thwart prevention and repression of money laundering. Furthermore, behind the apparent dogma of the "criminogenic character of cash" hides a program that exceeds the fight against crime, further marginalizing those who earn less and allows control of the private sphere[35].

REFERENCES

1. Abel Souto, M. (2002), El blanqueo de dinero en la normativa internacional: especial referencia a los aspectos penales, Servicio de publicacións e intercambio científico, Universidad de Santiago de Compostela, Santiago.
2. Abel Souto, M. (2005a), "Década y media de vertiginosa política criminal en la normativa penal española contra el blanqueo. Análisis de los tipos penales contra el blanqueo desde su incorporación al Texto punitivo español en 1988 hasta la última reforma de 2003", La Ley Penal. Revista de Derecho Penal, Procesal y Penitenciario, No. 20, octubre, pp. 5–26.
3. Abel Souto, M. (2005b), El delito de blanqueo en el Código penal español, Bosch, Barcelona.
4. Abel Souto, M. (2009), "Conductas típicas de blanqueo en el Ordenamiento penal español", in Abel Souto and Sánchez Stewart, pp. 175–246 and 325–327.
5. Abel Souto, M. (2011a), "La expansión penal del blanqueo de dinero operada por la Ley orgánica 5/2010, de 22 de junio", La Ley Penal. Revista de Derecho Penal, Procesal y Penitenciario, No. 79, febrero, pp. 5–32.
6. Abel Souto, M. (2011b), "La reforma penal, de 22 de junio de 2010, en materia de blanqueo de dinero", in Abel Souto and Sánchez Stewart, pp. 61–109.
7. Abel Souto, M. (2011c), "Luces y sombras en la reforma penal sobre drogas de 2010", La Ley Penal. Revista de Derecho Penal, Procesal y Penitenciario, No. 83, junio, pp. 61–86.
8. Abel Souto, M. (2012a), "Blanqueo, innovaciones tecnológicas, amnistía fiscal de 2012 y reforma penal", Revista Electrónica de Ciencia Penal y Criminología, No. 14, pp. 1–45.
9. Abel Souto, M. (2012b), "The Update of Penalty Concept and Adjustment of Crime in Money Laundering", Antiriciclaggio, No. 2/3, pp. 220–247.
10. Abel Souto, M. (2013a), "Money laundering, new technologies and Spanish penal reform", Journal of Money Laundering Control, No. 16, 3, pp. 266–284.
11. Abel Souto, M. (2013b), "Volumen mundial del blanqueo de dinero, evolución del delito en España y jurisprudencia reciente sobre las últimas modificaciones del Código penal", Revista General de Derecho Penal, No. 20, pp. 1–53.

32 FATF, 2012, pp. 25 and 99–102.
33 Jurado and García, 2011, p. 172.
34 Ley 7/2012, Article 7.
35 Pieth, 1992, p. 27.

12. Abel Souto, M. (2013c), "Anti-corruption strategy in the global era and money laundering", Fifth Session of the International Forum on Crime and Criminal Law in the Global Era, Beijing, pp. 1–7.
13. Abel Souto, M. (2013d), "El blanqueo de dinero como innovador instrumento de control económico y social", Revista Penal México, No. 5, pp. 109–140.
14. Abel Souto, M. (2014a), "Drugs criminal policies in the global era and money laundering", Sixth Session of the International Forum on Crime and Criminal Law in the Global Era, Beijing, pp. 80–91.
15. Abel Souto, M. (2014b), "Jurisprudencia penal reciente sobre el blanqueo de dinero, volumen del fenómeno y evolución del delito en España", in Abel Souto and Sánchez Stewart, pp. 137–201 and 309–317.
16. Abel Souto, M. (2014c), "Política criminal sobre drogas en la era global y blanqueo de dinero", Revista Cuatrimestral Europea sobre Prevención y Represión del Blanqueo de Dinero, No. 2, pp. 9–22 and also in Revista Penal (2015), No. 36, pp. 5–13.
17. Abel Souto, M. (2015), "El blanqueo de dinero: problemática actual española, con anotaciones de Derecho comparado estadounidense", Derecho Penal Contemporáneo, Revista Internacional, Bogotá, No. 53, pp. 5-68.
18. Abel Souto, M. and Sánchez Stewart, N. (2009) (coords.), I congreso de prevención y represión del blanqueo de dinero, Tirant lo Blanch, Valencia.
19. Abel Souto, M. and Sánchez Stewart, N. (2011) (coords.), II congreso sobre prevención y represión del blanqueo de dinero, Tirant lo Blanch, Valencia.
20. Abel Souto, M. and Sánchez Stewart, N. (2013) (coords.), III congreso sobre prevención y represión del blanqueo de dinero, Tirant lo Blanch, Valencia.
21. Abel Souto, M. and Sánchez Stewart, N. (2014) (coords.), IV congreso sobre prevención y represión del blanqueo de dinero, Tirant lo Blanch, Valencia.
22. Albrecht, H.-J. (2001), Criminalidad transnacional, comercio de narcóticos y lavado de dinero, translated to Spanish by Óscar Julián Guerrero Peralta, Universidad Externado de Colombia, Bogotá.
23. Álvarez Pastor, D. and Eguidazu Palacios, F. (2007), Manual de prevención del blanqueo de capitales, Marcial Pons, Madrid/Barcelona.
24. Angelini, D. and Gibson, S. (2007), "Organized crime and technology", Journal of Security Education, Vol. 2, No. 4, pp. 65–73.
25. Aránguez Sánchez, C. (2000), El delito de blanqueo de capitales, Marcial Pons, Madrid/Barcelona.
26. Baldwin, Jr. and Fletcher, N. (2004), "The financing of terror in the age of the internet: wilful blindness, greed or a political statement?", Journal of Money Laundering Control, Vol. 8, No. 2, pp. 125–158.
27. Berdugo Gómez De La Torre, I. and Fabián Caparrós, E.A. (2010), "La 'emancipación' del delito de blanqueo de capitales en el Derecho penal español", Diario La Ley, No. 7535, 27 de diciembre, pp. 1–19.
28. Bermejo, M.G. (2015), Prevención y castigo del blanqueo de capitales, Marcial Pons, Madrid/Barcelona.
29. Bermejo, M.G. and Agustina Sanllehí, J.R. (2012), "El delito de blanqueo de capitales", in Silva Sánchez, J.-M. (dir.), El nuevo Código penal. Comentarios a la reforma, La Ley, Madrid, pp. 439–462.
30. Blanco Cordero, I. (2011), "El delito fiscal como actividad delictiva previa del blanqueo de capitales", Revista Electrónica de Ciencia Penal y Criminología, No. 13–01, pp. 1–46.
31. Blanco Cordero, I. (2015), El delito de blanqueo de capitales, 4th ed., Aranzadi, Cizur Menor.
32. Blum, J.A. et al. (1999), Refugios financieros, secreto bancario y blanqueo de dinero, Naciones Unidas, Nueva York.
33. "Bruselas propone crear un centro europeo contra la ciberdelincuencia" (2012), Gaceta Informativa, Lex Nova, No. 436, 28 de marzo, in http://www.lexdiario.es/noticias/119713/bruselas (accessed January 2016).

34. Carazo Johanning, A.T. (2014), Algunas reflexiones sobre la política de drogas en Costa Rica, Center for the Administration of Justice, Florida International University, Miami.
35. Clough, J. (2010), Principles of cybercrime, Cambridge University Press, Cambridge.
36. Comisión Europea (2012), "Un centro europeo contra la delincuencia informática para luchar contra los delincuentes en línea y proteger a los consumidores que utilizan internet", in http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317 (accessed January 2016).
37. Convención de las Naciones Unidas contra la corrupción (2006), Instrumento de ratificación de la Convención de las Naciones Unidas contra la corrupción, hecha en Nueva York el 31 de octubre de 2003, BOE de 19 de julio de 2006, pp. 27132–27153.
38. Cuesta Arzamendi, J.L. de la (2010) (dir.), Derecho penal informático, Civitas/Thomson Reuters/Aranzadi, Cizur Menor.
39. Díaz y García Conlledo, M. (2002), "Blanqueo de bienes", in Luzón Peña, D.-M. (dir.), Enciclopedia penal básica, Comares, Granada, pp. 193–221.
40. Díaz y García Conlledo, M. (2013), "El castigo del autoblanqueo en la reforma penal de 2010. La autoría y la participación en el delito de blanqueo de capitales", in Abel Souto and Sánchez Stewart, pp. 281–299, 395 and 396.
41. Díaz-Maroto y Villarejo, J. (2009), "Recepción de las propuestas del GAFI y de las Directivas europeas sobre el blanqueo de capitales en el Derecho español", in Bajo Fernández, M. and Bacigalupo Saggese, S. (eds.), Política criminal y blanqueo de capitales, Marcial Pons, Madrid, Barcelona and Buenos Aires, pp. 21–66.
42. Díez Ripollés, J. L. (1992), "Alternativas a la actual legislación sobre drogas", Cuadernos de Política Criminal, No. 46, pp. 73–116.
43. Fabián Caparrós, E.A. (1998), El delito de blanqueo de capitales, Colex, Madrid.
44. Faraldo Cabana, P. (1998), "Aspectos básicos del delito de blanqueo de bienes en el Código penal de 1995", Estudios Penales y Criminológicos, No. XXI, pp. 117–165.
45. FATF (2010), Report, Money laundering using new payment methods, October, in http://www.fatf-gafi.org (accessed January 2016).
46. FATF (2012), International standards on combating money laundering and the financing of terrorism & proliferation. The FATF recommendations, February, in http://www.fatf-gafi.org (accessed January 2016).
47. Fernández Teruelo, J.G. (2010), "Blanqueo de capitales", in Ortiz De Urbina Gimeno, I. (coord.), Memento experto Francis Lefebvre. Reforma penal. Ley orgánica 5/2010, Ediciones Francis Lefebvre, Madrid, pp. 313–334.
48. Fernández Teruelo, J.G. (2011), Derecho penal e internet, Lex Nova, Valladolid.
49. Fernández Steinko, A. (2012), "Financial channels of money laundering in Spain", The British Journal of Criminology. An International Review of Crime and Society, Vol. 52, No. 5, September, pp. 908–931.
50. Ferré Olivé, J.C. (1989), "La descriminalización del tráfico y tenencia de drogas como alternativa político criminal", Lecciones y Ensayos, No. 52, pp. 11–22.
51. Ferré Olivé, J.C. (2013), "El nuevo tipo agravado de blanqueo cuando los bienes tengan su origen en delitos relativos a la corrupción", in Abel Souto and Sánchez Stewart, pp. 389–391.
52. Filipkowski, W. (2008), "Cyber laundering: an analysis of typology and techniques", International Journal of Criminal Justice Sciences, Vol. 3, No. 1, pp. 15–27.
53. Finklea, K.M. (2009), "Organized crime in the United States: trends and issues for congress", Journal of Current Issues in Crime, Law & Law Enforcement, Vol. 2, No. 1, pp. 9–40.
54. Fisher, J. (2012), "The vulnerability of her majesty's revenue & customs to penetration by criminal actors", Journal of Money Laundering Control, Vol. 15, No. 2, pp. 153–161.
55. Gless, S. (2012), "Strafverfolgung im Internet", Schweizerische Zeitschrift für Strafrecht, Vol. 130, No. 1, pp. 3–22.
56. Gómez Rivero, M.C. (2015), Nociones fundamentales de Derecho penal. Parte especial, Tecnos, Madrid.

57. Gómez Tomillo, M. (2006), Responsabilidad penal y civil por delitos cometidos a través de internet, 2nd ed., Thomson/Aranzadi, Cizur Menor.
58. González Cussac, J.L. and Cuerda Arnau, M.L. (dirs.) (2013), Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación, Tirant lo Blanch, Valencia.
59. González Rus, J.J. (2011), in Morillas Cueva, L. (coord.), Sistema de Derecho penal español. Parte especial, Dykinson Madrid, pp. 636–646.
60. Grupo de Estudios de Política Criminal (1992), "Manifiesto por una nueva política sobre la droga", in Una alternativa a la actual política criminal sobre drogas, Imagraf, Málaga, pp. 9–14.
61. Grupo de Estudios de Política Criminal (2010), "Propuesta alternativa en el ámbito de los delitos de blanqueo de capitales y encubrimiento", in Una regulación alternativa contra la corrupción urbanística y otras conductas delictivas relacionadas, Gráficas Luis Mahave, Málaga, pp. 63–70.
62. Grupo de Estudios de Política Criminal (2014), Autoevaluación. Política criminal de drogas, 23 de mayo, in http://www.gepc.es, (accessed January 2016).
63. Hassemer, W. (1994), "Gewinnaufspürung: jetzt mit dem Strafrecht", Wertpapier Mitteilungen, Zeitschrift für Wirtschafts- und Bankrecht (Gastkommentar), p. 1369, translated to Spanish by Miguel Abel Souto (1998) as "Localización de ganancias: ahora con el Derecho penal", Revista de Ciencias Penales, Vol. 1, No. 1, pp. 217–220.
64. Jurado, N. and García, R. (2011), "El blanqueo de capitales", in Avilés Gómez, M. (coord.), El enriquecimiento ilícito, Editorial Club Universitario, Alicante, pp. 159–193.
65. Lampe, E.-J. (1994), "Der neue Tatbestand der Geldwäsche (§ 261 StGB)", Juristen Zeitung, No. 3, pp. 123-132, translated to Spanish by Miguel Abel Souto and José Manuel Pérez Pena (1997) as "El nuevo tipo penal del blanqueo de dinero (§ 261 StGB)", Estudios Penales y Criminológicos, No. XX, pp. 103–148.
66. Levi, M. (2012), "Crimes of globalisation: some measurement issues", in Joutsen, M. (ed.), New types of crime. Proceedings of the international seminar held in connection with Heuni's thirtieth anniversary Helsinki 20 October 2011, Heuni, Helsinki, pp. 107–115.
67. Ley 7/2012, de 29 de octubre, de modificación de la normativa tributaria y presupuestaria y de adecuación de la normativa financiera para la intensificación de las actuaciones en la prevención y lucha contra el fraude, BOE del 30 de octubre.
68. Lorenzo Salgado, J.M. (2011), "Reformas penales y drogas: observaciones críticas. (Especial referencia a la LO 5/2010, de modificación del Código penal)", in Muñoz Conde, F., Lorenzo Salgado, J.M., Ferré Olivé, J.C., Cortés Bechiarelli, E. and Núñez Paz, M.A. (dirs.), Un Derecho penal comprometido: libro homenaje al prof. Dr. Gerardo Landrove Díaz, Tirant lo Blanch, Valencia, pp. 631–679.
69. Lorenzo Salgado, J.M. (2013), "El tipo agravado de blanqueo cuando los bienes tengan su origen en el delito de tráfico de drogas", in Abel Souto and Sánchez Stewart, pp. 223–249 and 377–379.
70. Manjón-Cabeza Olmeda, A. (2010), "Receptación y blanqueo de capitales (arts. 301 y 302)", in Álvarez García, F.J. and González Cussac, J.L. (dirs.), Comentarios a la reforma penal de 2010, Tirant lo Blanch, Valencia, pp. 339–346.
71. Martin, D. (1997), La criminalité informatique. Cyber-crime: sabotage, piratage, etc., évolution et répression, Presses Universitaires de France, Paris.
72. Martínez-Buján Pérez, C. (2015), Derecho penal económico y de la empresa. Parte especial, 5th ed., Tirant lo Blanch, Valencia.
73. Mata Barranco, N.J. de la (2010), "Ilícitos vinculados al ámbito informático: la respuesta penal", in Cuesta Arzamendi, pp. 15–30.
74. Miró Llinares, F. (2011), "La oportunidad criminal en el ciberespacio", Revista Electrónica de Ciencia Penal y Criminología, No. 13–07, pp. 1–55.
75. Moreno Alcázar, M.A. (2012), "Receptación y blanqueo de capitales", in Boix Reig, J. (dir.), Derecho penal. Parte especial. Volumen II. Delitos contra las relaciones familiares, contra el patrimonio y el orden socioeconómico, Iustel, Madrid, pp. 675–700.

76. Muñoz Conde, F. (2013), "El delito de blanqueo de capitales y el Derecho penal de enemigo", in Abel Souto and Sánchez Stewart, pp. 375 and 376.
77. Muñoz Conde, F. (2015), Derecho penal. Parte especial, 20th ed., Tirant lo Blanch, Valencia.
78. Núñez Paz, M.A. (2011), "Tipologías criminales de blanqueo. Técnicas de comisión", in Abel Souto and Sánchez Stewart, p. 217.
79. Núñez Paz, M.A. (2013), "El tipo agravado de blanqueo de dinero procedente de delitos urbanísticos", in Abel Souto and Sánchez Stewart, pp. 267–279, 393 and 394.
80. Palma Herrera, J.M. (2000), Los delitos de blanqueo de capitales, Edersa, Madrid.
81. Pérez Estrada, M.J. (2010), "La investigación del delito a través de las nuevas tecnologías", in Cuesta Arzamendi, pp. 305–319.
82. Philippsohn, S. (2001), "Money laundering on the internet", Computer & Security, Vol. 20, No. 6, pp. 485–490.
83. Pieth, M. (1992), "Zur Einführung: Geldwäscherei und ihre Bekämpfung in der Schweiz", in Pieth, M. (ed.), Bekämpfung der Geldwäscherei: Modellfall Schweiz?, Helbing & Lichtenhahn, Basel und Frankfurt am Main, Schäffer-Poeschel, Stuttgart, pp. 1–27.
84. Ping, H. (2004), "New trends in money laundering - From the real world to cyberspace", Journal of Money Laundering Control, Vol. 8, No. 1, pp. 48–55.
85. Quintero Olivares, G. (2010a), "Sobre la ampliación del comiso y el blanqueo, y la incidencia en la receptación civil", Revista Electrónica de Ciencia Penal y Criminología, 8 de marzo, pp. 1–20.
86. Quintero Olivares, G. (2010b), "La reforma del comiso (art. 129)", in Quintero Olivares, G. (dir.), La reforma penal de 2010: análisis y comentarios, Aranzadi, Cizur Menor, pp. 107–110.
87. Ruß, W. (1994), "Kommentar zum § 261 StGB", in StGB Leipziger Kommentar. Großkommentar, 11. neubearbeitete Auflage, Walter de Gruyter, Berlin, pp. 321–331, translated to Spanish by Miguel Abel Souto (1997) as "Comentario al parágrafo 261 del Código penal alemán: el blanqueo de dinero", Dereito. Revista Xurídica da Universidade de Santiago de Compostela, Vol. 6, No. 1, pp. 179–196.
88. Salas, L.P. (2014), La legalización de la marihuana medicinal en Estados Unidos, Center for the Administration of Justice, Florida International University, Miami.
89. Sandywell, B. (2010), "On the globalisation of crime: the internet and new criminality", in Jewkes, Y. and Yar, M. (eds.), Handbook of internet crime, Willan Publishing, Devon/Portland, pp. 38–66.
90. Schudelaro, T. (2006), "Electronic payment systems and money laundering: beyond the internet hype", Global Journal on Crime & Criminal Law, Vol. 10, No. 1, pp. 47–72.
91. Silva Sánchez, J.-M. (2010), "La reforma del Código penal: una aproximación desde el contexto", Diario La Ley, No. 7464, 9 de septiembre, pp. 1–13.
92. Terradillos Basoco, J.M. (2008), "El delito de blanqueo de capitales en el Derecho español", in Cervini, R. et al., El delito de blanqueo de capitales de origen delictivo. Cuestiones dogmáticas y político-criminales. Un enfoque comparado: Argentina-Uruguay-España, Alveroni, Córdoba (República Argentina), pp. 203–274.
93. Terradillos Basoco, J.M. (2012), Lecciones y materiales para el estudio del Derecho Penal, vol. IV. Derecho penal. Parte especial (Derecho penal económico), Iustel, Madrid.
94. The money laundering officer's practical handbook 2011 (2011), Compliance training products limited, Cambridge.
95. United Nations Convention against illicit traffic in narcotic drugs and psychotropic substances (1988), in http://www.unodc.org (accessed January 2016).
96. United Nations, Office on drugs and crime (2004), United Nations Convention against corruption, United Nations, New York.
97. Varese, F. (2012), "How mafias take advantage of globalization. The Russian mafia in Italy", The British Journal of Criminology. An International Review of Crime and Society, Vol. 52, No. 2, March, pp. 235–253.

98. Velasco San Martín, C. (2012), La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet, Tirant lo Blanch, Valencia.
99. Vidales Rodríguez, C. (1997), Los delitos de receptación y legitimación de capitales en el Código penal de 1995, Tirant lo Blanch, Valencia.
100. Vidales Rodríguez, C. (2008), El delito de enriquecimiento ilícito, Center for the Administration of Justice, Florida International University, Miami.
101. Vidales Rodríguez, C. (2012), El delito de tráfico de drogas en la legislación penal costarricense, Center for the Administration of Justice, Florida International University, Miami.
102. Vidales Rodríguez, C. (2015a), "El fenómeno asociativo como actividad delictiva previa al delito de blanqueo de capitales", Estudios Penales y Criminológicos, No. XXXV, pp. 87–123.
103. Vidales Rodríguez, C. (dir.) (2015b), Régimen jurídico de la prevención y represión del blanqueo de capitales, Tirant lo Blanch, Valencia.
104. Vogel, J. (1997), "Geldwäsche – eine europaweit harmonisierter Straftatbestand?", Zeitschrift für die Gesamte Strafrechtswissenschaft, No. 2, pp. 335–356.
105. Yan, L. et al. (2011), "Risk-based AML regulation on internet payment services in China", Journal of Money Laundering Control, Vol. 14, No. 1, pp. 93–101.
106. Zaragoza Aguado, J.A. (2015), in Gómez Tomillo, M. (dir.), Comentarios prácticos al Código penal, Aranzadi, Cizur Menor, pp. 635–713.

UDC: 004.7.056:621.39-182.3

DEVELOPMENT OF THE ANDROID-BASED SECURE COMMUNICATION DEVICE

Aleksandar Jevremović, PhD[1]
Mladen Veinović, PhD[2]
Singidunum University, Belgrade
Goran Šimić, PhD
University of Defence, Military Academy, Belgrade

Abstract: The possibility of achieving protected communication has long been a privilege just of professional services and systems that can afford great investment for the development of specialized devices for this purpose. Today, the popularization of open-source development model enables significant reduction of development costs and maintaining high levels of security. This development implies the inclusion of the existing components that enable verifying the implemented principles if it is necessary. This paper discusses key issues related to the development of mobile devices for secure communication based on the Android platform.

Keywords: custom cipher algorithm, network system security.

INTRODUCTION

The possibility of achieving protected communication has long been a privilege only of professional services and systems that are able to make big investments for the development of specialized devices. At this level a safe communication can be considered only the one that is based on the coding algorithm developed by the end user. In addition, the principles of operation of such cipher algorithms may not be known to anyone other than the system end user. From this approach the popular cipher algorithms (DES, AES, etc.) cannot be considered as safety ones.[2]

Therefore, the already built and in-the-box communication protecting systems run out of the question. Cryptographic solutions require reliable (safety) platform for implementation (hardware and system software) which can be verified (open source systems). Method of implementation and confidence in the cryptology synchronization procedures and resynchronization are a key factor for confidence in their custom cryptology solution. Such an implementation prevents the existence of secret doors through which the cipher keys can "leak". Moreover, the procedures about cryptology keys manipulation are essential for such considerations (storage, selection, distribution, deleting, etc.).

Today, the popularization of open-source development model enables significant reduction of development costs and maintaining high levels of security. This development implies usage of already built components that enable verifying implemented principles if it is necessary.

1 e-mail: ajevremovic@singidunum.ac.rs.
2 Bill Snyder, "Snowden: The NSA planted backdoors in Cisco products", InfoWorld, 2014.

This paper discusses key issues related to the development of mobile devices for secure communication based on the Android platform. This research is based on the collected experience[3], [4], [5], [6], [7], [8], [9], [10] in the development of top level communication protection systems based on Linux platform.

NETWORK LEVEL IMPLEMENTATION

Mobile computer networks include the 4G mobile telephony using standardized protocol stacks, OSI and TCP/IP. This standardization allows chaining protocols at different levels in order to achieve optimal performance of various network applications and variety of infrastructures. From the aspect of telecommunications, such stratification allows the implementation of the cipher system at various levels (from physical to the application), depending on the capabilities and needs of a particular telecommunications system.

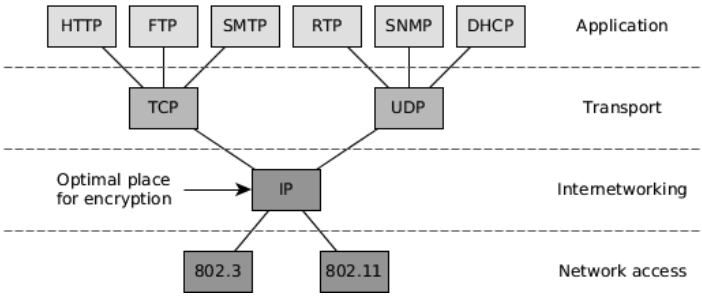


Figure 1: *Different communication levels for implementation of encryption systems*

Encryption system implementation based on physical layer requires the use of special telecommunication infrastructure and such a system would not be possible to use on the Internet network. In addition, these systems are implemented at the hardware level, which can significantly increase the cost of development. Such systems are not flexible, requiring thus the adaptation in accordance with the protected device physical interfaces. Also, they are specialized in non-standardized way and therefore, they need significant funds to invest in the development and implementation. On the other hand, the implementation of encryption functions at the hardware level leaves minimal space for "back door".

3 A. Jevremović., M. Veinović, "IP Security under Linux OS", Proceedings of 50th ETRAN Conference, Belgrade, Serbia, pp. 114-117, 2006.
4 A. Jevremović, M. Veinović, "IPsec – Analyzing Influence of Cryptographic Algorithm on Lan Networks Traffic", 14. Telecommunications Forum Telfor, IEEE, Belgrade, Serbia, 2006.
5 A. Jevremović, M. Veinović, G. Šimić, "Custom Cipher Algorithm for AJAX Requests Protection in Web applications", Proceedings of 52th ETRAN Conference, Belgrade, Serbia, pp: CD, 2008
6 A. Jevremović, M. Veinović, G. Šimić, "Zaštita bežičnih komunikacija korišćenjem sopstvenog šifarskog algoritma", 17. Telecommunications Forum Telfor, Belgrade, Serbia, 2009.
7 A. Jevremović, "Integracija sopstvenih kriptoloških sistema u standardnu računarsko-telekomunikacionu infrastrukturu", Univerzitet Singidunum, Belgrade, Serbia, pp. 1-122, 2011
8 M. Veinović, A. Jevremović, G. Šimić, "Model for Implementation of Custom Cipher and Steganographic Algorithms in Case of Web Image Galery", 16. Telecommunications Forum Telfor, IEEE, Belgrade, Serbia, pp. CD, 2008
9 M. Veinović, A. Jevremović, G. Šimić, "Analysis and Implementation of Custom Cipher Algorithm for IPsec under Linux OS", International Journal of Computer Science and Network Security, IJCSNS, Vol.8 No.7, pp. 80-86, 2008.
10 M. Veinović, A. Jevremović, G. Šimić, "Implementation of Proprietary Cipher Algorithm on Linux Operating System", Singidunum revija, Univerzitet Singidunum, Vol.5 No.1, pp. 92-102, 2008.

Implementation of the encryption system on the application layer is mainly an easy objective in cases where the developers develop complete application protocol, or when they are modifying the source code of the existing one. Otherwise, when it is necessary to protect the enclosed application protocols, this may represent an impossible task. Moreover, it is necessary for users to manage some cryptography function (e.g. the selection of the encryption system, algorithm, the encryption key, etc.), which significantly burdens their work and increases the possibility of errors. An implementation of the protection system at the application level is not reusable for more than one application protocol and it represents another disadvantage of such implementation.

However, it should be noted that for the implementation of a protection system at these levels, in the scenario to achieve maximum performance and safety, it is necessary to have the ability to modify the kernel of operating system.

Implementation of the encryption system on the network or transport layer represents the optimal choice for the aspect of compatibility with a variety of telecommunication infrastructures and the Internet, as well as from the aspect of all application protocols that the device uses. In this case preference is given to the network layer since the encryption function implementation at this level protects[11] the different protocols of the transport layer (TCP, UDP, etc.). Further, *IPsec* protection subsystem at the network layer can be easily used in combination with its custom cipher algorithm. However, it should be noted that for the realization of a system of protection at these levels, it is necessary to have the ability to modify the kernel of operating system in order to achieve maximum performance and safety.

SYSTEM LEVEL IMPLEMENTATION

One of the key issues for the implementation of custom encryption system is the selection of computer system level on which it will be implemented. In general, there are three possible levels of implementation: so called *user space* (in the form of an application or service), implementation at the level of the kernel of operating system and at the hardware level.

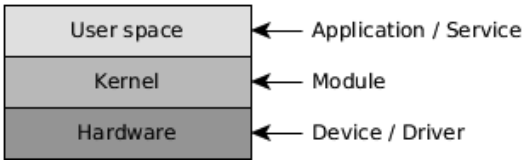


Figure 2: *Levels of implementation of custom encryption system*

Basic advantage of implementation of custom cipher algorithm at the user space is the ability to use a wide range of programming languages, libraries and architecture. Further, such a system is *easy to install* because there is no need for modification of the operating system or hardware. On the other hand, the implementations of custom cipher algorithm at the user space are limited. Routing communication data of other applications and services on encryption system are generally far from simple and often impossible. In addition, the realization of this level will have a negative impact on the performance of the encryption system.

Implementation of custom cipher algorithm at the hardware level may represent a good solution if there is a requirement of high performances and the use of resources that are located outside the computer system. On the other hand, such a realization is usually very

11 M. Šarac, M. Veinović, S. Adamović, D. Radovanović, A. Jevremović, "Analiza sigurnosti SSL saobraćaja u bežičnim računarskim mrežama", XI međunarodni naučno-stručni simpozijum INFOTEH-JAHORINA 2012, Jahorina, Republika Srpska, 2012

expensive. In addition, any changes to the system are much more difficult and expensive to implement than software changes. Finally, the user must have the ability to independently design and produce the desired hardware or he has to have the ability to thoroughly oversee this process if it is run by somebody else. At the hardware level maximum speed can be achieved of encryption and decryption produced via a dedicated crypto processor. Dedicated processor design techniques are well known to everyone. However, only a few countries in the world have the technology for the realization of these processors whose realizations are not trusted by the rest of the world.

Our experience indicates that the kernel of operating system represents optimal place for the implementation of custom cipher algorithm (full list of references are sited in introductory part). It can achieve improved performance due to reduced number of system calls. In addition, the cryptosystem in the core of operating system can easily be paired with the protocols of the transport and network layer as well as data link layer. However, for such an approach it is necessary to have access to the source code of the kernel, which is enabled within the Linux operating system.

COMPUTED AND ABSOLUTE SECURITY

The protection level is one of the first issues that should be determined in the very beginning project phase. There are two possible solutions: the processing encryption systems and absolutely safe encryption systems.

The safety processing ciphering algorithms are designed to use the keys of limited length (usually 128 to 4,096 bits). Due to limited key length breaking the cipher text is possible by trying all possible combinations of bits (keys) to find the corresponding one (total search space of all possible keys). The estimated number of combinations to try to find the used one is $2^{n-1}/2$, where n represents the length of the used key. Breaking of cipher text encrypted with keys longer than 256 bits is practically irrational due a lot of CPU time needed, so these encryption systems are considered efficient. For breaking of cipher texts encrypted by using of commercial ciphering algorithms (*DES, 3DES, AES*, etc.) there is no confidence that the complete cipher key search is necessary. It is suspected that there are shortened ways for that and there is also reasonable suspicion that these shortened procedures are known to those who have designed algorithms listed. It is based on some information published, mainly via the Internet. A particular problem is the use of asymmetric encryption system (RSA) due to the fact that scientifically (mathematically) it has not been proven that there are no shortened procedures for breaking algorithm.

Once designed cipher systems becomes obsolete quickly. The development of processors, computers and networks facilitating faster search of keys and such systems have to be examined and changed after a few years of use. The safety processing encryption systems are been attacked by using weaknesses of computer protocols, built-in backdoors, or human mistakes.

Different of safety processing ciphering algorithms, the content encrypted by using absolutely safe encryption systems cannot be broken, regardless of the amount of processing power engaged for this purpose. More precisely, it is achieved by using unique cipher key (so called *one time pad*). This further implies that the key length must be equal to or greater than the length of a message to be encrypted. Moreover, a new key has to be used for each message. Due to everyday improvement of storage media (more capacity at a reduced cost) it is becoming more realistic that absolutely safe encryption systems can be successfully applied for the protection of real-time communication. For instance, *one time pad* systems can be used for the protection of standard voice-coder systems instead of ordinarily used safety processing ciphering algorithms.

In both cases, regardless of which encryption system is used, there has to be established safety communication channel for exchanging the keys between the sides in communication. The development of special protocols which enable the exchange of secret keys through unsafe channel[12], [13], [14] can be used as alternative way for this purpose. However, according to the published results the performances of such protocols are still unsatisfactory as well as confidence in them. These are the main reasons that they are not used in absolutely safe encryption systems.

A simple and usable-in-practice method for absolutely safe encryption is bitwise processing of message with XOR logical function (exclusive disjunction) in which a bit array that came out of a random number generator is used as a second operand[15] (so called *sequential or Bit-for-bit encryption*). It is well known that such systems are the most resistant to errors in the channel (one false bit in the cipher text affects only one bit decoded incorrectly in an open message), which is important for mobile communications. A precondition for such a system is that both sides have to have the same secret random bit array by the same or greater length than the length of messages to be exchanged. The same simple function (XOR) is used in both of encryption and decryption of a message. Random bit arrays can be segmented and their segments can be indexed so that the same segment will never be used twice.

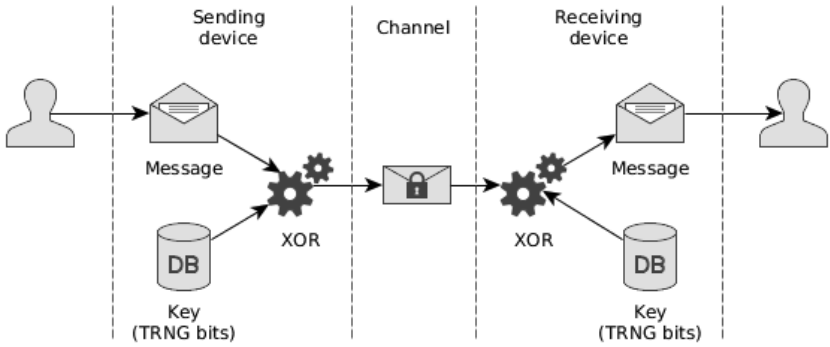


Figure 3: Implementation model for absolutely safe communication

The weakest part of the proposed solution is the necessity of the secret key exchange channel. The second one is the length of secret key - it should be equal to or greater than the total length of all messages to be exchanged within the planned period of use (e.g. one communication session). In case of intensive exchange of voice or video messages, the length of this series can be measured in tens or even hundreds of gigabytes for the planned use period of one month between the only two points that communicate. However, given the level of protection which is thus obtained, the problems that are avoided (connections, exchange session key, etc.) and low CPU requirements, the proposed solution should be put in consideration for practical applications.

12 W. Diffie, M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, pp. 644–654, 1976

13 M. Milosavljević, J. Jovanović, S. Adamović, M. Šarac, A. Jevremović, V. Miškovic, "Protokol za generisanje i razmenu apsolutno tajnih kriptoloških ključeva putem javnih kanala u savremenim računarskim mrežama", Zbornik radova 57. konferencije Etran, Zlatibor, Serbia, 2013

14 A. Jevremović, M. Veinović, G. Šimić, "Modifikacija IKEv2 protokola u cilju izbora radnog tajnog ključa simetričnih šifarskih Sistema", Zbornik radova 53. Etran, Belgrade, Serbia, pp. CD, 2009

15 M. Tatović, S. Adamović, A. Jevremović, M. Milosavljević, "One method for generating uniform random numbers via civil air traffic", Sinteza 2014, Belgrade, Serbia, pp. 606-609, 2014

LINUX & ANDROID

The kernel of Linux operating system is used as the basis for Android devices. This way numerous functions of the Linux operating system can be used in Android devices. In addition, since the code of Linux kernel is publicly available, this core part of operating system can be controlled, modified and extended in order to improve security features. Of course, in the development of security systems the practice is that all components that are not required are removed to simplify the system and to reduce the potential risk of installation of back-doors.

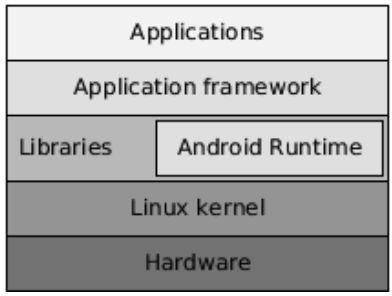


Figure 4: *Android architecture*

Support for *IPsec* protection system already exists in the Linux kernel, as *AH* and *ESP* protocols. Cipher algorithms used in these protocols are also implemented in the kernel, and they can be accessed via the standardized *Cryptographic* API. This means that the user defined cipher algorithm can be implemented as a kernel module and it can be used for communication protection via *IPsec* protection system.

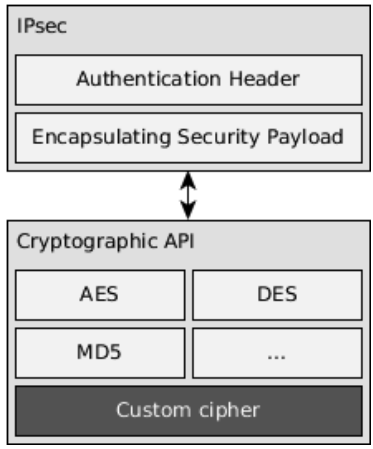


Figure 5: *Model of applying user defined cipher algorithm by using Cryptographic API of Linux kernel*

Another advantage of the implementation of the user defined cipher algorithm as a kernel module is that its exploitation is not limited just for communication protection. It can be used for many other purposes. For instance, it can be used for the protection of file-system (theft

device scenario). Additionally, the algorithm can easily be relocated to the external hardware[16] (a case in which the cipher algorithm acts as a device driver).

TRUSTING TO COMPILER, HARDWARE AND FIRMWARE

After checking the kernel source code and the necessary Android components, making modifications on them by incorporating custom cipher algorithm, the following steps are compiling for the installation on devices to be protected. The first potential problem occurs at the first step, i.e. compiling of the source code. It has to be made on an absolutely clean computer system (or on a system that does not hold undocumented functionality), and using the proven compiler. Otherwise, the back-door functionality can be inserted at this stage and in this way undo all efforts to develop a secure system.

The hardware devices procured on the market are also unreliable. Attaching the "back door" at the hardware level has long been the subject of suspicion of the researchers in this field, and recent discoveries reconfirm such a doubt.[17] Accordingly, the hardware of the device must also be thoroughly checked before use or independently developed. The same method should be followed for all the firmware incorporated in the device.

CONCLUSION

Highly secure systems for communication protection cannot depend on the already built solutions regardless of the fact that their producers published almost all details of their implementation. This paper presents a model for the development of its custom system for secure communication depending on custom encryption algorithms. The basic requirement is that all system components which can affect the safety have to be developed and tested and approved by the authors themselves. Linux/Android platform is proposed as a solution as it has the most of the necessary functions and that complete source code is publicly available.

Cipher algorithms will be firstly incorporated at the telecommunication level as a part of the development of safety network system. Such solution will aggregate particular implementations for each application protocol. More precisely, the proposal includes *IPsec* security extensions as the implementations below the network level which make the use of Internet impossible.

On the computer system, custom cipher algorithm can be implemented in user (application) space, the core of the operating system or at a hardware level. Although the implementation in user space represents the simplest approach, such a realization is difficult to protect the growing number of application protocols. Lowering of performances is also expected. The implementation at a hardware level should be appropriate regarding to the performances and security level, but such an approach is difficult to implement and rigid for modifications. Therefore, the solution presented in the paper proposes building of its custom algorithm in the form of Linux kernel modules.

This paper also analyzes the choice between processing encryption systems and absolutely secured encryption systems. With regard to the possibilities of modern devices based on Android, with the focus on the capacity of modern storage media, absolutely secured encryption systems are partially preferred.

16 M. Saarinen, "Linux for the Information Smuggler", Technical Aspects of Network Centric Warfare, Vol 17, Finnish National Defence College, pp. 228-239, 2004

17 J. Appelbaum, "To Protect And Infect - The Militarization of the Internet", 30C3: 30th Chaos Conference, Hamburg, Germany, 2013

The final problem in the implementation of safety communication device is how to obtain a "clean" platform on which the source code of the cipher algorithm, the core of operating system and other necessary software would be compiled. In addition, the hardware platform on which such software would be deployed should be "clean" – in other words it has to be without "back doors". This is the only way the user has a full control over the system.

ACKNOWLEDGEMENT

Authors of this paper were the participants on the scientific projects - TR32054, III44006, III44007 and ON174008 funded by Ministry of Education, Science and Technology Development Republic of Serbia.

REFERENCES

1. Jevremović., M. Veinović, "IP Security under Linux OS", Proceedings of 50th ETRAN Conference, Belgrade, Serbia, pp. 114-117, 2006.
2. Jevremović, M. Veinović, "IPsec – Analyzing Influence of Cryptographic Algorithm on Lan Networks Traffic", 14. Telecommunications Forum Telfor, IEEE, Belgrade, Serbia, 2006.
3. Jevremović, M. Veinović, G. Šimić, "Custom Cipher Algoritm for AJAX Requests Protection in Web applications", Proceedings of 52th ETRAN Conference, Belgrade, Serbia, pp: CD, 2008.
4. Jevremović, M. Veinović, G. Šimić, "Zaštita bežičnih komunikacija korišćenjem sopstvenog šifarskog algoritma", 17. Telecommunications Forum Telfor, Belgrade, Serbia, 2009.
5. Jevremović, "Integracija sopstvenih kriptoloških sistema u standardnu računarsko-telekomunikacionu infrastrukturu", Univerzitet Singidunum, Belgrade, Serbia, pp. 1-122, 2011.
6. Jevremović, M. Veinović, G. Šimić, "Modifikacija IKEv2 protokola u cilju izbora radnog tajnog ključa simetričnih šifarskih sistema", Zbornik radova 53. konferencije za elektroniku, telekomunikacije, računarstvo, automatiku i nuklearnu tehniku - Etran, Belgrade, Serbia, pp. CD, 2009.
7. Bill Snyder, "Snowden: The NSA planted backdoors in Cisco products", InfoWorld, 2014.
8. J. Appelbaum, "To Protect And Infect - The Militarization of the Internet", 30C3: 30th Chaos Conference, Hamburg, Germany, 2013.
9. M. Veinović, A. Jevremović, G. Šimić, "Analysis and Implementation of Custom Cipher Algorithm for IPsec under Linux OS", International Journal of Computer Science and Network Security, IJCSNS, Vol.8 No.7, pp. 80-86, 2008.
10. M. Milosavljević, J. Jovanović, S. Adamović, M. Šarac, A. Jevremović, V. Miškovic, "Protokol za generisanje i razmenu apsolutno tajnih kriptoloških ključeva putem javnih kanala u savremenim računarskim mrežama", Zbornik radova 57. konferencije za elektroniku, telekomunikacije, računarstvo, automatiku i nuklearnu tehniku - Etran, Zlatibor, Serbia, 2013.
11. M. Tatović, S. Adamović, A. Jevremović, M. Milosavljević, "One method for generating uniform random numbers via civil air traffic", Sinteza 2014, Belgrade, Serbia, pp. 606-609, 2014.
12. M. Saarinen, "Linux for the Information Smuggler", Technical Aspects of Network Centric Warfare, Vol 17, Finnish National Defence College, pp. 228-239, 2004.

13. M. Veinović, A. Jevremović, G. Šimić, "Model for Implementation of Custom Cipher and Steganographic Algorithms in Case of Web Image Gallery", 16. Telecommunications Forum Telfor, IEEE, Belgrade, Serbia, pp. CD, 2008.
14. M. Veinović, A. Jevremović, G. Šimić, "Implementation of Proprietary Cipher Algorithm on Linux Operating System", Singidunum revija, Univerzitet Singidunum, Vol.5 No.1, pp. 92-102, 2008.
15. M. Šarac, M. Veinović, S. Adamović, D. Radovanović, A. Jevremović, "Analiza sigurnosti SSL saobraćaja u bežičnim računarskim mrežama", XI međunarodni naučno-stručni simpozijum INFOTEH-JAHORINA 2012, Jahorina, Republika Srpska, 2012.
16. W. Diffie, M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, pp. 644–654, 1976.

UDC: 343.982.32
351.75:621.397.4

FORENSIC AND LEGAL ASPECTS CONCERNING THE USE OF THE VIDEO SURVEILLANCE SYSTEM IN PROVING CRIMES AND OFFENCES

Milan Gligorijević, PhD[1]
Academy of Criminalistic and Police Studies, Belgrade
Nebojša Jokić[2]
Ministry of the Interior of the Republic of Serbia, CERT Centre
Aleksandar Maksimović[3]
Ministry of the Interior of the Republic of Serbia, CERT Centre

Abstract: The use of modern technical and technological achievements and information technologies represent an essential segment of today's social life. The massive expansion, development and implementation of information and communication systems in all fields provides a real opportunity and possibility to a today's man to respond adequately to the growing civilizational challenges of modern times. One such system is the video surveillance system, conceived and designed with the aim of raising the general level of safety and security of all citizens. Besides its basic purpose, the system can be quite effectively used in detecting and proving different types of crimes. Its forensic aspects in proving criminal acts and offenses, as well as the legal framework for resolving sensitive matters concerning the processing of personal data will be discussed in this paper.

Keywords: information and communication system, video surveillance, detection of crimes and offenses, the processing of personal data

INTRODUCTION

Nowdays, any serious integral system for securing objects, persons and property necessarily implies the existence of video surveillance system. The essential function of the video surveillance system is to provide security status information. Based on this information, the user (security staff or the owner of a facility) is able to organize appropriate measures of protection. Archiving video information on object's security status has multiple purposes in the process of analyzing information on security status of a building, as well as in documenting various incidents. Video surveillance systems are able to timely detect undesirable events in the objects, or record materials, which can be used as evidence of offense or misdemeanor or any other damage. During the process of analysis (cause, criminal act, identification of the participants and the consequences), police which are the most common user of this information, collect and provide relevant evidence for the possible initiation of criminal or misdemeanor proceeding.

1 milan.gligorijevic@mup.gov.rs
2 nebojsa.jokic@mup.gov.rs
3 aleksandar.maksimovic@mup.gov.rs

Video surveillance system is essentially an electronic system for monitoring and recording events and situations in certain area, as well as transmitting signal from the camera to a specific location. [4]

Video surveillance system is not used only in "critical" situations, but also in many regular situations, for instance to control work in premises deal with money (banks, exchange offices); protect customers from theft; monitor vital manufacturing process, loading and unloading of goods, external spaces and outdoor storage and parking, goods in shops and warehouses, the exhibits, entry and exit of vehicles, workers in companies, patients in intensive care, visitors at certain event, etc. Planning and designing video surveillance system is a complex process that has to fit in with the results of the analysis of the security endangered objects, persons or material goods and with all existing specifics, position and purposes of such premise, and also to be fit in with the system technology.

Video surveillance system has been used in protecting facilities for several decades. At first, such systems were too expensive and they were profitable only when concerned to buildings of particular importance or risk. Extremely rapid technological development in recent decades has led to a drastic fall in prices of components in the field of information technologies, so today system of video surveillance is much more accessible and more present in the business world.

Also, it is important to emphasize that video surveillance system has preventive character, in terms of psychological impact on person with potentially bad intentions and deterring person from committing illicit acts. Given that video surveillance system represents a serious investment at first sight; its benefits (prevention of potential damages and efficient monitoring of daily operations) will be seen later as long-term cost effective.

More about the system, its structure, the way of functioning and possibilities of use in the field of gathering evidence for the prosecution of different types of crimes and misdemenoers, will be given bellow.

DESIGN, STRUCTURE AND FUNCTIONING OF VIDEO SURVEILLANCE SYSTEM

Designing video surveillance system is a complex process that has to be aligned with the analysis of the status of security of endangered facilities, persons or material goods and with all existing specifics, locations and purposes of such objects, as well as with the system technology. Such a process certainly requires knowledge of the system features which should meet the requirements of the use.

When selecting a video surveillance security system, it is extremely important to be familiar with the security problems related to objects, or make a quality assessment of the threat[5]. In addition, it is necessary to know the user's wishes and possibilities in terms of quality, communication and system size. All this can be considered as a starting point in the design of video surveillance systems.

Video surveillance system consists of the components given bellow:

1. Indoor and outdoor* surveillance *cameras (depending on the geometry/shape of a facility, possible approaches to a facility, arrangement of rooms to be monitored, etc.);

4 Ratcliffe, J., *Video surveillance of public places*, Washington, DS: U.S. Department of Justice, Offce of Community Oriented Policing Services, 2006.
5 Lomell, H. M., *Targeting the unwanted: Video surveillance and categorical exclusion in Oslo*, Norway. *Surveillance & Society, 2* (2/3), 2004.

2. Suitable camera lens (with manual or automatic adjustment of the lens aperture/lens opening);

3. Cable system for video signal transmission;

4. Switch, router, server and similar devices for connecting components;

5. Central devices (for processing and archiving images obtained from the camera);

6. Monitor to display images and monitoring;

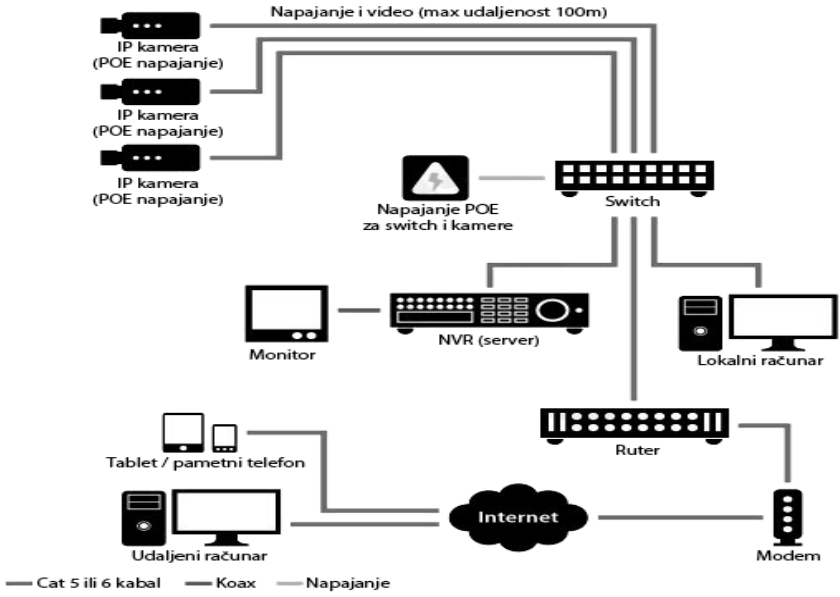


Figure1. *Schematic diagram of the structure of the video surveillance system*

Necessary preconditions for the functioning of this system are as follows:

- Minimum one IP camera (or an analog camera with a video encoder - video server)
- Computer network
- Switch
- PC for monitoring, and
- Software for recording and storage materials.

As for IP video surveillance, digitalization of the signal is the process performed in the camera itself. Therefore, the signal is sent to the recorder (NVR - Network video recorder - server) in digital format (video stream). Video recorder performs additional processing of video signals to perform the storage and distribution to other media. (Figure 1) The fact that the transmission of signal is performed in a digital format, led to a unique and logical conclusion that during the transfer, the signal cannot be lost, such as the case with analogue video surveillance. Since the process of digitization is performed in the camera itself, engaging the processor in recorder or server is minimized, which practically allows the storage and distribution of images from multiple cameras and even in a higher resolution, which is not the case with analogue transmission.

Also, if we perceive the process of system installation, IP systems are far more flexible than analog ones. Classic computer networks which can contain nodes and backbone[6] links are used for establishing connections between IP cameras and the recorder. Computer network allows users of video surveillance systems to distribute and share data and information, and other computing resources. The advantage of such system is that only one copy of the data should be stored on computer (server), and together with hardware and software resources should serve others.[7] Switches whose task is to direct the network packets to certain addresses are used to connect computers in a computer network. Computer-server, on which the software is installed to capture and process images, can be used for recording. Such systems allow progressive integration of different security systems such as access control system, alarm system, etc. In case there is no need to extend the system, NVR recorders or servers optimized for a number of cameras in the appropriate resolution, is certainly a good choice.

If there is a need for high-quality images with high content of fine details, and for systems with a large number of cameras, where should be stored images in large periods of time, IP video surveillance with megapixel cameras installed is a great choice.

SPECIFIC ISSUES AND LEGAL FRAMEWORK TO USE VIDEO SURVEILLANCE SYSTEM IN THE PROSECUTION OF CRIMES AND MISDEMEANORS

Using video surveillance is regulated by laws and by-laws, but also by the international documents related to the protection of personal data, policing, criminal procedure, special laws concerning video surveillance and other regulations governing safety in some specific places (e.g. banks, stadiums, etc.) [8].

European regulations mainly regulate privacy protection issues and processing of data collected by video surveillance system[9]. The most important European documents in this area are:

1. European *Convention for the Protection* of *Human Rights* and *Fundamental Freedoms,*

2. European *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and*

3. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In this respect, despite great political pressure exerted on national legislations to be harmonized with European standards, still many European countries have different regulations governing the powers and directions for video surveillance use.

In this field, worth mentioning is surely British concept of protection, security and safety of citizens and property which is primarily based on video surveillance, and which beside other regulations has a special regulation on the implementation of video surveillance stipulated by

6 Backbone network or the network backbone is part of a computer network infrastructure that connects different parts of the network, providing a path for the exchange of information between different LAN or subnets.

7 Ranđelović, D., *Upravljanje informacionim sistemima i njihova zaštita,* the edition of the monograph, the Academy of Criminalistic and Police Studies, Belgrade, 2014

8 Kovačević-Lepojević, M., Žunić-Pavlović, V., *Primena video nadzora u kontroli kriminala*, Faculty of Special Education and Rehabilitation, University of Belgrade, Belgrade, 2012

9 Hempel, L. & Topher, E., *CCTV in Europe,* Berlin: Centre for Technology and Society, 2004.

the Commissioner for Information. Also, Spain has adopted instructions on video surveillance of security services in a public space; Denmark has adopted a Rule Book which strictly prohibits private companies to survey public space and limits video surveillance use in many other ways[10]. Some countries, such as Germany, Luxembourg, Belgium, Finland, Greece and Italy have amended their existing laws on protecting personal data with new provisions concerning video surveillance. New laws stipulate the purposes and conditions of video surveillance use, the way of informing citizens, the quality of video recording, storage and processing data, etc. In accordance with the principle of transparency, Norway, France and Sweden have introduced procedures for the registration of video surveillance system.

Republic of Serbia has introduced innovations in its legislation concerning the use of video surveillance. The Law on Personal Data Protection regulates the conditions for collecting and processing personal data, the rights of an individual and the protection of the rights of persons whose data are collected and processed, limitations in the field of protecting personal data, the procedure in state authority competent to protect personal data, data security, keeping records, extracting data from Serbian state authorities and the implementation of the mentioned Act. Given that Commissioner for Information of Public Importance and Personal Data Processing is aware of the lack of provisions regarding video surveillance, it is necessary to develop a separate law on video surveillance, or within existing Law on Personal Data Protection, to enter detailed provisions governing the use of video surveillance, as foreseen by the Personal Data Protection Strategy.

The use of video surveillance in public places in Serbia is indirectly determined by specific regulations. In order to improve the functioning of the video surveillance system of roads and intersections in Belgrade, in accordance with the Law on Road Traffic Safety, the **obligatory Instruction on conditions of use and maintenance of video surveillance systems of urban roads and intersections in the city of Belgrade** was adopted[11]**.** These provisions govern the right of data access, the procedures of downloading images from the archives, the responsibility of the Belgrade Police organizational units and specify the manner of maintaining the system. The Law on Prevention of Violence and Misbehavior at Sports Events stipulates that the organizer is obliged to provide technical equipment for monitoring and recording the entrance as well as behavior of people in the sports facility. According to the Law on Games of Chance, the organizer of games of chance in betting shops, casinos, etc., is obliged to ensure continuous audio-video control of tables and gaming machine, entry and exit of the playrooms, protect players and visitors, and to store the documentation of continuous video surveillance for at least ten days. Also, according to the Law on Protection of the state border, for the purpose of keeping records, the border police of the Ministry of Interior are authorized to collect personal information by using different technical means, including the use of video surveillance systems.

In Serbia, there are no specific regulations governing the use of video surveillance in schools. According to the Law on the Foundations of the Education System, each school is required to prescribe measures, methods and procedures to protect the safety of students during their stay at the facility or any kind of activities organized by school, but there are no recommendations for schools to introduce a system of video surveillance as one of the measure of protection. In practice, the decision to introduce video surveillance in the school brings the school board on a proposal given by the principal and with the consent of the parents' council and student parliament. The emphasis is on the implementation of video surveillance and the way of financing, but generally less attention is paid to ethical and security issues.

10 Andenas, M. & Zleptnig, S., *Surveillance and data protection: Regulatory approaches in the EU and Member States*, European Business Law Review, 2003

11 *Obavezna instrukcija o uslovima korišćenja i održavanja sistema video nadzora gradskih saobraćajnica i raskrsnica za grad Beograd*, Ministry of Interior, 2015.

As recommended by international regulations (provisions concerning protection and safety of prisoners), video surveillance should be used in institutions for execution of criminal sanctions as additional tool of the so-called dynamic security which insists on developing positive relations between prisoners and staff[12].

In the Directorate for Execution of Criminal Sanctions of the Ministry of Justice of the Republic of Serbia, video surveillance system is stipulated by the Rule Book on Arms and Equipment of Security Officers, but only as accompanying part of electronic equipment such as alarm systems, identification systems, etc. The conditions of use are not specifically regulated by the regulations relating to the functioning of the Directorate for Execution of Criminal Sanctions of the Republic of Serbia, but the mode of use shall be decided on the level of each institution individually.

Based on the observations made by the Commissioner for information of public importance, concerning the unlawful personal data processing in the Ministry of Interior through a system of video surveillance (recording traffic participants using the so-called "Interceptor", audio and video surveillance of the police officers during th execution of their tasks and duties within police authorities, etc.), this regarding we started defining the legal framework and designing the legal norms in the context of the draft law on records and data processing at the Ministry of Interior of the Republic of Serbia. In this way, for the first time, in a clear, precise and transparent manner, processing personal data through video surveillance system at the MOI, a set of personal data to be processed, and the very purpose of data processing are regulated. After the adoption of the aforementioned Act (expected soon) and the new Law on Police, the scope of video surveillance use in the Ministry of the Interior will receive full legal basis.

POSSIBILITIES OF USING VIDEO SURVEILLANCE SYSTEM TO PROVIDE EVIDENCE FOR PROSECUTING CRIMES AND MISDEMENEORS

The development of modern innovative technologies has caused the change in the method/way of committing criminal offenses, and therefore the development of security technology to control crime. For these reasons, the use of video surveillance system in controlling crime, its prevention and collection of evidence necessary for the prosecution of crimes and offenses is of the utmost importance. The video surveillance system can monitor and record the commission of a crime in real time thus providing evidence. Video recording is documented in more qualitative way, not only the entire situation and structure of the crime scene, location of evidence, their connection and relationship with other conditions and circumstances, but also the activities undertaken during criminal investigations and inspections of the scene[13]. Video can display one or more relevant facts that are the subject of evidence, scene of the crime, the perpetrator or the flow of the offense. Beside the use of video recordings at the crime scene, modern technology allows the use of video surveillance for prevention. One of the instruments of global security policy is a system of video surveillance to be applied within the framework of the strategy for preventing crime in conjunction with other security measures in order to achieve the most effective results.

12 Recommendation Rec (2003) 23 of the Committee of Ministers to member states on the management by prison administrations of life-sentence and other long-term prisoners, Council of Europe, 2003
13 Žarković, M.: *Krivičnoprocesni i kriminalistički aspekti uviđaja na mestu događaja*; Belgrade 2005.

Video surveillance for monitoring[14]- technology for controlling communications and the Internet, etc.,[15] have been used for the crime control and crime prevention. Monitoring system in the context of methods of preventing and combating crimes could be defined as a system for monitoring, supervising or controlling (surveillance/observation system), which continuously or periodically collects and analyzes data and performs the collection and analysis of information on criminal activities of individuals or group of persons, on the basis of which can be made conclusions on how to implement a certain action in relation to the expected results[16]. The technical supervision includes automatic monitoring of traffic. In Finland, police have found wide use of automatic traffic control, mainly for monitoring compliance with speed limits. Signs warn motorists in advance of the existence of automatic speed cameras.[17]

Video surveillance can be used in the implementation of many operational - tactical and special evidentiary actions. Depending on the object of surveillance, as well as the manner of implementing, can be distinguished:

- Optical - visual, video observation (surveillance, monitoring);
- Acoustics - sound, verbal, audio observation (surveillance, monitoring);
- Optical - acoustic observation (surveillance, monitoring);
- Observation of non-verbal communication (letters, telegrams, e-mail, SMS messages and other forms of electronic information exchange);
- Observation of an electronic locating in space (GPS, mobile phones, etc.), Marinkovic, 2010: 511[18]

An investigation with the help of video surveillance system[19] (hereinafter after forensics video investigations) has become a very powerful and irreplaceable weapon to fight crime and has a special role in the criminal proceedings. Forensic video analysis can be used for collecting information and finding out delinquent behavior. During forensic video investigation, relevant information from video images can be viewed and collected as evidence. Based on the video, the time, place, route, region, area of the offense can be determined but further police work accelerated and improved. In the context of forensic video investigation, there is a "*trend methods*", which means that material evidence and traces of the crime can be found and provided under video surveillance.[20] Forensic video analysis should be an integral part of the criminal-forensic processing of the crime scene to achieve positive results of the investigation.

Forensic data collected by video surveillance should be used under special conditions and stipulated by regulations on the protection of personal data, which are in accordance with EU. The Charter for a democratic use of video surveillance regulates the operation and development of public video surveillance system managed by public, national, regional or local authorities. The rules stipulated by the Charter should also be applied to private video

14 Monitoring, tracking or monitoring of technical devices and systems over time is called monitoring.
15 The Police Act of Finland stipulates conditions for the technical monitoring. The police have the right to carry out technical surveillance in a public place in order to maintain public order and peace prevent offenses, identified suspects for criminal offenses.
16 Popara, V., Protić, G., Žarković, I.: *Dokazi i operativni značaj monitoringa tehničkim sredstvima u realizaciji kriminalističkih poslova*; Conference of Science, Position and Perspectives of Criminalistic, Criminology and Security Studies in sovereign conditions, Sarajevo, 2013, 172-186
17 Popara, V., Protić, G., Žarković, I.: *Dokazi i operativni značaj monitoringa tehničkim sredstvima u realizaciji kriminalističkih poslova*; Conference of Science, Position and Perspectives of Criminalistic, Criminology and Security Studies in sovereign conditions, Sarajevo, 2013, 172-186
18 Marinković, D. (2010). *Suzbijanje organizovanog kriminala – specijalne istražne metode*. Novi Sad: Prometej
19 *Video crime scene investigation*
20 Xu, Feng.: *Method research and practical application of video investigation*, Thematic conference proceedings of international significance, Tom 1, Volume 1., pp. 443-449, KPA Belgrade 2014.

surveillance systems, particularly in cases when their use and the data can be made available to the authorities. [21]

Relevance and authenticity of a video is a precondition for accepting video footage as evidence. One of the conditions to use video footage as evidence in criminal and misdemeanor proceedings is that the video is made in accordance with the law. Video footage can be made by the police or other person having no status of officials. The authenticity of the video will be determined by an expert opinion. The question of the credibility of the photos and video footage will be resolved by applying analytical photogrammetry to reconstruct perspective beam in space. This way, options of specially developed computer program would allow reliable authentication of footage and details of the situation at the scene. [22]

Video control methods applied in specific cases, as well as their results have shown that ability of police to combat crime can be improved by using information and communication technologies, and forensic video investigations can empower efficiency and effectiveness of policing.[23]

CCTV (CLOSE-CIRCUIT TELEVISION)

There are three types of situation where the program has been found to be effective in crime prevention:

- Policing in the community;
- Video surveillance CCTV
- Improved street lighting [24]

CCTV (*Closed-Circuit Television*) video surveillance represents the British national symbol of situation crime prevention. In addition to the undeniable role of the CCTV system in the role of crime prevention, the video surveillance system can contribute to detecting and identifying the offender or offense. Video footage can help in the identification of potential witnesses whose statements can contribute to solving criminal offense.

CCTV systems in public places are widely used in the UK, US and many other Western countries, such as Germany, Norway, Sweden, Austria, etc. Raising the efficiency of prevention programs with the promotion of evidence-based approaches is one of six guiding principles of the United Nations Crime Prevention. The use of CCTV system helps in crime prevention, primarily in the field of property offenses as well as criminal acts and offenses in public places. Two following elements are essential to make the process of crime prevention successful.

1. The perpetrator should be aware of cameras;

2. Potential perpetrator of a criminal offense or misdemeanor should be aware that the video represents proof and possibility of his/her recognition and subsequent retrieval and arrests. [25]

British criminologists believe that video surveillance systems can significantly contribute to crime prevention because they enable: detection of perpetrators at the time of the offense or later; reducing the time of committing a crime, enhancing the natural control, improving

21 The Charter for a Democratic Use of Video Surveillance, European forum for urban security
22 Žarković, M.,Bjelovuk. I.; Kesić, T.: *Kriminalističko postupanje na mestu događaja i kredibilitet naučnih dokaza***.** Belgrade: the Academy of Criminalistic and Police Studies, 2012.
23 Xu, Feng.: 2014., op. cit, pp. 443-449
24 Welsh, C., B.: *Evidence-based crime prevention: scientific basis, trends, results and implications for Canada*; Research report: 2007-1
25 Ratcliffe, J., 2006.

the performance of physical security, strengthening social cohesion, raising prudence, reinforcing the fear of public shame, stimulating developments in the areas covered by video surveillance and increase in reporting of cases to the police. [26]

The conclusion of most evaluation is that this measure gives better results when it comes to the prevention of crimes against property (especially vehicle safety), as well as improving security in public transport and traffic in general.

The positive effects of the use of video surveillance systems are:

- Deterring perpetrators – giving up from committing the offense;
- Early detection of the perpetrator;
- Alerting the perpetrator and intervention teams;
- Easy access video footage necessary for forensic investigation ;
- Identification of the perpetrator (identifying familiar face in 130 pix / m resolution, the identification of unknown persons in 330 pix / m resolution);
- Digital recording [27] in real time (live image).

USE OF INNOVATIVE FORENSIC TECHNOLOGY - VIDEO SURVEILLANCE SYSTEM

To identify unknown offenders and misdemeanors previously recorded by surveillance video cameras can be used methods of 3D photogrammetric anthropology[28] and 3D facial reconstruction[29]. These methods are applied in forensic investigation (mostly robbery or other similar crimes) in the process of identification of unknown and masked perpetrators.

Simply applying of these methods enables the measuring (of certain parts of a body) and reconstructing events. On the basis of the camerawork, it is possible to determine the height of visible silhouettes of an unknown perpetrator using a 3D reconstruction forensic method. The height of an unknown perpetrator is measured using a 3D human-like model (virtual model) to which it is possible to change the height, rotate all the important positions of joints in the body. By changing the height and position of the joints, it is possible to put 3D model of a human skeleton on a 3D virtual scene, in the same position and attitude of the body seen by the video surveillance camera. [30]

To perform forensic identification and find suspects in the mass are used television cameras and software that search videos in low, then in high resolution. Thereafter, the software determines the size and position of the person in regards to the camera and compares the data from the database. It is extremely important that the technical quality of the video (resolution and format) be at a satisfactory level and be able to identify unknown perpetrators. Recognition and face detection software is suitable for public places, border crossings, airports, stadiums, and military and infrastructure facilities of importance.

Axxon Face Intellect integrated Module is an integrated module for face recognition used to identify individuals automatically based on video clips. It automatically performs detecting and recording of Person's image, and compares it within the existing data basis for obtaining a

26 Kovačević-Lepojević, M.; Žunić-Pavlović, V.: Belgrade 2012.
27 Kovačević-Lepojević, M., Žunić-Pavlović, V., *Mere javnog nadzora u službi prevencije krimi*nala, Faculty of Special Education and Rehabilitation, University of Belgrade, Belgrade
28 Based on the photo of the perpetrator, anthropological points of particular parts of the body are measured based on which are produced virtual models (dolls) that are compared with the video and then the estimation based on the identity of the seven levels of probability is performed
293D face reconstruction is a method using the appropriate software to reconstruct a person's face look, facial bones, and the head: skull, an eye part, jaw and other immutable characteristics of persons.
30 http://www.forenzika.com/video1.htm

positive person's identification. This system enables real-time notification of recognition and other events. Using this module, after the identification of the person who is already in the database of the persons under investigation, the operator receives all available information and informs the police. [31] The module for face recognition is most commonly used with the system for access control.

Modern technology allows the use of infrared camera recording techniques used for secret recording with the aim of identifying, since the heat of the human body represents the individual characteristics of each individual.

Despite the fact that video surveillance is of the utmost importance for preventing and detecting crimes, it also finds its role in road safety. In this context, there are systems that control the traffic flow, identify traffic policy violations and recognize the license plates of vehicles in motion. Unlike the basic system for motion detection (which trigger sensor camera), systems for identifying the problems are software programs that interpret video footage from CCTV cameras. The program attempts to identify problems such as potential robberies or street fights. [32]

Axxon Intellect Auto Module enables successful monitoring, controlling and managing of public traffic. By using this module, it is possible to identify license plates, perform traffic control and search of certain vehicles; automatic enforcement of speed limits across photo / video; automatic implementation of punishing running a red light over photo / video; to collect traffic data. The system for license plate recognition performs recording of vehicles, directs the movement of vehicles, and records the license plate of the vehicle in motion, after which it is compared with the data from the database[33]. Thanks to existing systems, the traffic safety can be improved, video footage can be browsed and searched or it can be used as valid evidence.

CONCLUSION

In accordance with the requirements of modern methods of committing crimes and misdemeanors, forensics should develop, promote and apply appropriate methods to be used during the criminal investigation and forensic processing of criminal events, as well as perform testing and analysis of material evidence in forensic laboratories. Everyday technology development leads to improving techniques, systems and devices. Using video surveillance system will improve the operative police work, and thus the level of detection and prevention of crimes and misdemeanors, and their sanctions. The Court can base a judgment on evidence emerged as a result of video surveillance in public places. Establishing a system of video surveillance in public places will enable faster police response with the necessary powers and resources, taking measures and actions aimed at preventing the commission of offenses and misdemeanors. Video footage can help police to reconstruct events and find the offenders, but also create conditions for preventive action. Also, this system will promote cooperation with the local community and thereby the effective work of the police in dealing with security issues, with the aim of increasing personal and property security of the citizens. The video surveillance system has an important role in the prevention of crime, and as such, it should be applied respecting the rights to privacy and protection of personal data. In this domain, bearing in mind all the details pointed out in the context of our paper, we believe that it clearly and unambiguously points to the justification of the existence and use of video surveillance in proving criminal acts and misdemeanors. Nowadays, the safety of people and property is

31 http://www.axxonsoft.com/rs/integrated_security_solutions/face_recognition/
32 Ratcliffe, J., *Video surveillance of public places*, Washington, DS: U.S. Department of Justice, Office of Community Oriented Policing Services, 2006.
33 http://www.axxonsoft.com/rs/integrated_security_solutions/lpr/

one of the key pillars of the existence and survival of a society, and as such almost priceless. Of course, all of this will be meaningful as long as people operate within a legal framework and regulations, on which one comfortable and modern country should be based.

REFERENCES

1. Andenas, M. & Zleptnig, S., *Surveillance and data protection: Regulatory approaches in the EU and Member States*, European Business Law Review,2003.
2. Hempel, L. & Topher, E., *CCTV in Europe.* Berlin: Centre for Technology and Society, 2004.
3. Kovačević-Lepojević, M., Žunić-Pavlović, V., *Primena video nadzora u kontroli kriminala*, Fakultet za specijalnu edukaciju i rehabilitaciju, Univerzitet u Beogradu, Beograd, 2012.
4. Kovačević-Lepojević, M., Žunić-Pavlović, V.: *Mere javnog nadzora u službi prevencije kriminala*, Fakultet za specijalnu edukaciju i rehabilitaciju, Univerzitet u Beogradu, Beograd.
5. Lomell, H. M., *Targeting the unwanted: Video surveillance and categorical exclusion in Oslo*, Norway. *Surveillance & Society, 2* (2/3), 2004.
6. Manojlović, Z.: Pravni okvir za primenu video nadzora, Br.11/14.Narodna skupština, Republika Srbija
7. Marinković, D. (2010). Suzbijanje organizovanog kriminala – specijalne istražne metode. Novi Sad: Prometej
8. *Obavezna instrukcija o uslovima korišćenja i održavanja sistema video nadzora gradskih saobraćajnica i raskrsnica za grad Beograd*, Ministarstvo unutrašnjih poslova, 2015.
9. Podrški, F..; Tršinski, S.; Kancir, K.: *Prijedlog unapređenja rada policije uvođenjem videonadzora javnih prostora*, Casopis Policija I sigurnost (Zagreb), godina 17. (2008), broj 3-4, str. 243-253
10. Popara, V., Protić, G., Žarković, I.: *Dokazi i operativni značaj monitoringa tehničkim sredstvima u realizaciji kriminalističkih poslova*, Znanstvena konferencija, Mesto i perspektive kriminalistike, kriminologije i sigurnosnih studija u suverenim uvjetima, Sarajevo, 2013., 172-186.
11. *Preporuka Komiteta ministara državama članicama o tretmanu zatvorenika koji izdržavaju doživotne i druge dugogodišnje kazne od strane zatvorskih uprava*, Savet Evrope, br. 23., 2003.
12. Ranđelović, D., *Upravljanje informacionim sistemima i njihova zaštita,* Edicija monografije, Kriminalističko-policijska akademija, Beograd, 2014.
13. Ratcliffe, J., *Video surveillance of public places*, Washington, DS: U.S. Department of Justice, Offce of Community Oriented Policing Services, 2006.
14. The Charter for a Democratic Use of Video Surveillance, European forum for urban security
15. United Nations Office on Drug and Crime (UNODC), United Nations Human Settlements Programme (UN-HABITAT); Crime prevention assessment tool; Criminal justice assessement toolkit; United Nations, New York, 2009.
16. Welsh, C., B.: Evidence-based crime prevention: scientific basis, trends, results and implications for Canada; Research report: 2007-1
17. Xu, Feng: *Method research and practical application of video inestigation*, Thematic conference proceedings of international significance, Tom 1, Volume 1., pp. 443-449, KPA Belgrade 2014.
18. Žarković, M., Bjelovuk. I.; Kesić, T.: *Kriminalističko postupanje na mestu događaja i kredibilitet naučnih dokaza*, Beograd: Kriminalističko-policijska akademija, 2012.
19. Žarković, M.: *Krivičnoprocesni i kriminalistički aspekti uviđaja na mestu događaja*, Beograd 2005.
20. http://www.forenzika.com/video1.htm
21. http://www.cadzone.com/crime-zone
22. http://www.axxonsoft.com/rs/integrated_security_solutions/face_recognition/

UDC: 004.7.056
355::004

SECURITY RISKS ON SOCIAL NETWORKING WEBSITES

Dejan Vuletić, PhD[1]
Jovanka Šaranović, PhD
Ministry of Defence of the Republic of Serbia, Strategic Research Institute

Abstract: This paper aims to provide a useful introduction to security risks in the area of social networking websites (social networks). A large number of users and the huge number of interactions are suitable for the rapid spread of malicious programs and spam, privacy breaches, identity abuses, frauds and other threats. This paper emphasizes the benefits of a safe and well-informed use of social networking websites. The paper presents the basic elements of the Guidelines for the use of social networks in the state administration, the autonomous province and local self-government in Republic of Serbia. The final part of the paper contains the consideration of social networking websites in military sector.

Keywords: social networking websites, users, security risks, public sector, army.

INTRODUCTION

Following a brief history of the Internet, we can see the development of a large number of virtual communities and groups around the world. With the appearance of the Internet, these communities in a very short time became truly global. Virtual communities are created with the advent of the Internet and new forms of communication, due to the basic need of the people for association, assembly and communication.

The advantage of communication innovation was first noticed by the academic population, leading to the establishment of the first social networks that were originally closed. The ease of use and the emergence of personalization features for profiles on portals, allowed users to present themselves, their interests, aspirations, thoughts, hobbies, etc.

The development of information technology has changed the way people communicate with each other, whereby in this communication mediated by computers and the Internet, as a global worldwide network. The most obvious sign of these changes is the creation of a fully interactive communication environment in a computer-mediated communication, created thanks to the flexibility of today's information technology. Distribution of this environment has created a completely new social environment, popularly called cyberspace. This social environment is a fertile ground for the creation of new social ties. Creating interactive media has enabled both individuals and community groups to direct discussions around common interests. In social environments, information is the basic medium of exchange that is available to the individual to build his/her cyber identity. Therefore, the information becomes a means of self-presentation and emotional presentation of the individual.[2]

1 E-mail: dejan.vuletic@mod.gov.rs.
2 Rheingold H., *The Virtual Community: homesteading on the electronic frontier.* 1993. http://www.rheingold.com/vc/book/

ABOUT SOCIAL NETWORKS

Online Social Networks or Social Networking Sites (SNSs) are one of the most remarkable technological phenomena of the 21st century.[3] Since the commercial success of an SNS depends heavily on the number of users it attracts, there is pressure on SNS providers to encourage design and behaviour which increase the number of users and their connections. Sociologically, the natural human desire to connect with others, combined with the multiplying effects of Social Network (SN) technology, can make users less discriminating in accepting "friend requests". Users are often not aware of the size or nature of the audience accessing their profile data, and the sense of intimacy created by being among digital "friends" often leads to disclosures which are not appropriate to a public forum. Such commercial and social pressures have led to a number of privacy and security risks for SN members.

Andreas Kaplan and Michael Haenlein define social media as a group of Internet applications that are built on the ideological and technological foundations of Web 2.0 technologies that enable the creation and exchange of user-generated content. Social media are media for social interaction and represent a kind of tools that go beyond the sphere of social communication.[4]

Bruce Lindsay, an analyst with the US Congressional Research Service (CRS) defines the social network as well as Internet applications as means allowing people to communicate and share resources and information.[5] Nicole Ellison and Danah Boyd define social network sites as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system.[6]

Social network is a term for a form of human interaction in which through existing acquaintances meets new people to achieve social or business contacts. Web social networking sites allow users to meet new individuals from anywhere in the world without the need for actual physical contact. On the Internet, one can find several different social networks that offer different levels of interaction between the user's networks, depending on the amount of personal information that the user is sharing. The most popular networks of this type include Facebook, MySpace, Twitter and LinkedIn. On these social networks, it is necessary to create user profiles whereby requiring personal, sometimes sensitive information.[7]

Social network is possible to define as a web service that allows individuals to create a public (all users have access) or limited (only certain users have access to) personal profile in the system, create a list of acquaintances, browse and search list of acquaintances and others.[8]

The defining characteristics of an SNS are:[9]

- tools for posting personal data into a person's "profile" and user-created content linked to a person's interests and personal life,

- tools for personalised, socially-focused interactions, based around the profile (e.g. recommendations, discussion, blogging, organisation of offline social events, reports of events),

3 Hogben G., *Security Issues and Recommendations for Online Social Networks*, European Union Agency for Network and Information Security (ENISA), Heraklion (Greece), 2007, p. 2.
4 Kaplan A., Haenlein M., *Users of the world, unite! The challenges and opportunities of social media*, Business Horizons, Vol. 53, Issue 1. Kelley School of Business, Indiana University, 2010, p. 61.
5 Lindsay B., *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations*, *CRS Report for Congress*, Congressional Research Service, 2011, p. 1.
6 Ellison N., Boyd D., *Social Network Sites: Definition, History, and Scholarship*, Journal of Computer-Mediated Communication 13, The Pennsylvania State University, 2008, p. 211.
7 *Sigurnosni rizici društvenih mreža*, Hrvatska Akademska Istraživačka mreža – CARNet, Zagreb, 2009, p. 1.
8 *Ibid*, p. 5.
9 Hogben G., *op.cit*, p. 5.

- tools for defining social relationships which determine who has access to data available on SNSs and who can communicate with whom and how.

SNSs may be seen as informal but all-embracing identity management tools, defining access to user-created content via social relationships. The value of SNSs lies not just in the content provided (which is group-specific), but in its replication in electronic form of the web of human relationships and trust connections.

The success of some social networks depends on the number of users who can use functions that the network offers. However, with the number of users of a social network increasing, the financial value of the social network is growing, which allows the owner of the network expansion of marketing solutions available on the social network.[10]

Being a user of social networks has certain advantages such as a sense of connection with other individuals, meeting like-minded, new way to share life experiences and scientific discoveries, and controlling the amount of personal information that will be displayed on a social network (which in other forms of social media, such as blogs, is not possible). Ability to manage the amount of personal information on a social network is certainly an advantage, because the user chooses what personal information to reveal and thereby protect their privacy. Users are often not aware of the number of individuals who have access to their personal information. User data are often not adequately protected, resulting in security incidents occurrence and abuse of personal data. Social networks are becoming a worldwide phenomenon. Social networks provide users with an easier way of communication, the opportunity to meet new people and exchange of data. The original social network on the Internet did not have a large number of functions, so the number of security incidents was minimal.[11]

The success and popularity of some social networks depend on adapting to users' needs, as well as setting up of new technologies in order to attract new customers and retain existing ones. Some social networks have achieved great success when it comes to the number of users because of the ability to quickly adapt.[12]

THREATS IN SOCIAL NETWORKS

Communication on social networks has many advantages, but carries with it certain risks. Attackers may compromise the privacy of users in many ways. Most social network users inadvertently reveal much information to attackers. In order to start new friendships with strangers, users reveal personal and sometimes sensitive information, which in some cases can pose a security risk. It is believed that the greatest damage to the users of a social network can cause programs by unknown authors containing personal questions that the user should respond. Unaware of the danger of such programs, they are forwarded to users in the list of friends, who again after completing the programs are sent to users from the list of friends, and so on.[13]

Fake profiles are not required to have a malicious effect, however, if it is their purpose, can cause considerable damage to persons whose identity is used. The risks of fake profiles are: damage to the reputation of individuals, blackmailing individual, use of false profile to incite other users to disclose personal and confidential information and marketing activities through fake profiles.

10 *Sigurnosni rizici društvenih mreža*, *op.cit.*, p. 1.
11 *Ibid*, p. 5.
12 *Ibid*, pp. 9–19.
13 *Ibid.*, pp. 9–19.

Cyberbullying is a term used to describe the harm to another individual by means of technology, usually using the mobile phone or through the Internet. Usually there is a modified multimedia (photos, videos, etc.) that aim to humiliate the individual, and degrading messages and comments on someone's user profile.

The best-known security flaw on Facebook is caused by improper handling ActiveX controls for uploading photos (Facebook Photo Uploader) on the user's profile. When one tries to upload photos to the profile, he/she is given a warning that it is necessary to incorporate an additional ActiveX control in order to upload the desired photos. If the user has agreed to install a malicious ActiveX control on his/her computer, there is a possibility that an attacker takes control of the user's computer, and executes arbitrary code. This failure was resolved in a short period of time.

Also, there have been several cases on Facebook where an unknown attacker managed to get the users' names and passwords for specific members, and thus compromise the privacy of the data stored in the profiles. Customer safety has also been severely compromised by the appearance of worms Net-Worm.Win32.Koobface.b. It is known that the worm spreads via spam, and modifications to Facebook resulted in automatically sending spam messages to users on a compromised account's friend list.

The dialog box appears on the screen, telling the user to install Flash program on the computer to stream media content, which then infects the user's computer with the worm Koobface. The attacker will then use the infected computer to further spread malicious software or carry out other forms of attack.

Among the best known security vulnerabilities on the network Twitter is a flow relating to allowing the execution of certain code on someone's profile. The mentioned security flaw is used by a worm named "StalkDaily". The worm "StalkDaily" quickly expanded on Twitter. The user could infect profile simply by viewing the profile of another user who is infected with malicious software.

Also, one of the attacks on the Twitter is caused by insufficiently good authentication to the network. A hacker named "Hacker Croll" was able to detect the user name and password of an administrator of the Twitter, and was able to endanger the safety of millions of users. A hacker broke into the mailbox of the administrator and then found the username and password for Twitter. As evidence for the above mentioned actions, the hacker provided a screenshot of the administrator's account and warned the owners of Twitter of insufficiently good authentication procedures for administrator accounts. Possible protection against these attacks is the use of two or more factor authentications when logging in to the administrator account.

A security vulnerability of LinkedIn was discovered in LinkedIn's add-on for the Internet Explorer. Using spam messages, the attacker could mislead users to visit a malicious page and download malicious program code. Because of flaws in ActiveX controls of the said tool, the attacker could take control of users' computers or execute DoS (Denial of Service) attack. Security flaw in LinkedIn's add-on for the Internet Explorer has been corrected.

Similarly to other networks, the most common attacks are spam messages and directed phishing attacks (spear phishing attack). LinkedIn users often receive emails from network administrator or other users of the network. In this case, the attacker sent spam e-mail messages on the e-mail addresses of 10,000 LinkedIn users that appeared to have been sent by the network administrator. However, the specificity related to phishing attacks is that the attacker was sending spam messages that might interest the user. Thus, the attacker has previously managed to find out personal information about users to which the spam message will be sent. In this case, the spam messages contained a link to a malicious site, which infected users with a malicious program. The attacker could then gain access to the users' computer, and compromise the privacy and safety of users.

According to Hogben Giles, main threats on social networks are:[14]

- Digital dossier aggregation.
- Secondary data collection.
- Face recognition.
- Content-based Image Retrieval (CBIR).
- Difficulty of complete account deletion.
- Spam.
- Cross site scripting (XSS), viruses and worms.
- Spear phishing.
- Infiltration of networks.
- Profile-squatting and reputation slander through ID theft.
- Stalking.
- Bullying.
- Corporate espionage.

The same author gives some recommendations for reducing threats:[15]

- Encourage awareness-raising and educational campaigns.
- Review and reinterpret the regulatory framework.
- Increase transparency of data handling practices.
- Discourage the banning of SNSs in schools.
- Promote stronger authentication and access-control where appropriate.
- Implement countermeasures against corporate espionage.
- Maximise possibilities for abuse reporting and detection.
- Set appropriate defaults.
- Providers should offer convenient means to delete data completely.
- Encourage the use of reputation techniques.
- Build in automated filters.
- Require consent from data subjects to include profile tags in images.
- Restrict spidering and bulk downloads.
- Take the measures of protection from spam and phishing.
- Promote and research image-anonymization techniques and best practices.
- Research into emerging trends on social networks.

SOCIAL NETWORKS IN THE STATE ADMINISTRATION, AUTONOMOUS PROVINCES AND LOCAL SELF-GOVERNMENTS OF SERBIA

The bodies of state administration, autonomous provinces and local self-government, (public administration), as the citizens' service, in order to establish regular, rapid and transparent communication with the public and provide information about the work of public

14 Hogben G., *op.cit.*, pp. 3–4.
15 *Ibid.*, pp. 4–5.

administration and independent institutions, should create an interactive and proactive communication on social networks.[16]

The development of social networks (Facebook, Twitter, LinkedIn, etc.) on the Internet has changed the way of communication and content sharing. The users come to more content through social networks compared to traditional search via search engines or accessing the web sites. In order to increase the availability of published information, it is necessary to maintain a web presence, adapt to quick and easy sharing of content on social networks using web technologies that allow this. In this regard, it is recommended to share content that changes on a daily basis (news, current affairs, events, activities, etc.).[17]

The main features of social networks is that they are the most effective and quickest source of information, are transparent, always available, free, public, dynamic, multimedia, and provide the necessary two-way communication. When most government agencies use social networks as a tool for communicating with citizens and keeping them informed, it would undoubtedly lead to greater confidence in the operation of the state. There is no doubt that fast, accurate and continuous information provided to the citizens, leads to increased trust, which creates a positive attitude towards a state agency, which is a good way of representing and communicating with citizens on social networks.[18]

Most people using smart phones spend a lot of time browsing Facebook or content of some other popular social networks. According to research of the Republic Agency for Electronic Communications on the number of sold phones and SIM cards, it can be concluded that every citizen of Serbia has two mobile phones. Another important consideration in the decision on opening an online account is the possibility of referring to the development of mutual relations of trust between state institutions and Internet users.[19]

Timely, clear and direct communication with citizens will reinforce the impression of an efficient and transparent work of state institutions. On the other hand, avoiding the usual technical terminology which is sometimes incomprehensible for the citizens and the use of simple everyday language, will bring state institutions closer to the Internet users and will help consolidate the relationship of trust and understanding.

One of the many advantages of social networks consists of the fact that when one wants something to suggest to the public and is not sure what the reaction will be to it, it is recommended to first communicate on social networks. This provides several things – primarily allows people who understand the scope of work of national authorities to directly participate in the creation of something new, and the authorities get the opportunity to see and hear what it is that citizens and businesses need. Since the job of the state is to help citizens and ensure smooth operation of businesses, appropriate authorities, via social networks, can see what they need to change to facilitate daily operations.

Finally, it is important to note that any form of communication, being it internal or external, belongs to the public relations. The way of communications with citizens and the public must be such as to give the impression that the institution is willing to listen to and acknowledge everyone's opinion.

16 *Guidelines for the use of social networks in the state administration, the autonomous province and local self-government*, Directorate for eGovernment, Ministry of State Administration and Local Self-Government, Belgrade, 2015, p. 4.
17 *Guidelines for creating web presentation of state administration, territorial autonomy and local governments v. 5.0*, Directorate for eGovernment, Ministry of State Administration and Local Self-Government, Belgrade, 2014, pp. 10–11.
18 *Guidelines for the use of social networks in the state administration, the autonomous province and local self-government*, *op.cit.*, p. 4.
19 *Ibid*., p. 5.

SOCIAL NETWORKS IN THE ARMY

Social networks at the same time could be used for defence activities (prevention, warning, forecasting, institutional communication, crisis management) and for offensive action (influence, propaganda, deception).[20]

By using Internet-based platforms like Facebook and Twitter, social media provides new ways to connect, interact and learn. Social media, with a variety of available platforms, can instantaneously connect users within a global network, making the transfer of information even more pervasive. Today, social media is so widespread and transparent that one may already be involved even if not actively participating. Social media is highly effective tool to use when reaching out to large communities and audiences. But with this substantial ability to connect with the masses, comes risk. Using social media to spread information is becoming the standard. More and more units are using social media to communicate, so it's more important than ever to understand the risks associated with using the various platforms.[21]

The Army understands the risks associated with social media and has worked hard to develop training to help soldiers and family members use social media responsibly. Soldiers using social media must abide by the Uniform Code of Military Justice (UCMJ) at all times. Commenting, posting, or linking to material that violates the UCMJ or basic rules of soldier conduct is prohibited. Social media provides the opportunity for soldiers to speak freely about what they're up to or what their interests are. However, soldiers are subject to UCMJ even when off duty, so talking negatively about supervisors, or releasing sensitive information is punishable under the UCMJ. It is important that all soldiers know that once they log on to a social media platform, they still represent the Army.[22]

When using social media, soldiers must avoid mentioning rank, unit locations, deployment dates, names, or equipment specifications and capabilities.[23] Geotagging photos and using location-based social networking applications is growing in popularity, but in certain situations, exposing specific geographical location can be devastating to Army operations. While soldiers are engaged in Army operations, they should turn off the GPS function of their smartphones. Failure to do so could result in damage to the mission and may even put families at risk.[24]

Soldiers cannot include any copyrighted or trademarked material on their social media platforms. Social media is about connecting, so it is only natural that Army leaders may interact and function in the same social media spaces as their subordinates. How they connect and interact with their subordinates online is up to their discretion, but it is advised that the online relationship function in the same manner as the professional relationship.[25] If a leader comes across evidence of a soldier violating command policy or the UCMJ on social media platforms, then that leader should respond in the same manner they would if they witnessed the infraction in any other environment. Using rank, job, and/or responsibilities in order to promote oneself online for personal or financial gain is not appropriate. Such actions can damage the image of the Army and an individual command.[26]

By watching the wall on a Facebook site, or by reading the comments on a blog post, social media managers can get a feel for what the online community wants to hear about. Sometimes, it is useful to talk to an audience directly. Ask for feedback and suggestions, and then

20 Montagnese A., *Impact of Social Media on National Security*, Centro Militare Di Studi Strategici, Rome, 2012, p. 21.
21 *U. S. Army Social Media Handbook,* Online and Social Media Division, Office of the Chief of Public Affairs, Pentagon, Washington DC, 2011, p. 3.
22 *Ibid.*, pp. 3–4.
23 *Ibid.*, p. 5.
24 *Ibid.*
25 *Ibid.*, p. 11.
26 *Ibid.*, p. 6.

act on that feedback. A social media presence accomplishes very little if the online audience is not interested in what's being said. Listening to an audience can mean the difference between maintaining a successful social media presence or an irrelevant one.[27]

Using social media to communicate with stakeholders during a crisis has proven to be an especially effective due to its speed, reach and direct access. In recent crisis, social media has helped distribute command information to key audiences and media while also providing a means for dialogue among the affected and interested parties.[28]

The Army recognizes that social media gives people the ability to communicate with larger audiences faster and in new ways. It has become an important tool for Army messaging and outreach. The Army understands the risks associated with social media and has developed training to help soldiers and family members use social media responsibly.[29]

Most of social media failures can be attributed to organizations rushing into social media before determining what exactly the organization aims to achieve with social media platforms. Using social media effectively is a process and it requires strategy, goals, manpower and foresight. By reading the comments on a Facebook wall or blog post, social media managers can get a feel for what the online community wants to hear. It is also useful to talk to your audience directly.[30]

Social media sites provide their own free analytics tools that allow administrators to track views, impressions and comments. By using numbers in conjunction with comments and reader feedback, it is easier than ever to determine how organizational messages are received and how the audience is responding to the content. Some analytics tools provide graphs and charts, but ultimately the presentation of information depends on the platform. These different presentations make for a richer statistical analysis. Using free analytics tools can help a unit demonstrate the usefulness of a social media platform, and even highlight the success of a specific social media campaign.[31]

Keep your social media presences up-to-date by using mobile devices, if necessary. The myriad of mobile devices available today allow you to update social sites without being tied to your computer at a desk. Crisis happen all the time, so be prepared. Whether the installation is on lockdown, you're waiting out a storm or you're at a remote site at the scene, mobile devices allow you to share updates immediately. Ensure your mobile devices are continuously charged and be creative in finding power solutions that work for your situation.[32]

Social media is becoming a valuable tool for keeping families and soldiers connected, which is vitally important to unit well-being.[33] The Department of Defence specifically encourages service members and their families to use social media. Social networking sites provide a safe space for individuals to share their problems with others and to receive advice from others while maintaining a comfortable emotional distance. Social media also affords users tremendous opportunity to exchange information in a rapid, efficient, low-cost manner. Research is mixed regarding the power of social media to connect people or isolate them, and to alleviate or exacerbate stress. It is likely that a range of outcomes may be associated with social media use depending on a wide range of factors.[34]

27 *Ibid*, p. 9.
28 *Ibid*., p. 10.
29 *U. S. Army Social Media Handbook (version 3.1)*, Online and Social Media Division, Office of the Chief of Public Affairs, Pentagon, Washington DC, 2013, pp. 1–2.
30 *Ibid*., p. 5.
31 *Ibid.*
32 *Ibid*.
33 *Ibid*., p. 19.
34 *Social Media Communication with Military Spouses*, The Military Reach Team, The University of Minnesota, Minnesota, 2015, pp. 4–13.

CONCLUSION

Social networks are a phenomenon that in the past decade spread rapidly and globally. Social networks have changed the way of communication, the daily activities of people, and in a way, changed the world. Social networks are communication tools and they can be a threat or an opportunity for national security.

Social networks made a major shift in communication in the public sector, the army, the business area. With the advent of technologies that use social networks, new vulnerabilities that attackers could exploit will appear.

Users of social networks should definitely pay attention to threats which can endanger large amounts of personal or confidential information. By using anti-virus, anti-spyware tools and similar mechanisms for the protection and application of precautions when using social networking, users will primarily provide privacy for data that will not be disclosed to anyone.

That is why wider adoption of the national strategy of social networks is very important. According to Macnamara, a small number of government agencies and institutions in the world has adopted a national strategy to deal with the proper use of social networks.[35] The lack of strategy for social networks presents large national security risks.

The future of social networks is hard to predict, but there are still some limits that can be moved in order to achieve even better communication among users. The idea is emerging as the next major shift in communication via social networks is the possibility of communication between users of different social networks. Also, it is expected that the created user profiles on social networks will be able to install other web services, applications, etc.[36]

REFERENCES

1. Ellison N., Boyd D., *Social Network Sites: Definition, History, and Scholarship*, Journal of Computer-Mediated Communication 13, The Pennsylvania State University, 2008.
2. *Guidelines for creating web presentation of state administration, territorial autonomy and local governments v. 5.0*, Directorate for eGovernment, Ministry of State Administration and Local Self-Government, Belgrade, 2014.
3. *Guidelines for the use of social networks in the state administration, the autonomous province and local self-government*, Directorate for eGovernment, Ministry of State Administration and Local Self-Government, Belgrade, 2015.
4. Hogben G., *Security Issues and Recommendations for Online Social Networks*, European Union Agency for Network and Information Security (ENISA), Heraklion (Greece), 2007.
5. Kaplan A., Haenlein M., *Users of the world, unite! The challenges and opportunities of social media*, Business Horizons, Vol. 53, Issue 1. Kelley School of Business, Indiana University, 2010.
6. Lindsay B., *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations*, *CRS Report for Congress*, Congressional Research Service, 2011.
7. Macnamara J., *Social Media Strategy and Governance - Gaps, risks and opportunities*, Australian Centre for Public Communication, University of Technology, Sydney, 2011.
8. Montagnese A., *Impact of Social Media on National Security*, Centro Militare Di Studi Strategici, Rome, 2012.

35 Macnamara J., *Social Media Strategy and Governance - Gaps, risks and opportunities*, Australian Centre for Public Communication, University of Technology, Sydney, 2011, p. 2.
36 *Sigurnosni rizici društvenih mreža*, *op.cit*., p. 26.

9. Rheingold H., *The Virtual Community: homesteading on the electronic frontier.* 1993.http://www.rheingold.com/vc/book/

10. Sigurnosni rizici društvenih mreža, Hrvatska akademska istraživačka mreža – CARNet, Zagreb, 2009.

11. Social Media Communication with Military Spouses, The Military Reach Team, The University of Minnesota, Minnesota, 2015.

12. U. S. Army Social Media Handbook, Online and Social Media Division, Office of the Chief of Public Affairs, Pentagon, Washington DC, 2011.

13. U. S. Army Social Media Handbook (version 3.1), Online and Social Media Division, Office of the Chief of Public Affairs, Pentagon, Washington DC, 2013.

UDC: 343.123.12
343.982.35

IMPLEMENTATION OF NEW EQUIPMENT, MEANS AND MEASURES IN SECURING THE CRIME SCENE AND CRIME SCENE INVESTIGATION[1]

Zvonimir Ivanović, PhD[2]
Academy of Criminalistic and Police Studies, Belgrade
Oliver Lajić, PhD
Academy of Criminalistic and Police Studies, Belgrade
Milan Žarković, PhD
Academy of Criminalistic and Police Studies, Belgrade

Abstract: Start of digitalization and the introduction of technical solutions in everyday police work are more and more making sense, and in this sense in the world it takes a growing toll. Modern police services tend to introduce new technologies in police activities and other measures and actions. EDEN CBRNe FP 7 Phase two project pointed out the multiple possibilities of use of these solutions and devices based on them. In the framework of this project there are presented very broad deployment options of those devices and measures that represent auxiliaries and, in some cases, indispensable means and devices for the dealing with such conditions and situations. The instruments, equipment and measures that we are trying to show here range from Nut mini smart tracker with bluetooth[3] technology and can bind different data for from photo to video recording of a small amounts of data, through drones that can be exploited in different circumstances and conditions, and suffer those circumstances cases in which people could not suffer as well as monitoring and service system for receiving data from the field and from the devices and the funds that make up a unique ecosystem with multiple and very useful features built in and capabilities. The user of this system will use its maximum capability and speed up the reaction of the prosecuting authorities and acting in the direction of solving a crime. This system can be best used when securing of the scene and in crime scene investigation.

Keywords: investigation, information - communication technology, securing the crime scene, new technology, police measures and actions

INTRODUCTION

In classical criminalistics theory working with crime scene introduces physical presence on the scene, processing of the traces and objects at it and gathering information from witnesses or present people at the scene. In modern theory interdisciplinary approach prevails. It is not only necessary to be present at the crime scene but of utmost importance there is in-

1 This paper is the result of the realisation of the Scientific Research Project entitled „Development of Institutional Capacities, Standards and Procedures for Fighting Organized Crime and Terrorism in Climate of International Integrations". The Project is financed by the Ministry of Science and Technological Development of the Republic of Serbia (No 179045), and carried out by the Academy of Criminalistics and Police Studies in Belgrade (2011–2014). The leader of the Project is Associate Professor Saša Mijalković, PhD.
2 E-mail: zvonimir.ivanovic@kpa.edu.rs.
3 More information can be retrieved at: https://www.bluetooth.com/ last time accessed 03.02.2016.

formation flow, or more precisely information analysis and centralisation of information flow, of course mainly intelligence information flow. Through this information flow it is possible to obtain and maintain everlasting or instant surveillance over the scene of crime. This also can help in making decisions, and actually shortening of time needed to react, therefore it can represent decision making tool and tool for human resources deployment. In quick reactions this kind of information flow with real time tracking changes is also of great importance. In circumstances of actual Serbian reality this can be seen as a pure science fiction, but we are trying to present it as very near future for police in Serbia.

At the crime scene there is a great possibility to engage new and practically verified devices to get as much information as it can be covered from the crime scene. It was a case with photo camera, video cameras, stereophotogrametry, 3d Scanners of crime scene and now we can go further. There are many gadgets available on the market, but which of many is suitable for implementing in crime scene processing? We will show some of those and we will present their comparative advantages, because of their testing in the real environment, and by no chance we do not recommend any of them as the best, we just are trying to give you in scent of what should or could be in real environment and also what are possibilities of those presented.

FIRST RESPONDING

In law enforcement philosophy the crime scene processing is in vast majority of cases of essential importance, because of its significance later in the trial process. But crime scene processing and securing of that crime scene are timely of great importance not only for the trial but for preventing and proactive acting in order to prevent future accidents caused by initial security concern or additional consequences and relicts of initial crime act. This should also be in mind when thinking of implementing new technologies, devices and systems. In terms of starting it is significant to mention that in all police stations since 2002 GIS software support has been installed with Arcview and ArcMap so there are possibilities based on this software to trace in real time activities on the field. This software has possibilities to run under intranet of Ministry of Interior and it can have proxy connection with outside – internet filtered with secured logging in and limited access with very different inputs with different objects embedding. This solo gives incredible opportunities which frankly are not exploited not even at the minimum. But there are numerous possibilities present online for implementing in this process, and of course there are commercial software solutions. It is a matter of strategical orientation and of course question of security protocols and standards implementation with possibilities of exploitation of security flaws by unauthorised persons. In the light of the newest changes in law system in Republic of Serbia and new Law on Police (Official Gazette of Republic of Serbia nr.6/2016) it is of significance article 37. In this article which is about official badge and legitimation of police officers there are some sentences which stipulate following: Official legitimation of police officer can be used for: accessing of MOI intelligence (information) system, digital signing of documents, encrypting of official documents, physical access to certain objects and areas where there is a necessity of higher level of protection and in other prescribed cases by the law. In this view it is very important that people who are the first responders have proper equipment with them and devices capable to transfer real status of things to central information intelligence center in order to make decisions faster or to help them in making decisions on the site of actual happening. This being said gives intro for the thinking about platforms of operating systems (OS) existing in open source environment, first of them goes as google android software[4] platforms (there are ten actual versions

4 https://en.wikipedia.org/wiki/Android_(operating_system) retreived 26.01.2016.

of OS with open source[5]) all of them capable to have standalone performance on the different devices. Most common usage is mobile usage from tablets to handheld devices, all capable to perform different communication and other information traffic. This presents a world full of opportunities in today's world with 4G communications in version of Cat4 capable of transferring 150 Mbit/s in download and 50Mbit/s in upload of data[6] through mobile and cellular phones, and yet we are still waiting for something to happen by itself.

According to a Statistica's estimate, Android smartphones had an installed base of 1.6 billion units in 2014, which was 75% of the estimated total number of smartphones worldwide[7]. Android has the largest installed base of any mobile operating system and, since 2013, the highest-selling operating system overall[8] with sales in 2012, 2013 and 2014[9] close to the installed base of all PCs[10]. In the third quarter of 2013, Android's share of the global smartphone shipment market was 81.3%, the highest ever,[11] and the Android share—led by Samsung products—was 81.3%[12].

By August 2015, two continents went mobile-majority, judged by web use ("desktop" has 51.6–56.7% use worldwide, depending on week or weekend use[13]); because of Android (see usage share of operating systems), that has majority use on smartphones in virtually all countries (all continents have gone Android-majority, including North America[14] except for Oceania, because of Australia),[15] with few exceptions (all of which have iOS -majority); in the US Android is close to iOS, having exchanged majority position a few times,[16] Canada and the following are also exceptions: Japan, Philippines, Australia and the only exceptions in Europe are the UK, Switzerland, and the Nordic countries Denmark, Norway and Sweden.

By 2016, virtually all countries in the world, have gone Android-majority on smart-

5

Version	Code name	Release date	API level	Distribution
6.0	Marshmallow	October 5, 2015	23	0.7%
5.1.x	Lollipop	March 9, 2015	22	15.7%
5.0–5.0.2		November 3, 2014	21	16.9%
4.4–4.4.4	KitKat	October 31, 2013	19	36.1%
4.3.x	Jelly Bean	July 24, 2013	18	3.5%
4.2.x		November 13, 2012	17	12.2%
4.1.x		July 9, 2012	16	9.0%
4.0.3–4.0.4	Ice Cream Sandwich	December 16, 2011	15	2.7%
2.3.3–2.3.7	Gingerbread	February 9, 2011	10	3.0%
2.2–2.2.3	Froyo	May 20, 2010	8	0.2%

6 https://en.wikipedia.org/wiki/4G#Data_rate_comparison retreived26.01.2016

7 "Market share of smartphone OS of total smartphone installed base in 2013 and 2014". Statistica. Retrieved February 18, 2015. And "Smartphone OS worldwide by installed base in 2014 (in millions)". Statistica. Retrieved February 18, 2015.

8 Mahapatra, L. (November 11, 2013). "Android Vs. iOS: What's The Most Popular Mobile Operating System In Your Country?". Retrieved January 30, 2014. Also in Elmer-DeWitt, P. (January 10, 2014). "Don't mistake Apple's market share for its installed base". CNN. Retrieved January 30, 2014. "Samsung sells more smartphones than all major manufacturers combined in Q1". Retrieved May 12, 2014. And also Yarow, J. (March 28, 2014). "This Chart Shows Google's Incredible Domination Of The World's Computing Platforms". Retrieved April 23, 2014.

9 Global mobile statistics 2014 Part A: Mobile subscribers; handset market share; mobile operators". mobiThinking. May 2014. Retrieved September 9, 2014.

10 Rowinski, Dan (December 10, 2013). "The Post-PC Era Begins In Earnest Next Year: In 2014, smartphones will most likely eclipse PCs in terms of the number of devices in use around the world". readwrite. Retrieved September 9, 2014.

11 "Android tops 81 percent of smartphone market share in Q3". Retrieved November 4, 2013.

12 Lunden, I. (July 1, 2013). "Android, Led By Samsung, Continues To Storm The Smartphone Market, Pushing A Global 70% Market Share". TechCrunch. AOL Inc. Retrieved July 2, 2013.

13 "StatCounter Global Stats – Browser, OS, Search Engine including Mobile Usage Share". statcounter.com.

14 ibidem

15 Ibid.

16 Locus citatus

phones[17]; excluding United States and Canada (while including North America continent as a whole), Australia and Japan. A few countries loose Android-majority, such as the UK, if tablets are included.

Those devices and technical equipment with their capabilities and characteristics have very bright future for crime scene processing and securing of the crime scene and evidence, because of their usefulness in activities of first responders, especially in the future. In that manner it is possible to think in two different levels of usefulness of new technologies, devices and systems in police (and generally law enforcement officers) procedures: sensing of different agenses present at the site of occurrence and their constant renewing of status at that scene and also transferring of that kind of data to center of decision making through secure platform.

DEVICES

In this course we can start thinking about some commercial and some non-commercial devices and their capabilities of connecting in order to make it easier on the scene of event with possibility to become criminal or even an event of mass destruction or life threatening disaster. The first of those could be usage of so called "gadgets" with specific characteristics for instance commercial goods in form of Nut mini smart tracker[18] with Bluetooth[19] technology or any other device with similar technology for example – NFC[20] as one of the electronic communication protocols. Both of the two mentioned have their commercial usage and their commercial value is very low which recommends them as very economically valuable for law enforcement needs. It is of strategical and tactical importance to decide which of those to use, but eventually any of them could be used simultaneously. The only thing that one has to keep in mind is to have staff using the right software and hardware with the support for these devices – meaning that handheld devices or mobile phones in use have compatible communication capabilities to serve these tracking devices. In usage of those devices there are commercial implementations of software solutions especially targeting law enforcement like Prometech. With its Tag & Trace[21] system solution one of firms out here made some impact in UK. Tag & Trace uses NFC technology[22] to track persons and objects. In the field of emergency response this can help organize the decontamination and triage process by supporting a streamlined IT workflow for handling victims during incidents. The system allows first responders to register contaminated and injured people at the earliest possible moment and track their progress throughout the response chain. Producer of the Tag & Trace advertises product as smart and cost effective way to share and structure information about victims in large scale incidents. Tracking information is available in real time, at the headquarters, providing commanders with the strategic overview needed to improve decision making. The system can be used to track people, items or samples found in or near the incident area. Tag & Trace does not require a permanent network uplink, but rather will synchronize whenever a connection is available. This also can be a downside of this device usage in real conditions, because of not having present devices with communication capabilities we cannot have real time updates from tracker and tagging then doesn't have operative value. It also can be said for the other

17 http://gs.statcounter.com/#mobile_os-ww-monthly-201601-201601-bar retrieved February 06 2016
18 http://www.nutspace.com/products/nutmini retreived 26.01.2016.
19 https://www.bluetooth.com/what-is-bluetooth-technology retreived 26.01.2016.
20 https://en.wikipedia.org/wiki/Near_field_communication retreived 26.01.2016.
21 http://www.prometech.eu/products/tag-trace/
22 As a new form of RFID NFC TAGs can be used over different handheld devices in order to monitor and tag and trace assets and there are many applications which provide surveillance and monitoring of movement of those devices.

Bluetooth device but actually there are more devices with Bluetooth technology built in than with NFC technology, so one has to have that in mind when deciding what to use and which communication devices are going to be used as uniform for the CSI processing and securing the scene and evidence. Specific for NFC is that when one of the connected devices has Internet connectivity, the other can exchange data with online services. In connection with Bluetooth technology the principle is similar but there is a question of power consumption in both cases and with new standards in Bluetooth technology with low power consumption also adds to their value. Both devices shown here can be used for victims tagging and tracing, but also for the same for samples and items. Throughout these devices it is possible to make triage at the crime scene and prioritize what to do and when with different urgency levels of victims, samples and items (objects, evidence, traces) or to make it easier to decide how to and to what to give priority and also to act quicker. Besides track and trace it is possible to set decontamination and triage status (severity of injury or possible consequences for victims) through out of taking pictures or small size videos, including audio and textual description, which then can be posted or transferred to some system over the handheld devices. In that way there are possibilities for command centers and upper management to react and survey actual acting at the crime scene and manage crisis situations with more reliable information for it. These devices need additional systems as shown and in that can be used even non-commercial open source systems for transferring of the video or images along with audio and description data Windows, or Linux, even Mac OS X (truthfully very rare in our surrounding) based Servers on the net and connect it to some system to unify and sort that information and lay it over map of the terrain (which also can be open source like google maps or something similar or over ArcMap and ArcView already licenced in MOI) where you can monitor and surveillance actions in real time and decide on that with great certainty. For both devices there are different specifications but what needs to be pointed out is that individual tags are cheap, waterproof and can be scanned and updated by simply holding a tagging device in the immediate vicinity. Also vast majority of systems is optimized to facilitate quick processing of a high number of persons and items. For all devices explained it is very important that they have or provide communication interface for easy integration with any of the systems for their usage. Both presented do, and each of them has its own downs and ups.

Besides presented there are also widely available both commercially and free (open source) devices which can present sensors as early warning technology and their assimilation into the existing software solutions for Decision Support Systems. These are keys to get fast reaction capabilities of all first responders, decision makers etc. Throughout shown procedures of tagging, tracing and shown new means for info gathering this integration of sensors, deployment of human resources and their input based on crime scene inspection and information gathering, it is of essential importance to have working system to manage that information and validated and qualitative affirmed sensors. When it comes to sensors for instance for Chemical Warfare Agense (CWA) such as sarin or any other warfare chemical weapon there are much better options with commercial than open source systems. There are tools available for integration and exploitation of smartphone technology which may help in the response phase with specific focus on First Responder support. One of them is connected with EDEN FP7 Phase II security program of EU, with EDEN toolstore we can see many new features and software and hardware solutions. The main concepts that are addressed in EDEN project are: increased awareness about the health status of the contaminated people combined with proper decision support tools can save lives. Smart management with devices sensors and systems connected could be demonstrated in SESMER software solution of Selex ES commercial entrepreneur shown on figure 1.

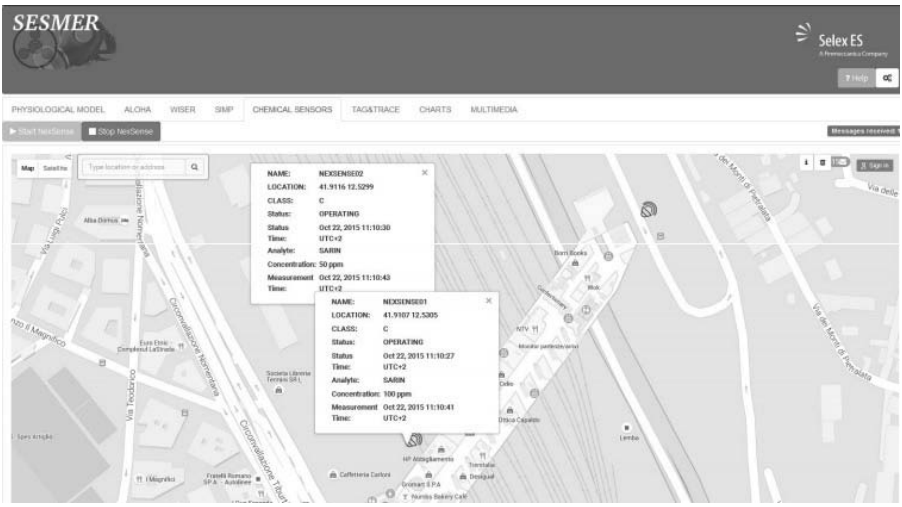


Figure 1

In this picture there can be seen deployment of sensors for detecting the presence of different CWA at the scene, and that could be done without endangering any of law enforcement officers on the field. All of them could be deployed by means of aerial vehicles such as helicopters or UAV (unmanned aerial vehicles) to the scene and especially on the spot planned to be most affected by certain agense.

Nexsense provides different types of sensors. One of those is MEMS sensor technology using UHFAIMS (ultra-high field asymmetric ion mobility spectroscopy). Sensing instruments come as the result of a partnership with Owlstone Nanotech. It allows reduced false alarm rate and chemical identification in severe environments and it is used for Chemical Warfare Agent (CWA) and Toxic Industrial Chemical (TIC) point detection and as identification equipment. It is aimed for markets: Military, Police, Fire Departments and other First Responders. Its characteristics are: the ability to identify sufficient key features in both the, chemicals of interest and in the clutter to clearly discriminate between them. It also detects and identifies broad range of chemicals across widely varying concentrations and environmental conditions. It is easy to use, because it is portable, network enabled, and it is simple but comprehensive operator interface. High and low field are generated by applying a high frequency (MHz) high-voltage waveform across "filter" electrodes. Next one of the sensors is Nexsense C Handheld. Key Capabilities of this sensor are: Continuous Monitoring with detection of threat in 3s, Identification of detected threat in 10s, highly sensitive – in the UH –FAIMS region the chemical behaviour is much more, distinct resulting in a system that is more sensitive than conventional IMS systems, reliable - by identifying the substance the system minimises false alarms. Also it has broad-band threat spectrum - Chemical Warefare Agents (CWAs), Toxic Industrial Chemicals (TICs) and their precursors, it is simultaneous - one operating mode for all threat types. It doesn't have any Radiation Source in Handheld unit – unlike other FAIMS systems the sensor does not contain a radioactive source therefore that means that by this we are removing the need for user licences and special storage and disposal.

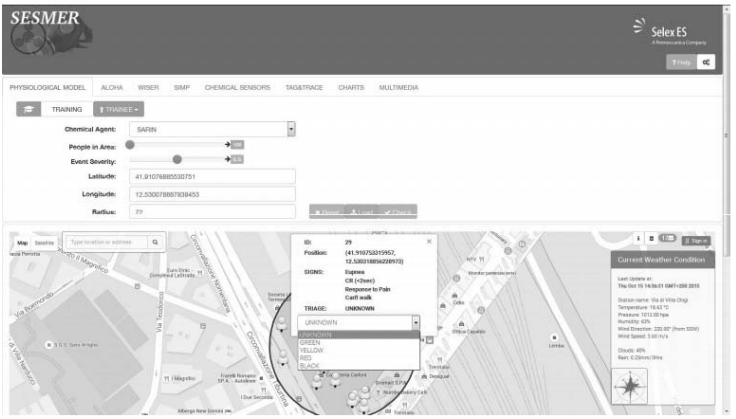


Figure 2

After the deployment of sensors you can connect in real time and project over the map (open source or not) all the possible affected personnel and checked victims with already shown Tag & trace technologies (no matter which device used NFC or Bluetooth), and also send that information to the ambulance or other emergency service or they can read the same map and use the same software system and decide on priorities of emergency services in coordination with the decontamination teams (whether they are military or territorial defence or any other). All of presented can be integrated in one system with different levels of access and scope of insight based on the level.

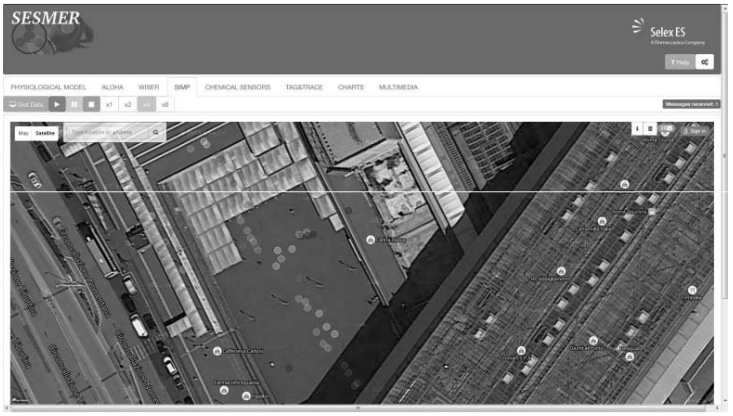


Figure 3

These tools can even be used in modelling the impact of CWA release in terms of casualties, crowd dynamics and effects on the existing health service infrastructures (hospitals, ambulance services, etc.) as well as decontamination analysis. Of very interesting implementation in this kind of systems there is software which predicts the movement of masses in the critical moment, where the mass is controlled by panic fear and irrational motivation or striving. There are predictable models for social behaviour derived from behavior of other

collective groups of species in nature such as ants (swarm behavior)[23] or herds[24] of cattle and similar, also there are researches of human acting and behavior[25] under stress especially in these types of environments. One of those models was implemented in the scenario for presentation of SESMER model, by which it was possible to predict movement of individuals as part of collective mass and also through that prediction it was possible to plan engagement of police and other emergency and military personnel in present situation on the field. This gives great opportunities for personnel engagement planning and better human resources management through the implementation of new technologies and their embedding in systems which all are presented here. It also serves to better decision making and lowering risk for deployed personnel.

One of interesting software for implementation in such environments is Nanotics[26]. It is commercial software and it was technologically developed in research labs – Data integration and development framework. It provides:

- Open code for clients & partners
- Stability and quality
- 8 years of continuous developments and upgrades

In particular the so-called SEMP Servers Management solution can also be taken into consideration, because it is easy to use, offers complete coverage, it is on web, also it is very stable, largely adopted. Besides that, it offers working with Multi-platforms and it is Modules based

Next one worth reconsidering is Eonix. Initially all Products, Services and development were developed for: Integration with mobile applications solutions Medical Education Companies Associations Public Sector Research. These are based on: Geolocation data, Team information, Samples and Observation data, Bi-directional Alerts management, Mobile solution, Central web server, Web services connections, Secured systems and connections, Traceability. From the following illustrations in figures 4, 5 and 6 one can see the practical use value of these sollutions. Eonix provides multilayers of data presenting and gives headquarters insights from different perspectives and of course therefore facilitates decision making more easily than in any other way.

Figure 4

23 https://en.wikipedia.org/wiki/Swarm_behaviour last time accessed 05.02.2016.
24 https://en.wikipedia.org/wiki/Collective_animal_behavior last time accessed 05.02.2016.
25 http://www.public.asu.edu/~huanliu/papers/IS10.pdf last time accessed 05.02.2016.
26 http://eonix.be/nanotics/ last accessed 02.01.2016.

In this figure we can see that there are multiple personnel deployed at the field and that all of them provide feedback over from their locations and the system presents it as alerts and gives unique identifier to any of subjects or their alerts and projects it on the map and over all screens for all authorised users. It also provides systems classification of all data carriers and providers of information with labeling, even the sample diverging and their connections. At the very end it provides also the possibility for communication directly with data provider.

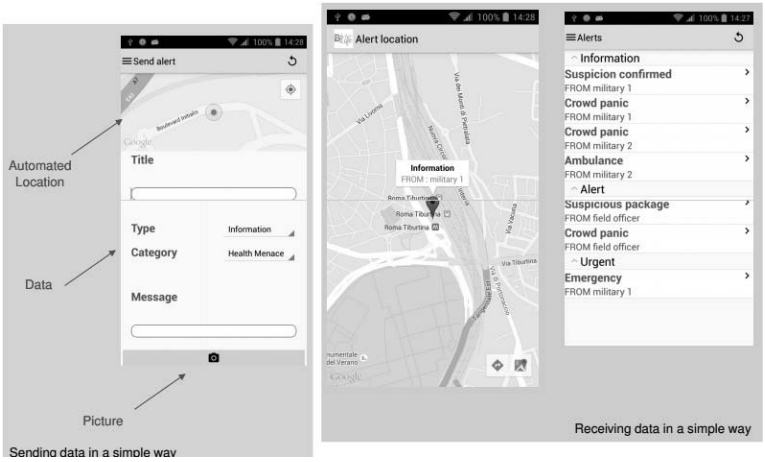


Figure 5

Figure 5 gives overview of next steps and integration of digital handheld devices such as smart phones and showing the system overlapping of different information and their presentation on the screen of possible HQ or any other authorised center for surveillance of these actions.

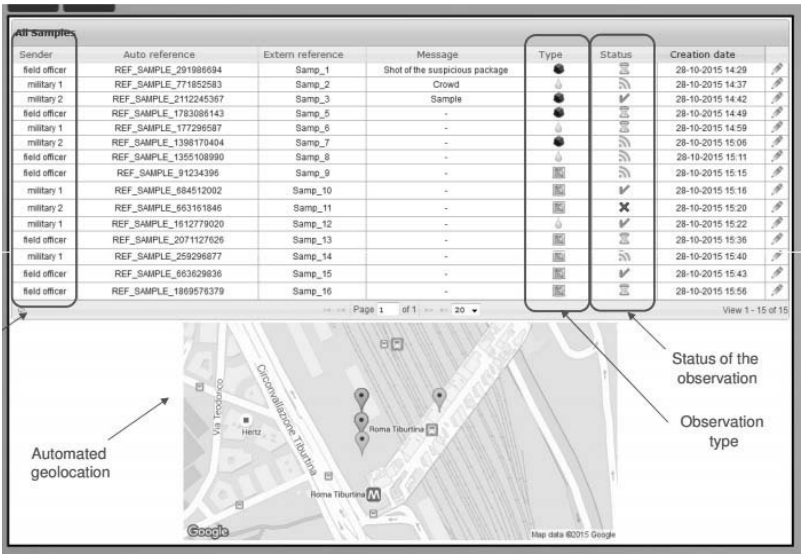


Figure 6

Those examples give more insight into the manner that system could be working and specially framed are special interesting moments presented in figure 6. There we can see au-

tomatically generate geospatial data over the map and we can see the origin of the data in the system (whom is it coming from – who is the source, besides where it comes). We can even see the type of observation for the source of data and the status of that observation.

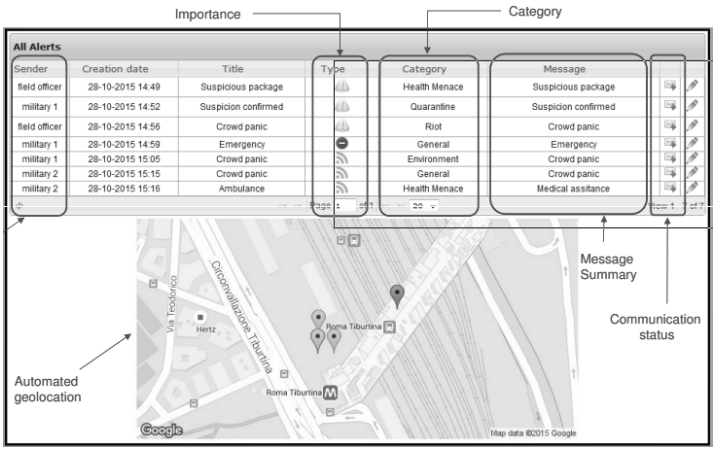


Figure 7

All of mentioned is followed with the difference in importance of alerting embedded in the data and severity of emergency and also the category of source determined data. Especially interesting is system generated messages summaries, where one can read short summary of emergency and significance of data presented by particular subject at the scene. It goes to that end that it provides communication status of particular subject – by which it means it is possible to connect with that particular subject and from the first hand get the information from him or her.

CONCLUSION

For the upcoming new technologies and the existing one and their place among common people there are huge possibilities in their implementation for everyday life. Moreover, there are very large scale possibilities for embedding those in state agency services such as emergency services, police services and even military services. In all countries in the world, especially developed countries, there is implementation of technologies firstly in military purposes followed by civil state services. In this article we are speculating with civil state services, but we are not limiting those to it, so there could be possible military or state security interest for those technologies and devices. In the shown implementations and possible systems implementations over those devices, technologies and handheld devices we can infer that their usefulness is of extreme interest for our emergency, police and other state government agencies. In shortening time to respond to emergency situations, this adds to informed, adequate, quick and very precise answer to any level of governance, especially in emergency or disaster situations. What we also showed here are the possibilities of implementation of the existing and wide accepted mobile technologies and mobile phones with their capabilities adapted to the expectations of emergency services. With that embedding and interconnecting of different technologies and devices we have shown capabilities for different systems to overhaul and exploit possibilities of intercommunication of Internet of things (IOT). These possibilities are no longer future, they are present, and we need to address them as soon as possible. This article shows their existence and near availability.

REFERENCES

1. Lunden, I. (July 1, 2013). "Android, Led By Samsung, Continues To Storm The Smartphone Market, Pushing A Global 70% Market Share". TechCrunch. AOL Inc. Retrieved July 2, 2013
2. Mahapatra, L. (November 11, 2013). "Android Vs. iOS: What's The Most Popular Mobile Operating System In Your Country?". Retrieved January 30, 2014. Also in Elmer-DeWitt, P. (January 10, 2014). "Don't mistake Apple's market share for its installed base". CNN. Retrieved January 30, 2014. "Samsung sells more smartphones than all major manufacturers combined in Q1". Retrieved May 12, 2014.
3. Marinković, D. Lajić Oliver, Kriminalistička metodika, Beograd KPA, 2015,
4. "Market share of smartphone OS of total smartphone installed base in 2013 and 2014". Statistica. Retrieved February 18, 2015. And "Smartphone OS worldwide by installed base in 2014 (in millions)". Statistica. Retrieved February 18, 2015.
5. Global mobile statistics 2014 Part A: Mobile subscribers; handset market share; mobile operators". mobiThinking. May 2014. Retrieved September 9, 2014.
6. Rowinski, D. (December 10, 2013). "The Post-PC Era Begins In Earnest Next Year: In 2014, smartphones will most likely eclipse PCs in terms of the number of devices in use around the world". readwrite. Retrieved September 9, 2014.
7. Android tops 81 percent of smartphone market share in Q3". Retrieved November 4, 2013.
8. Yarow, J. (March 28, 2014). "This Chart Shows Google's Incredible Domination Of The World's Computing Platforms". Retrieved April 23, 2014.
9. Žarković, M. Ivanović, Z. Kriminalistička takika Beograd, 2014.
10. "StatCounter Global Stats – Browser, OS, Search Engine including Mobile Usage Share". statcounter.com.

INTERNET SOURCES

11. http://gs.statcounter.com/#mobile_os-ww-monthly-201601-201601-bar
12. http://www.nutspace.com/products/nutmini
13. https://www.bluetooth.com/what-is-bluetooth-technology
14. https://en.wikipedia.org/wiki/Near_field_communication
15. http://www.prometech.eu/products/tag-trace/
16. https://en.wikipedia.org/wiki/Swarm_behaviour
17. https://en.wikipedia.org/wiki/Collective_animal_behavior
18. http://www.public.asu.edu/~huanliu/papers/IS10.pdf
19. http://eonix.be/nanotics/
20. https://www.bluetooth.com/
21. https://en.wikipedia.org/wiki/Android_(operating_system)
22. https://en.wikipedia.org/wiki/4G#Data_rate_comparison

UDC: 004.912(497.11)
35.077::004(497.11)

TECHNIQUES OF CYBERSPACE INFORMATION SEARCHING IN SERBIAN TEXT DOCUMENT: CASE STUDY FOR CRIME LAW

Vojkan Nikolić[1]
Predrag Djikanović
Slobodan Nedeljković
Ministry of the Interior of the Republic of Serbia, SATIT

Abstract: The Government of the Republic of Serbia in the process of developing e-Government implemented a large number of e-Government services. Everyday people use these services and produce large amounts of data and text documents. Text documents are usually in HTML, PDF and Microsoft Word format and in the Serbian language. With the increasing amounts of text documents in e-Government, the Republic of Serbia needed e-Government services for drawn data and information from a variety of existing text documents that are usually in the format prepared for printing. For the technical realization of this case study a special application that includes Lucene library spaces is specifically developed. Lucene is a great tool for indexing and searching large amounts of information quickly. The procedure quick search of the unstructured text documents in the Serbian language contributes to the detection and processing of criminal offenses in order to increase the level of security in the Republic of Serbia. In this paper, the authors deal with the possibilities of Lucene indexing and Lucene searching of data and documents of the crime unstructured text documents in e-Government in the RS Serbian language in order to find elements of crime in Cyberspace.

Keywords: text mining, natural language processing, unstructured data, Apach Lucene

INTRODUCTION

Many expansion of the Internet as the main medium for the exchange of information and its availability encourage more people to create and share data, information and knowledge. Considering that the Government of the Republic of Serbia (RS)[2] in the process of development of e-Government implemented[3][4] a large number of eGovernment services, daily using these services people produce large amounts of data and documents. A large amount of it is in the form of text in text documents and there is a need for eGovernment services to data and information drawn from a variety of existing text documents that are usually in the format prepared for printing[5].

1 E-mail: vojkan.nikolic@mup.gov.rs.
2 The strategy and action plan for the development of electronic administration until 2013 ("RS Official Gazette", Nos. 55/05, 71/05-correction, 101/07 and 65/08).
3 V.Nikolić, P. Đikanović, D. Batoćanin, e-Government Republic of Serbia: The registration of motor vehicles and trailers, YU INFO 2013.
4 V.Nikolić, J. Protić, P. Đikanović, G2G integraatioin MOI of Republic of Serbia with e-Government PORTAL, ETRAN 2013.
5 D. Randjelovic, B. Popovic, V. Nikolic, S. Nedeljkovic, Intelligent search terms in the case of police services in eGovernment, New information technology for analitycal decision-making in the biological, economic and social systems, (M44), State university in Novi Pazar, 2014.

If we are interested in a topic or area of e-Government RS, considering the amount of documents simply would not have had enough time to read all of these documents and even less would have been able to "get out" important information located in them. It is obvious that there is a need for the selection and separation of information.

One approach to this problem is the process of text mining (Eng. text mining).[6] Depth analysis of the text refers to finding interesting and nontrivial information and knowledge in unstructured text documents, then their grouping and classification. Natural language, which is usually found in the documents, is not suitable for analytical processing, a text in the document is unstructured. These documents can be processed on a computer that must be adapted and prepared for computer processing. It involves a series of activities and procedures of the text documents, which together make the process of preprocessing.

The concepts and application of the Natural Language Processing (NLP) can be seen as a set of techniques and methods for automatic generation of texts in a natural language. This concept is applicable and supports many languages. Trends in the development of e-Government indicate the necessity of application of NLP in the e-Government services of the Republic of Serbia[7][8].

Lucene library spaces were used[9] for the technical realization of the indexing process and the subsequent process of searching through information of the unstructured data in e-Government in the RS Serbian language. Lucene allows to index any text document realized in a free form and can be used with virtually any data source, as long as we can extract textual information. Lucene is used for indexing and searching data stored in HTML documents, Microsoft Word documents, PDF files, and so on. The greatest amount of unstructured documents in e-Government RS is precisely in these formats.

In this paper, the authors deal with the possibilities of Lucene indexing and Lucene searching of data and documents of the crime unstructured text documents in e-Government in the RS Serbian language in order to find elements of crime in Cyberspace.

LUCENE ARHITECTURE

Information Retrieval (IR) library. Information retrieval refers to the process of searching for documents, information within documents or metadata about documents. Lucene lets you add searching capabilities to your applications. It is a mature, free, open-source project implemented in Java; it's a project in the Apache Software Foundation, licensed under the liberal Apache Software License. As such, Lucene is currently, and has been for quite a few years, the most popular free IR library.[10]

Applications such as Amazon are among the commercial application that uses Lucene for indexing and allowing effective searching. Lucene is able to index text from a various formats such as PDF, HTML and Microsoft Word, and also in various languages[11]. One of the Lucene concepts is presented in Figure 1.

6 Gerald Kowalski, Information Retrieval Architecture and Algorithms, The Springer International Series (2011).
7 Peter Teufl, Udo Payer, Guenter Lackner, From NLP (Natural Language Processing) to MLP (Machine Language Processing), Computer Network Security (2010).
8 Z. Stevic, M. Rajcic-Vujasinovic, I. Radovanovic, V. Nikolic, Modeling and Sensing of Electrochemical Processes upon Dirac Potentiostatic Excitation of Capacitive Charging/Discharging, Int. J. Electrochem. Sci., 10 (2015) 6020-6029.
9 V. Nikolić, B. Markoski, M. Ivković, K. Kuk, P. Djikanović, Information retrieval for unstructured text documents in Serbian into the crime domain, str. 6., CINTI 2015.
10 E. Hatcher, O.Gospodnetić, M. McCandless, Lucene in action, Manning Publications, 2009.
11 Paul, T. (2004). The Lucene Search Engine. http://www.javaranch.com/journal/2004/04/Lucene.html.

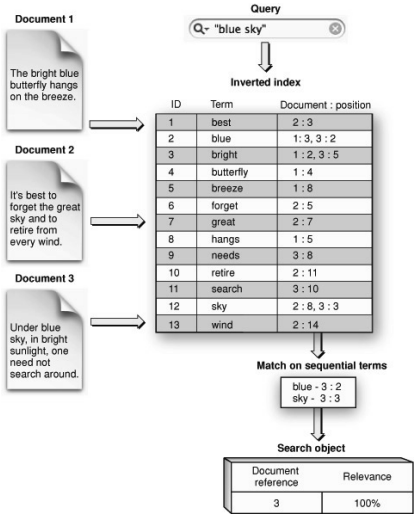


Figure 1: *Basics of search engine*

THE PROCESS OF INDEXING

The process of indexing consists of several procedures and operations that make the Lucene indexing method[12]. All these operations are discretely separated into three operational groups, which are shown in the following Figure 2:

- extracting text from the document,
- analysis,
- adding to the index.

Essentially each of these groups are quite different and relatively complex operations. The first step in indexing is to extract the text from the original document content. Then, the extracted text is used to create the document. The resulting document is made up of fields. Such developed text fields are analyzed and a set of tokens is formed. The last step in the indexing of text documents is to combine tokens with the corresponding indices.

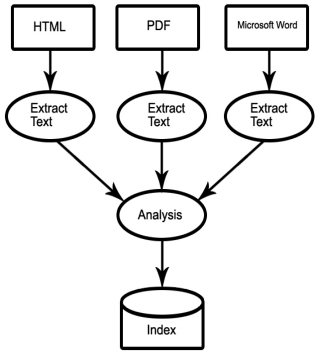


Figure 2: *Indexing with Lucene*

12 V. Nikolić, S. Nedeljković, P. Djikanović, Information retrieval for unstructured text documents: Lucene indexing, EUROBREND 2015.

Extracting text from the document

In order to index the text with the help of Lucene, we have the right to "draw" the plain text, the format in which it can be processed by Lucene, and then create a Lucene document. Suppose that the index you want to add some indexes in PDF format. To create such a document to index, you must first use the method to extract the information in the form of text from PDF manuals and then the extracted text is used to create documents. Also, if you want to add text index in Word, or any other document that is not in full text format. Also, if handled with HML or HTML documents using plain text characters, you need to properly prepare your data for indexing. When you get the text that you want to index and create a document with the fields, the text needs to undergo a process of analysis.

Analysis

The analysis of converting text data into the base unit time is called token. This is the process of converting raw text in tokens. With Lucene this is achieved by using Analyzer, Tokenizer and Token Filter classes. Tokenizer is responsible for the input of component pieces, the tokens. Token filters can further modify the tokens produced by the tokenizer.

Once you create Lucene document fields, you can invoke the Index Writer. After that, Lucene first analyzes the text, then text data divided into tokens, and then can perform a large number of operations with them. Lucene filter performs a search for a specific word or set of words that can be written small and capital letters.

During the analysis, text data passes through several operations: the removal of common words, ignoring punctuation, words reduce the root-form, the changing of words to lowercase, etc. The analysis takes place immediately prior to indexing and query. The analysis converts text data into symbols, and these symbols are added to the terms of the Lucene index.

Lucene library contains a variety of built-in analyzer. Some of them are: SimpleAnalyzer, StandardAnalyzer, StopAnalyzer and SnowballAnalyzer. They are different in the way they treat text and mode of application and the type of filter used. Such analysis can have advantages, the removal of preindexing, decreasing the size of the index, it can have a negative impact on processing precise queries. By applying Lucene it is possible to have more control over the process analysis using custom analyzer.

Adding to the index

After analyzing the input text, Lucene index is corrected. Lucene uses the data structure known as an inverted index. Inverted index uses both disk space and enables faster lookup key time. Its structure is inverse, because the tokens that are used are extracted from the input form document in the form of lookup keys. This mechanism ensures that the document is not treated as a central entity. This means that it directly seeks concrete word instead of scanning the entire document.

Rank-based measures

Lucene's default scoring system works very well for most cases. It uses seven different variables to determine the final ranking of each document. They are (from lucenetutorial.com):

- tf = term frequency in document = measure of how often a term appears in the document,
- idf = inverse document frequency = measure of how often the term appears across the index,
- coord = number of terms in the query that were found in the document,
- lengthNorm = measure of the importance of a term according to the total number of terms in the field,

- queryNorm = normalization factor so that queries can be compared,
- boost (index) = boost of the field at index-time,
- boost (query) = boost of the field at query-time.

CASE STUDY

The Criminal Code of the Republic of Serbia consists of 36 chapters and considers the issues of guilt and sanction provisions in relation to criminal offenses. One of the segments covered by this Code are injuries. They are processed in code in many aspects. This study is based on the possibility of bodily harm, three members chosen for our further research. These are: a) Serious bodily harm Article 121, b) Common assault and Article 122 c) Coercion Article 135 of the Criminal Code of the Republic of users Serbian representatives of the Serbian government, citizens, representatives of businesses, lawyers and others. For the interpretation of this Code it is essential to define the meaning of physical injury by major users.

Fundamentally it uses a great deal of intelligence to determine which Documents are most important to you based on your query. For our experiment, we used the Criminal Code RS, which is written in Latin script in the Serbian language. It, in contrast to the English language, contains the following characters: č, ć, ž, đ and š.

For these characters to be identified and subsequently for the process of indexing to be executed, it is necessary that Lucene be supported for the Serbian language. This support has Lucene 5.2.0 version that we used. For this version of Lucene there is also editor in which it is possible to monitor the indexing and later retrieval. This is LUKE 5.2.0. Luke is a handy development and diagnostic tool, which accesses the already existing Lucene indexes and allows you to display and modify their content and the way to reconstruct the original document fields, edit them and re-insert to the index.

For the purpose of normalization in the context of indexing is used:

public class ***SerbianNormalizationFilterFactory***

extends TokenFilterFactory

In this experiment StandardAnalyzer Lucene 5.2.0 is used. If you use StandardAnalyzer (), then by default uses the STOP_WORDS_SET, which is a set of basic English stop-words.

Considering the text of the Serbian language, we could directly use StandardAnalyzer (). For our purposes, it was necessary to include stop-words Serbian language. This was done by inserting a new argument set to StandardAnalyzer () and defining over CharArraySet as follows:

CharArraySet set = IndexFiles.fromFileToCharArrraySet(stopwPath);

Analyzer analyzer = new StandardAnalyzer(set);

Using CharArraySet is possible to stop-words reintroduced into the text file stop.txt and in the code only define the location where this file through stopwPath. Actually we only defined paths .txt files where they are. The code is defined as follows:

String docsPath = “D:/Na1”;

String stopwPath = “D:/NaS/stop.txt”;

String indexPath = “D:/Na”;

docPath is the way where we accommodate the input document to Lucene indexes, stopwPath input document Serbian stop-words and the places indexPath Lucene index files.

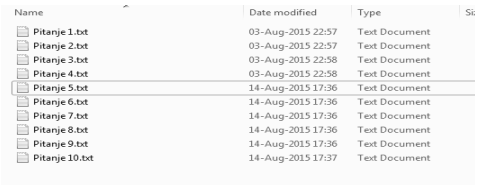
Stop-words we have added about 700 most common words: koju, koje,... A part of this list is shown in Figure 3.

Figure 3: *Stop words*

Experimenting with the scoring system in Lucene may determine relevance of some document to the query. We can see in Luke how often a query term appears in a document. Using Luke, we can open up our index and see its content. It should give us statistics on the elements, number of documents indexed etc. Luke can also be used to run raw Lucene searches against our index[13]. Top ranking terms on the right we see the terms stored most frequently in field of Luke named_content.

The main part of our evaluation process is calculating the AP values of all queries. These AP (Average Precision) values are then averaged over the queries to find MAP (Mean Average Precision) values of each index. Therefore, it is important to clarify this process with an example calculation.

We started the evaluation process by preparing the 10 queries shown on Figure 4, format Pitanje N.txt. Next to each query, we also put the corresponding keyword query which was actually used in the evaluation. Finally, we ran the queries for all indices and calculated the performance using the MAP metric.



Poštovani, prošle godine su me napala dva mladića, jurila po gradu i posle kilometer su me sustigli nakon čega se desila tuča i tom prilikom su njima nanete teške telesne povrede (prelom jagodične kosti i polomljena vilica). Da li postoji mogućnost da ja budem kažnjen kaznom zatvora iako ni na koji način nisam isprovocirao tuču? Unapred zahvalan

Figure 4: *10 prepared queries*

Before starting to analyze the results, we want to clarify the evaluation queries for those readers who have little or no knowledge about the criminal code. Suppose that we had a query (as one version of root word kaznu) that should retrieve 3 documents (i.e. the set of relevant documents is of size 3).

13 V. Nikolić, M. Ivković, S. Nedeljković, P. Djikanović, Information retrieval for unstructured text documents: Lucene searching, AIIT 2015.

In the query details we see that the input has been parsed into text: "kaznu". We select the single search result by a GUI front-end to the Lucene Luke tool, on the Explain control panel. Lucene's default similarity function is based on TFIDFSimilarity. The following formula (straight from Lucene's Similarity function) illustrates the basic factors used to score a document (Equation 1).

$$score(q,d) = coord(q,d) \cdot queryNorm(q) \cdot \sum_{t\ in\ q}(tf(t\ in\ d) \cdot idf(t)^2 \cdot t.getBoost() \cdot norm(t,d)) \quad \ldots (1)$$

This pops up another window which explains the query score. Here is the text of the explanation:

0.2813 weight(contents:kejriwal in 8) [DefaultSimilarity], result of:

0.2813 fieldWeight in 8, product of:

1.0000 tf(freq=1.0), with freq of:

1.0000 termFreq=1.0

1.1252 idf(docFreq=14, maxDocs=17)

0.2500 fieldNorm(doc=8)

where the ranking score is calculated as 1.0000 * 1.1252 * 0.2500 = 0.2813.

The performance of Information retrieval (IR) systems is a measure which uses several evaluation metrics. Precision is one the most commonly used metrics in the IR world where it basically measures how precisely the system picks the related documents among all documents (Equation 2).

$$Precision = \frac{Relevant\ Retrieved}{Retrieved} \quad \ldots (2)$$

Recall is another widely used IR metric and it is the proportion of the retrieved related documents to the total number of related documents that should have been retrieved (Equation 3).

$$Recall = \frac{Relevant\ Retrieved}{Relevant} \quad \ldots (3)$$

One of the related documents is put back to the 2nd place of the list, another related document is put back to the 3rd place and the final document to the 6th place. Using this information we can calculate the AP (Equation 4) value as

$$AP = \frac{1/2+2/3+3/6}{3} = 0.55 = 55\% \quad \ldots (4)$$

In this equation, 1/2 is the "precision at recall level 2" and 2/3 is the "precision at recall level 3", etc. Note that the AP value will be 100% only if all the relevant documents are retrieved on top of the list [15].

CONCLUSION

The aim of this study was to present the possibilities of access to Lucene indexing and Lucene searching of data and documents of the crime unstructured text documents in the e-Government in the RS Serbian language in order to find elements of crime in Cyberspace. Considering that the criminal activity of the offender is also present in Cyberspace, fast search techniques are important for the detection and processing of criminal offenses in order to increase the level of security in the Republic of Serbia.

In addition, the paper presents the possibilities of technology and Lucene indexing and searching of the unstructured data and documents in e-Government of the Republic of Serbia in the Serbian language. At first it presented data mining and architecture Lucene library spaces, as well as the core Lucene, and then the possibility of its application.

For this experiment a special application is developed that includes specific functions using Lucene, which is carried out Lucene indexing process and subsequent data search. The emphasis is put on three articles of the law relating to the physical violation of the Criminal Code of the Republic of Serbia. The paper used the 10 questions asked by users in relation to these articles of the law. At a special event queries are presented below search results and ranking of the three documents constituting three members related to personal injury Criminal Code RS.

REFERENCES

1. D. Randjelovic, B. Popovic, V. Nikolic, S. Nedeljkovic, Intelligent search terms in the case of police services in eGovernment, New information technology for analitycal decision-making in the biological, economic and social systems, (M44), State university in Novi Pazar, 2014
2. E. Hatcher, O.Gospodnetić, M. McCandless, Lucene in action, Manning Publications, 2009
3. Gerald Kowalski, Information Retrieval Architecture and Algorithms, The Springer International Series (2011)
4. K.Soner, An ONTOLOGY-BASED retrieval system using semantic indexing, Graduate School of Natural and Applied Sciences of Middle East Technical University 2010
5. Lucene (http://lucene.apache.org/)
6. Paul, T. (2004). The Lucene Search Engine. http://www.javaranch.com/journal/2004/04/Lucene.html
7. Peter Teufl, Udo Payer, Guenter Lackner, From NLP (Natural Language Processing) to MLP (Machine Language Processing), Computer Network Security (2010)
8. The strategy and action plan for the development of electronic administration until 2013 ("RS Official Gazette", Nos. 55/05, 71/05-correction, 101/07 and 65/08).
9. V. Nikolić, B. Markoski, M. Ivković, K. Kuk, P. Djikanović, Information retrieval for unstructured text documents in Serbian into the crime domain, str. 6., CINTI 2015
10. V. Nikolić, M. Ivković, S. Nedeljković, P. Djikanović, Information retrieval for unstructured text documents: Lucene searching, AIIT 2015
11. V. Nikolić, S. Nedeljković, P. Djikanović, Information retrieval for unstructured text documents: Lucene indexing, EUROBREND 2015
12. V.Nikolić, J. Protić, P. Đikanović, G2G integraatioin MOI of Republic of Serbia with e-Government PORTAL, ETRAN 2013.
13. V.Nikolić, P. Đikanović, D. Batoćanin, e-Government Republic of Serbia: The registration of motor vehicles and trailers, YU INFO 2013. godine
14. Z. Stevic, M. Rajcic-Vujasinovic, I. Radovanovic, V. Nikolic, Modeling and Sensing of Electrochemical Processes upon Dirac Potentiostatic Excitation of Capacitive Charging/Discharging, Int. J. Electrochem. Sci., 10 (2015) 6020-6029

UDC: 005.52:343.9
343.9.018

CRIME MAPPING AS A STAGE OF THE PREDICTIVE ANALYTICS

Slavisa Djukanovic, MA[1]
Damir Amedovski, MA
Ministry of the Interior of the Republic of Serbia, SATIT

Abstract: Thanks to the rapid and unstoppable trend of the development of information and telecommunication technologies in contemporary society, as well as to the fact that a whole new scientific field Data Science has differentiated, processing of large amount of data Big Data has quite reasonably found a place, role and implementation in the security services, especially in the preventive treatment. Predictive analytics has appeared as an area of the new scientific field. Predictive analytics as a scientific discipline is currently the highest form of scientific application in the security services. It has several stages: consolidation of large volumes of structured and unstructured data, creation of target cubes (data about data), and creation of predictive model based on historical data, extraction of analytical extract and presentation - visualization. Mapping or formation of the spatial dispersion of certain security interesting phenomena and events by using modern IT tools provides a powerful tool in understanding these interesting security events (crimes) and of course a tool for direct actions of the security services regarding prevention. Mapping of some of the most common crimes in the Republic of Serbia in the period from 2011 to 2015 will be shown in the paper by using modern IBM tools which are used in the Ministry of the Interior of the Republic of Serbia. The territorial dispersion of the Republic of Serbia, the Police Directorate for the City of Belgrade, as well as certain parts of the city of Belgrade (New Belgrade) will be shown. The aim of this paper is to show an easy way of immediate preventive police actions in order to reduce the growth rate of the most common crimes in the Republic of Serbia by mapping crime.

Key words: crime analysis, predictive analytics, maps, policy

INTRODUCTION

In this paper we will try to briefly introduce the process of collecting and processing data on crimes committed in the Republic of Serbia in the period from 2011 to 2015. Before the introduction of modern software solutions in the Ministry of the Interior, statistical data processing was reduced to the process of recording, processing and use of crime data. The data were generated by putting questions to the system at specified period. They were in txt format and later they were processed in MS Excel. Probability of error in data processing was very large. After the redesign of the system and the introduction of modern software tools IBM Cognos BI 8.0[2], data processing is fully automated and the probability of error during the processing of large amounts of data is significantly decreased. The first part of this paper is about the organization of data in tables, forms of tables. Connection with ESRI maps through IBM

1 E-mail: slavisa.djukanovic@mup.gov.rs.
2 http://www.ibm.com/analytics/us/en/technology/business-intelligence/ na dan 25.02.2016

Cognos BI 8.0 is shown in picture 1 through spatial distribution of crimes on the territory of New Belgrade in the period mentioned above. For demonstration, robbery under Article 206 of the Criminal Code of the Republic of Serbia[3] is shown as the most massive crime in the Republic of Serbia. Each crime is shown through one table box; that box has its own attributes, place and time of occurrence, method of the crime, perpetrator, victim, damage etc. At the end, the aim of application of the tool IBM Cognos BI 8 is visualization of territorial dispersion of the crime on the map in order to observe certain characteristics in the execution of this crime and all in order to reduce criminal rate in the Republic of Serbia by preventive work and policing.

CRIME ANALYSIS DATA

Data collection and collation are significant components of the crime analysis process, and analysts spend a substantial amount of their time and energy on collecting and preparing data for crime analysis purposes. Police agencies use many different methods for collecting and managing their data, so analysts must deal with data that are in many different formats and of varying quality. This chapter provides a general overview of the most common data types, as well as of the discussion of their use in crime analysis.

To ensure understanding of many of the basic concepts discussed throughout this and the following chapters, brief definitions of some key terms are in order.

A database is a collection of data that have been organized for the purposes of retrieval, searching, and analysis through a computer. Databases can contain seemingly infinite numbers of records of cases. In crime analysis, a record or case would be a crime report, an accident report, or an arrest report. Within a database, the data are organized into a matrix, which is a table with individual cells organized in rows and columns. Each row contains all the information for one particular record (e.g. crime report) and each column contains information about one particular characteristic describing the data (e.g. date, time, location), as in Table 1. The columns are also called variables or fields. Most modern databases, e.g. Microsoft Access, SQL Server, Oracle 11.g.[4] allow users to examine complex relationships among various tables through what are called relational databases.

SECONDARY DATA

Secondary data are data that have been collected previously; such data are typically housed in electronic databases. The use of secondary data is common in crime analysis, because police agencies, city departments, and government entities routinely collect and store data that are relevant to the issues crime analysts examine. For example, police agencies collect crime reports, accident reports, and arrest reports, and city agencies collect data on street networks, keep business registries, and compile information on the usage of utilities, and collect tax and license data. The U.S. Bureau[5] of the Census collects socio-demographic data, such as information about income, education, age, and race. Secondary data may be either qualitative (i.e. primarily narrative) or quantitative (i.e. numeric).

3 Criminal Code of the Republic of Serbia, "Official Gazette of the Republic of Serbia", no. 85/2005 and 72/2009

4 R. Gnanadesikan, Methods for Statistical Data Analysis of Multivariable Observations, John Willey, New York, 1997

5 R. Boba, Crime Analysis and Crime Mapping, Florida Atlantic University, California, 2006

Table 1: *Sample Data Table, Number of crimes under Article 206 of Criminal Code of the Republic of Serbia, on an annual and monthly basis in the Republic of Serbia by year respectively.*

The number of crimes	206
2011	3.370
2012	3.680
2013	3.663
2014	3.107
2015	2.912

2011	1	323	2012	1	375	2013	1	407	2014	1	355	2015	1	286
	2	424		2	370		2	356		2	331		2	325
	3	358		3	386		3	345		3	245		3	303
	4	225		4	322		4	318		4	262		4	198
	5	231		5	235		5	312		5	242		5	162
	6	230		6	207		6	241		6	195		6	197
	7	247		7	197		7	236		7	204		7	146
	8	227		8	204		8	242		8	179		8	162
	9	203		9	237		9	237		9	224		9	237
	10	237		10	295		10	275		10	209		10	275
	11	248		11	389		11	290		11	307		11	265
	12	417		12	463		12	404		12	354		12	356

PRIMARY DATA

Since the secondary data that crime analysts use have been collected for purposes other than crime analysis, they are not always adequate to allow analysts to examine a topic fully. When that is the case, the crime analyst needs to collect primary data – that is, data collected specifically for the purposes of the analysis at hand. Analysts collect primary data through surveys, interviews, field research, and direct observation; such data may be coded and entered into a database or may be left in narrative form.

An example of the collection of primary data is the gathering of information about drug market areas. Typically, a crime analyst who needs such information cannot find it in any existing official database, but needs to collect and organize the data him – or herself. The analyst might conduct interviews with detectives to locate drug market areas and then conduct field observation of the areas to collect data on characteristics, which he or she would then code into a database to be analyzed along with other data (e.g. drug arrest). Another example is a crime analyst's need to identify and document environmental characteristics type of location or neighbourhood. In examining an ongoing problem of robberies at self-serve laundries, for instance, the analyst could record information about characteristics of the buildings and their surrounding areas, such as lighting, access control, and landscaping, and then examine these data to assist police in understanding why particular laundries have been robbed and others have not. For primary data to be both accurate and pertinent to the analysis, the crime analyst must invest explicit effort in collecting the data.

GEOGRAPHIC DATA

Just as police agencies enter crime reports into computer systems, crime analysts enter data about the geographic features associated with crime and other activity into geographic information systems for analysis purposes. After introducing the four types of geographic data, or features, a GIS is used to represent objects or locations: point, line, polygon, and image features. The kinds of data associated with these features, also called attributes, are discussed below.

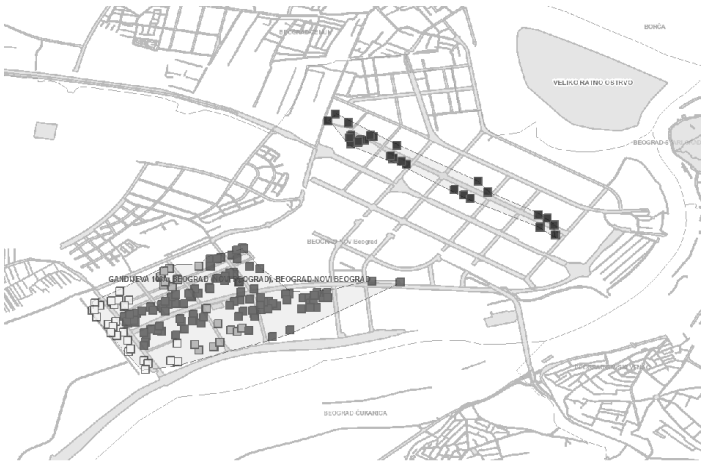


Figure 1: *Point Feature Map*

Point data. A point feature is a discrete location that is usually depicted by a symbol or label, as seen in Figure 2 and it illustrates how a database would display the attribute data associated with each point. In this example the points represent (location of the crime – robbery, in the reporting period). The point circled on the map in Figure 1 corresponds to the first record (row) in the table. The variables in the database provide additional information about that location, such as the street, address, (object of occurrence), and type of location of the street. In Figure 1 annual data are presented respectively, using different colours.

Line data. A line feature is an element that can be represented by a line or set of lines. In Figure 2, the lines represent street segments.

The circled line corresponds to the first record displayed in Table 3. Typically, each record in street data represents a street segment. The variables describe the attributes of that particular street segment and contain the addresses at the beginning and the end of the street segment. The variables "left from" and "left to" contain the addresses that start and end the range on one side of the street segment, and "right from" and "right to" contain the other side's range. The direction, street name, and type of street are also shown.

Data displayed in Tables 1,2 and 3 represent the use of one of the benefits of modern software tool ",drill-down" as an option from the general to the specific display. First we represent the data for the territory of the Republic of Serbia (Table 1), then we represent the data for one municipality which has the highest number of crimes under Article 206 CC RS (Table 2) and finally we represent one segment or part of New Belgrade municipality where this crime is mostly concentrated in location (Table 3) – Hot spots.

Polygon data. A polygon feature is a geographic area represented by a multisided figure with a closed set of lines. The polygons in Figure 3 show police districts.

Table 2: *Point Feature Attribute Data, Number of crimes on the territory of New Belgrade respectively*

The number of crimes	NEW BELGRADE
	206
2011	330
2012	392
2013	329
2014	213
2015	244

2011	1	41	2012	1	36	2013	1	27	2014	1	37	2015	1	15
	2	32		2	39		2	25		2	17		2	29
	3	27		3	45		3	40		3	12		3	16
	4	19		4	46		4	36		4	9		4	15
	5	42		5	28		5	32		5	14		5	13
	6	18		6	29		6	14		6	14		6	20
	7	42		7	15		7	26		7	17		7	11
	8	17		8	21		8	22		8	18		8	24
	9	20		9	34		9	20		9	21		9	25
	10	20		10	27		10	24		10	12		10	33
	11	20		11	29		11	27		11	20		11	23
	12	32		12	43		12	36		12	22		12	20

With the polygon feature, the unit of analysis in the area, so the lines (borders) of the polygon do not have attribute data – only the area itself does. In Table 4, the variable called "feature" describes the type of feature of these data and "district" is the name/label for that polygon.

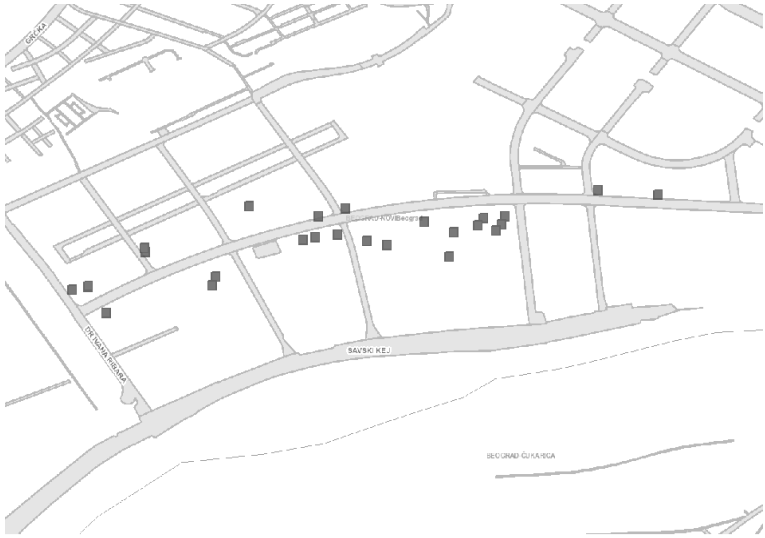


Figure 2: *Line Feature Map, Review of crimes under Article 206 in Jurija Gagarina Street, in New Belgrade municipality.*

Table 3: *Line Feature Attribute Data*

JURIJA GAGARINA STR	14	7	151	2
	14	1	151	1
	33	1	153	2
	78	2	153	1
	81	4	155	1
	110	1	167	2
	123	3	182	1
	131	1	197	1
	133	1	208	1
	134	1	219	3
	140	1	229	1
	141	1	231	3
	147	1	277	1
	147	1	BB	3

Image data. Even though an image feature has attribute data, those data are used only for the purpose of locating the feature within the GIS.

TABULAR DATA

Tabular data describe events that are not inherently geographic, but that may contain geographic variables. Crime reports, accidents, and student information are examples of tabular data. The next section discusses the common types of both tabular and geographic secondary data used in crime analysis.

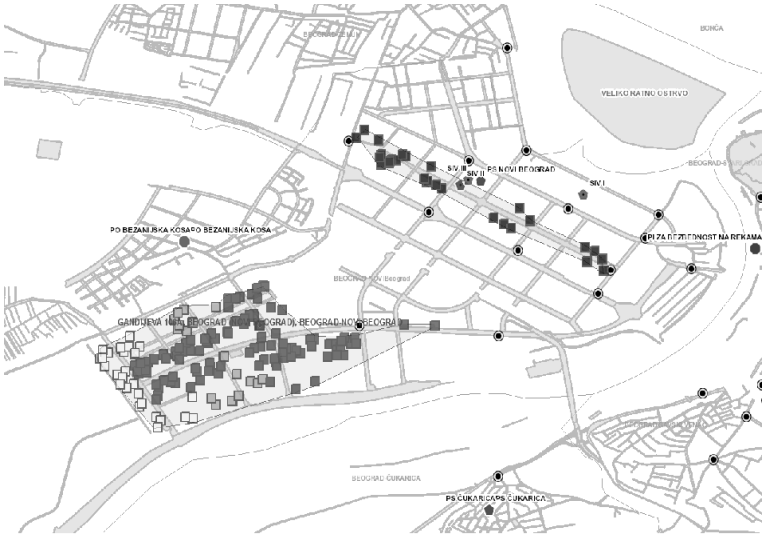


Figure 3: *Polygon Feature Map*

DATABASES USED IN CRIME ANALYSIS

Databases are vital tools for conducting crime analysis and crime mapping because they allow analysts to use computers to analyze large numbers of observations efficiently. Crime analysts use many different tabular and geographic databases, but, for the sake of brevity, only the most commonly used ones are detailed below.

Tabular Databases

Crime analysts use four types of secondary data most frequently: data on crime incidents, arrests, calls for service, and accidents (also called crashes).

Crime Incidents

The data about crime incidents used in crime analysis come from crime reports taken by police officers or other police personnel. Crime reports provide information for other databases that are linked to a crime incidents database, such as suspect, witness, victim, vehicle, and property databases. The crime incidents database contains information from each crime report concerning the nature of the crime, such as the type of crime and how, when, and where the crime has occurred. The unit of analysis is the criminal incident; therefore, there is one record for each criminal incident. Crime incidents databases contain many variables; however, the following are the variables typically used in crime analysis:

- Record number: a unique number used to identify the crime and related information.
- Date of report: the date the crime was reported to the police. Crime statistics tallied with the time when crimes were reported rather than when they occurred.
- Type of crime (state and federal): the type of crime the officer assigned to the event, as dictated by the laws of the state. Often, the corresponding federal code is also included.
- Location of the crime: the address where the crime occurred as well as the area, such as police district or beat and census tract. Some databases also include the type of location, such as vacant lot, single-family home, or commercial business.
- Date and time of occurrence: the date and time when the crime occurred. This can be different from the date of report and can also be a range of time if the exact time of the crime is not known (e.g. burglary, car theft).
- Method of the crime (also called MO or modus operandi): how the crime occurred, such as the point of entry, method of entry, the weapon that was used, suspect's actions. Numerous variables are used to capture this information.
- Disposition: the outcome of the incident (e.g. cleared by arrest, pending). A disposition is assigned when the initial report is written and is then updated if and when an investigation leads to arrest or another status.

Other Databases

In addition to the types of databases above, the following kinds are used less frequently in crime analysis:

- *Property database:* This database contains information about types of property that have been stolen, found, or used in the commission of crimes. The unit of analysis is the piece of property, thus multiple records for property can result from one criminal incident. This database is normally linked to the crime incidents database.
- *Vehicle database:* This database contains information about vehicles stolen, recovered, or used in the commission of crimes. The unit of analysis is the vehicle, and each record includes

information about the vehicle (vehicle identification number (VIN), make, model, colour, and year) and the nature of the incident (data, time, location). This database is normally linked to the crime incidents database.

- *Persons database:* This database contains information about all individuals involved in criminal incidents, including witnesses, victims, investigative leads, suspect (some police agencies have suspect databases that are separate from their persons and arrest databases), and arrestees. In these databases, the unit of analysis is the individual. Each record contains information about the individual (name, birth date, address, physical, description, aliases) and the nature of the contact (e.g. suspect, arrestee, witness, and victim). This database is normally linked to the crime incidents database.

- *Field information database:* Many police agencies collect information from the field through "field interview cards" filled out by officers. This information is collected when an officer determines that a crime report is not necessary, but the agency would like to document this incident outside of the call-for-service record

- *Traffic database:* In addition to accident data, police agencies collect data on traffic citations and vehicle stops. Particularly in the past few years, with the emergence of research on racial profiling, vehicle stop data have become a significant concern for crime analysis.

CONCLUSION

The authors of the paper have tried as much as possible to show the change of approach in the process of recording, processing and use of crime data in order to understand collected data better. The new table design, new options and speed of data processing is also a challenge of new IT tools. Crime mapping or showing the territorial distribution of crimes in a certain area with all the attributes of crime execution is an excellent material in the crime solving process, as well as in the process of using the features of the execution for future cases. Therefore, well collected and processed crime data, as well as their adequate storage in databases is one of very important tools in the process of monitoring the execution phenomenon of such and similar crimes and all that in terms of preventive work of police forces to reduce crime growth rate. By using modern software tools, work with large amount of data is simpler, more accurate, more comprehensive and much faster.

REFERENCES

1. Confronting modern organized crime and terrorism, 3, 4, Criminal Police Academy, Belgrade, 2012
2. Confronting modern organized crime and terrorism, Book 2, Criminal Police Academy, Belgrade, 2011
3. Dragisic, Z.: Organized crime - the way to ochlocracy, Archibald Reiss days, Thematic proceedings of international significance, Volume 2, Academy of Criminalistic and Police Studies, Belgrade, 2011, p. 631-640
4. Djukanovic, S., Milosavljevic, B. Comparative analysis of security assessments, Culture police, KP special edition 2 year 9th, p. 513-525 UDC: 351.86 351.74 / .75, year 2012
5. Djukanovic, S., Gligorijević, M., Subošić, D. Video-conferencing as a means of communication managers in the Ministry of Internal Affairs of the Republic of Serbia, Journal of Safety, Belgrade, 2012, vol. 3, No. 2, p. 248-264 UDK - 004.7: 621.397.4: 354.31 (497.11).

6. Djukanovic, S., Gordon, B., Ranđelović, D. Predictive analytics in police work, Archibald Reiss days, Thematic proceedings of international significance, Volume 1, Academy of Criminalistic and Police Studies, Belgrade, 2015, p.101- 108

7. G. Kvascev, Z. Djurovic, B. Kovacevic, "Adaptive Recursive M-Robust System Parameter Identification Using the QQ-plot Approach", *IET Control Theory and Applications*, vol. 5, no. 4, pp. 579–593, 2011

8. Jovanovic, P., Petrovic, D. Contemporary trends in management development, Faculty of Organizational Sciences, Belgrade, 2007

9. L. Ljung, T. Soderstrom, *Theory and Practice of Recursive Identification*, MIT Press, Cambridge Massachusetts, 1983

10. Milosavljevic, B, Police Science, Police Academy, Belgrade, 1997

11. Petrovic, M.: Management Science, Nis, 2010

12. Randjelovic, D. High-tech Crime, Criminal Police Academy, Book 12, Belgrade, 2013

13. R. Boba, Crime Analysis and Crime Mapping, Florida Atlantic University, California, 2006

14. R. Gnanadesikan, *Methods for Statistical Data Analysis of Multivariable Observations*, John Willey, New York, 1997

15. Teofilovic, T. The political principles of modern national security, Academic Edition, Belgrade, 2012

16. Teofilovic, N, Teofilović, T. Relationship between the government and organized crime, Science and Society Association of Serbia, Belgrade, 2007

17. Criminal Code of the Republic of Serbia, "Official Gazette of the RS", no. 85/2005 and 72/2009

18. http://www.ibm.com/analytics/us/en/technology/business-intelligence/

UDC: 519.17:007.3

USE OF MATHEMATICAL METHODS IN INFORMATION – ANALYTICAL ACTIVITY

Lepiokhin Alexander, LLD[1]
Academy of the Ministry of the Interior of the Republic of Belarus,
Law Informatics Department

Abstract: The paper focuses on some aspects as to obtaining information about criminal activity (including cybercrime) and analyzes it by using mathematical methods, for example theory of graphs to construct relations of events. The basis of this analysis is the introduction of the order parameters as the vertices of a graph, as well as establishment of the relationships and dependencies between the parameters as the edges and the construction on their basis of a graph model of the analyzed events (G = (V, E). The proposed approach can be used in the information-analytical support of law enforcement activity of the Ministry of Interior and the investigation of any crime (including cybercrime) taking into account sophistication of their commission and complexity of detecting them.

Keywords: mathematical methods, getting of the information, analyzing of information, theory of graphs, mathematical models, order parameters.

INTRODUCTION

Current trends, as well as the objective prerequisites of modern society dictate changes in the criminal environment of society, creating new ways and methods of committing criminal acts. Moreover, the information processes that accompany these phenomena cause the focus of attention of law enforcement bodies not only on fixing the illegal activity and the corresponding reaction of the state in the framework of the existing legislation on the disclosure and investigation of crimes, but primarily on the preventive, proactive activities of law enforcement agencies aimed at the implementation of preventive functions of the relevant state bodies. Obviously, for the qualitative implementation of the above activities of the law enforcement agencies, not only information but also analytical support of law enforcement activity must be appropriate.

These circumstances show that in the framework of information-analytical work the emphasis of its implementation from the information component (which is also important) should shift towards analytical support implementation of their functions by law enforcement agencies. The modern reality is constant and repeated increase of information flows and data volumes. Sources of such information include: information from different data bases of the Interior, relevant information to the decision of the official tasks of automated data banks of other state bodies, information formed in the course of activity of internal affairs (reports, certificates, service materials, etc.), information from other government agencies, legal entities and citizens, information from the media, including those posted on the Internet, as well as other sources.

1 E-mail: prav_informatika@mail.ru.

Accordingly, the present phase of development of society is characterized by the explosive nature of the information generated by the growth in various areas, including, and relevant to the operational activity. In fact, under the so-called information redundancy, the question of obtaining information is not acute. Yes, there are questions regarding maintenance of the properties of the information necessary for management decision - timeliness, adequacy and reliability, but more acutely as we believe the question of its timely processing and acting upon the appropriate decisions arises.

Therefore, the implementation of the functions and tasks entrusted to the law enforcement bodies and the bodies of internal affairs depends on the ability to quickly and efficiently process and analyze these large volumes of information and give the final finished product - the optimal management decision.

SOLUTION BY THE MATHEMATICAL METHODS

In our opinion, solution of the problem of improvement of information and analytical support is not possible without the appropriate scientific and methodological support, tools analytical solutions applications. First of all, we need to talk about mathematical models and methods that allow for the selection operation, ranking and verification of information obtained and processed products - analytical documents, and therefore making their decisions based on tactical and strategic.

The analysis of existing approaches to information and analytical work in law enforcement bodies in general, and in the Ministry of Interior in particular, shows that it has a superficial character in general consisting mainly in the comparison of certain indicators of an operational activity with the previous period and in some cases to conduct the factor analysis and development regression models used in the prognostic activities. Without belittling this approach, however, it should be noted that this technique has serious methodological limitations, both in terms of the target activity, and quality of its implementation.

Obviously, there is a need to use other tools in the information-analytical activities. In our opinion, a significant help in this can have the use of tools of mathematical science and above all we should talk about the application of mathematical methods and models in the information-analytical work of law enforcement agencies.

Regarding the application of mathematical models in the information-analytical work should be right to highlight some methodological limitations of their use, as the popularity of this method of scientific knowledge has led to its very active implementation in modeling various socio-economic processes (including, as we believe it is appropriate to speak of the management of bodies of internal affairs). At the same time as we believe it is very important in the development of mathematical models of management of any social process or phenomenon to identify the control parameters of the system, i.e. those effects (changes) have a significant impact on the system.

On the one hand, the traditional models are characterized by a certain redundancy and complexity leading to, what is believed, the cease in expressing the true causal patterns of the development of social processes. On the other hand, such models usually describe the trend trajectory and as a rule do not take into account the point of bifurcation and cannot offer a significant development of the phenomenon of the process, even in the medium term, i.e. they have a fairly limited horizon of forecasting.

Two logical questions with regard to the abovementioned arise and they deal with:

1. The selection of control parameters of the system.
2. The application of appropriate mathematical methods.

Note that the answer to the first question is outside the scope of this report since the extraction and characterization "order parameters" of the system is sufficiently serious scientific problem which is currently at the stage of detailed study.

Answering the second question we should take into account the fact that the tool can be used differently, but it is important to consider it from one side limited character methods for different applications. On the other hand, it is important not to pass the threshold of redundancy, i.e., not to get the model for model without its analytical component.

One of the solutions to the issue of the analytical support of Law Enforcement is to use the provisions of the graph theory.[2],[3] Accordingly, a tool for the analysis of the information is the development in a general form graph model G = (V, E)[4],[5], the definition graph vertices (V1, V2, ... Vn - control parameters – "order parameter") and its edges (E1, E2, ... Em for directed graphs) regarding formation of weighting coefficients impact on the control parameters.

Exercising the formalization of the task information and analytical support, the paper presents a system of the Ministry of Internal Affairs' body in a directed weighted graph G as follows: "order parameters" will correspond to the vertices in a graph, the weighting factors impact on the control parameters will be presented in the form of two oppositely directed arcs (one for each direction), the parameters listed above we define weights arcs.

We introduce the notation:

$GV = \{v_1, v_2, \ldots, v_n\}$ – a plurality of vertices of the graph G;

$GE = \{e_1, e_2, \ldots, e_m\}$ – a plurality of arcs of the graph G;

$GT = \{t_1, t_2, \ldots, t_m\}$ –

A plurality of weights of arcs corresponding to the temporal characteristics of the impact on the parameters of the order:

$GQ = \{q_1, q, \ldots, q_m\}$ –

A set of weights of arcs corresponding weighting coefficients impact on the system:

Thus, the graph model of the system of the Ministry of Internal Affairs' bodies can be represented as follows:

G = (GV, GE, GT, GQ).

2 Emelichev, V. et. al. (1990). Lectures in graph theory / V. Emelichev [et al.]. - M .: Nauka. Ch. Ed. Sci. lit., 1990, p. 384

3 Zykov, A. (2004). Fundamentals of graph theory. – M.: «University Book», 2004, p. 664

4 Araslanov, S. (2013). Graph theory. Lectures and practical exercises: Proc. manual / - Kazan: Publishing House of Kazan. state. arhitekt. univ. 2013 , p. 86

5 Wilson, R. (1977). Introduction to the theory of graphs. Translated from English. M.: Mir, 1977, p. 208

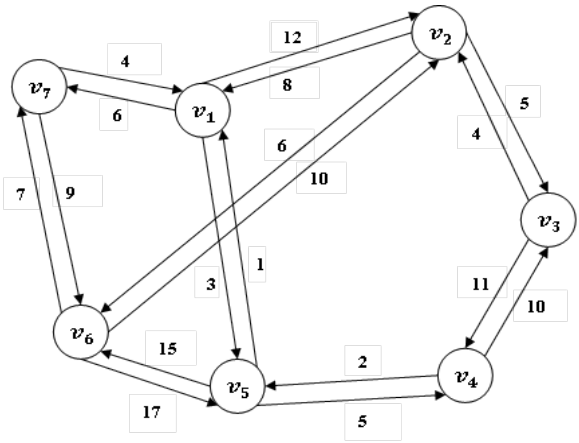


Figure 1: *Example of directed graph with weights coefficients*

An example of the use of graph theory in the information and analytical work can be a criminal scheme links built with the help of specialized software (for example, such as Analyst notebook I2[6] and others), where the vertices are the entities and the arcs will serve as the relationship between these entities.

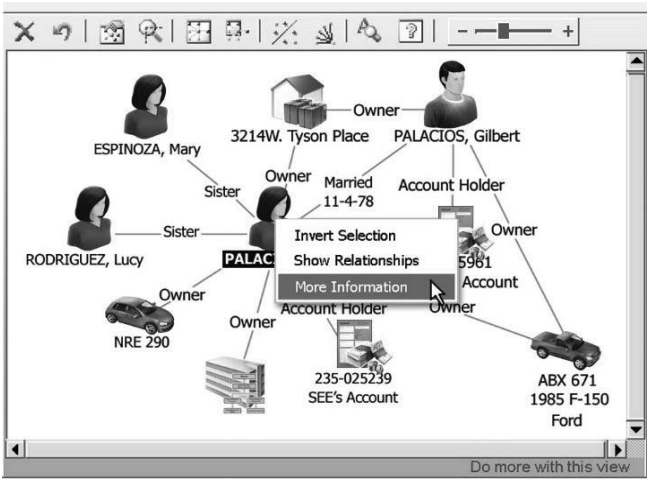


Figure 2: *Example of scheme links of the criminal record*

CONCLUSION

The presented approach is one of the possible solutions to the issue of improving information-analytical activity of law enforcement bodies in general and in the Ministry of Internal in particular. We assume that the use of mathematical methods and models in this activity, and in the first place in analysis of the information, will significantly improve the accuracy of the analytical and forecasting activities in the field of law enforcement activity.

6 http://www-03.ibm.com/software/products/ru/info-exchange-visualizer-sdk date of access:12.02.2016

REFERENCES

1. Araslanov, S. (2013). Graph theory. Lectures and practical exercises: Proc. manual / - Kazan: Publishing House of Kazan. state. arhitekt. univ. 2013, p. 86.
2. Emelichev, V. et. al. (1990). Lectures in graph theory / V. Emelichev [et al.]. - M .: Nauka. Ch. Ed. Sci. lit., 1990, p. 384
3. Zykov, A. (2004). Fundamentals of graph theory. – M.: «University Book», 2004, p. 664
4. Wilson, R. (1977). Introduction to the theory of graphs. Translated from English. M.: Mir, 1977, p. 208
5. http://www-03.ibm.com/software/products/ru/info-exchange-visualizer-sdk
6. date of access:12.02.2016

UDC: 007:004.056
377:004.056

EDUCATION IN INFORMATION SECURITY AS A TOOL FOR ASSURANCE OF CYBERSECURITY[1]

Stanislav Šišulák[2]
Academy of Police Force, Bratislava

Abstract: Cyber security plays a key role in the current security environment aiming at protection of the sensitive ICT-safety, and at the same time, it takes an important position in NATO standards. As the author presumes a rapidly increasing number of security incidents in the near future, education is essential for the security strategy. The education in IT-security should include the following tasks and topics: the safe environment, awareness and competence building in the information security. Education should both provide the comprehensive system of knowledge and focus on its application in the practice. Provided that ICT users have got better skills and abilities, the State can quicker and smoother react on security incidents and prevent or minimize impacts on the sensitive ICT-infrastructure.

Keywords: cyber security, information security, incident, standards, education, infrastructure, management, organisation, user, security awareness, lecturers

INTRODUCTION

Cyber security has become an issue of striking importance. Big cyberattacks permanently constrain the states to undertake more active steps in the sphere of prevention and security. Hereby we mean security incidents which can significantly disorganize and disorient the whole society. All states are currently exposed to the following main security threats: cybercrime, cyber terrorism, political and ideological extremism, hacktivism, cyber espionage, i.e. "cyber fight". Currently, there prevails a high grade of dependence of organizations on information and communication technologies (hereinafter referred to as "ICT") and on electronic data processing. Any ICT-abuse can cause disruption of continuity of organization's operations, and cause serious business losses and minimize return on investment. People are usually aware of the necessity of secure ICT. To secure such developed technologies is rather an expensive matter. We should consider it why organizations are prepared to spend a lot of money for their IT-systems in order to save, make an access to information and transfer them. The thing is that the value of information has significantly increased. It has obviously no sense to spend a lot of money for an equipment serving as a data processor, provided that the information themselves would be valueless. As the US-President **Ronald Reagan** said in 2008[3] "information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified border". Regarding education in information secu-

1 This study is a partial output from the project implementation: "Centrum excelentnosti bezpečnostného výskumu" kód ITMS: 26240120034 supported by the Research & Development Operational Programme funded by the ERDF.
2 Vice rector of the Academy of Police Force in Bratislava, stanislav.sisulak@minv.sk.
3 The Spokesman Review [quot. 2015-12-02] available on: <http://www.spokesman.com/stories/2008/jul/10/information-is-the-oxygen-of-the-modern-age-it/>

rity, we have to admit that many experts on information security are autodidacts. Such way of education would last several years. Information security autodidacts, however, have grown up together with the development of internet and its information security. Regarding the needs of education in the information security, there is a dramatic difference among people, groups and organizations; although any person living in the modern world needs a basic awareness of security of information, not everybody needs the same level of computer literacy. Professionals who are well-experienced with teaching, can usually define better, which fields should be included into the curriculum for specific groups of people. However, if somebody tries to educate the above field without a correctly defined curriculum, he or she or the organization can shortly face difficult problems due to the fact that some people can get either too little education or, corresponding education but not in correct fields, whereas other people spend disproportionate time and means to push their career at the expense of improvement of skills, which are of importance to them. In our practice, we often have to face the fact that a hacker has a better knowledge of the organization's profile and the security of its computer network than the organization's own staff experts do. Moreover, many organizations are even not aware of the fact that they had been hacked a couple of months ago before they found it out. As we do know, to identify hackers is rather complicated as they usually leave the organization through its backdoor.[4] There are thousands of ways of how a hacker or a group of hackers can get an access to the IT-network of any organization. However, there are other thousand ways of how to prevent any undesirable access. There is a single constant way how to prevent it: the education which must be continual. Continual education of each employee of the organization is strongly required, i.e. the IT-education is not a must only for IT-specialists or IT-professionals. Due to a growing threat of misuse of data, everybody should be literate in IT-security, regardless of his/her position, function or rank. The way of how to ensure a systematic education of the society in the field of IT-security is not only a subject to the theory and law but also a subject matter of international conferences throughout the world or of meetings of legislative bodies of individual states. The organizations, which decide to ensure their information security through investments into education in IT-security, can be sure to have undertaken an important step to protect the most endangered information. However, not even the education itself can guarantee the fully functional and effective management system of IT-security, if the organization's management does not actively support the correspondent education and its employees show lack of interest.

IT - SECURITY VERSUS CYBERSECURITY

The above issue is marked by its new terminology as the basis for the identical comprehension of the contents by all users who can understand the same meaning of concrete words in the concrete sphere. A lot of various neologisms have been borrowed from English into Slovak, whereas English original words have undertaken Slovak conjugation and declension regardless the professional meaning of the issue or event themselves. We can state that there is a big number of explanatory dictionaries which aim at the unification and mutual comparison of notions. We cannot, of course, omit specific expressions of various special fields, as well as themes of processes of informatisation. What is the problem of having several definitions?

4 Backdoor is a name of IT-method of bypassing normal authentication, which usually prevents a user from unauthorized access to a computer and its using. Backdoor bypasses standard authentication mechanisms and takes a (typically hidden) method of accessing either a programme or an IT-system. In order to get an access, backdoors can avoid firewall by pretending to be a default browser. This code can look like an individually installed programme, or it can be a modification of the already-existing system (plugin). To get an access, it is enough to enter fictitious user name and password which will be accepted by the hacked system without control, and the system will assign administrator level access to the hacker.

When different definitions are applied in the discussion, it can hardly be stated that they would be correct, sound and complete for parties to the discussion. For example, if a single definition only considers a hardware (computers, mobile phones, networking devices) but the data are ignored, whereas another definition defines both the hardware and the data, one party to the discussion will adopt a conclusion whereas the second party will not, as the definition would be of less importance for the second party. It can even be worse because - in practice – there are many documents used containing the expressions which have not been clearly defined yet. Is there any possibility to work with many different definitions, like e.g. "cyber-room"? Yes, it is possible but it is much more difficult than it should be. Definitely, it is easier if the parties are aware of the fact that the definitions used by them are not identical but, in spite of that, they can take their differences into consideration.

We can state that various organizations use various definitions of the frequently used word of "cyber-room". Some of them have no official definition at all but it seems to be no serious obstacle to discuss it. Discussing a "cyber-room", it is important to reduce its meanings to a single "preferred" definition and to prevent thus any modification of the meaning, and to ensure its single meaning among interested parties. Provided that the expression still would have modified meanings, it would be more difficult to understand mutual position in the fight against security incidents. That is why we are going to deal with some basic expressions. The most frequently used expression is "IT-security". Under informatisation, IT-security is defined as an ability of network or IT-system as a whole, which is reliably marked by resistance against casual events or illegal or wilful acts, which would endanger accessibility, originality, integrity and confidentiality of preserved or transferred data and services provided by or accessible through such networks and systems.[5] Regarding definitions, it is necessary to consider the documents adopted by the Council of Europe and the Security Committee which had been created following the Council Decision 2011/292/EU of March 31, 2011. Its task is to examine and assess security matters related to the Council proceedings and, if necessary, to make recommendations. The Security Committee has three expert sub-groups: information assurance, Global satellite Navigation System (GNSS) and security accreditation. The Council Decision on the security rules for protecting the EU classified information EÚ (EUCI)[6] stipulates that EUCI must be manipulated within communication and information systems in accordance with the conception of information security. Information security throughout communication and information systems means that such systems will protect information manipulated throughout the systems, and they will correctly and timely function under the supervision of authorized users. Effective information security must ensure a good level of confidentiality, integrity, undeniability and believability.[7] A kind of clearness in the definition of expression throughout European rules is given as "Definitions" under Article 3 of the Directive of the EP and of the Council concerning the measures to ensure a high common level of network and information security across the Union (COM(2013) 48 final).[8] The notion of "security" is defined here as the ability of networks or IT-System at a certain level of liability to resist casual events or wilful act, which endanger accessibility, originality, integrity and confidentiality of preserved or transferred data or related services provided by the networks or IT-System, or which are available through networks or IT-System.

5 Ministry of Finances of the Slovak Republic [quotes 2015-12-11] available on: <http://www.informatizacia.sk/informacna-bezpecnost/>

6 EU-classified information (EUCI) [quot. 2015-12-11] available on:<http://data.consilium.europa.eu/doc/document/ST-6488-2015-INIT/sk/pdf>

7 EU-Council, EU. [quot. 2015-12-11] available on:<http://www.consilium.europa.eu/sk/general-secretariat/corporate-policies/classified-information/information-assurance/>

8 EurActiv Information security will be governed by unified rules throughout Europe (Informačná bezpečnosť bude mať celoeurópske pravidlá) [qout. 2015-12-18] available on:<http://www.euractiv.sk/lisabonska-strategia/clanok/informacna-bezpecnost-bude-mat-celoeuropske-pravidla-024630>

Let us examine the difference between cyber and information securities. Obviously, we are not the only ones who are interested in the difference. Both expressions are frequently used and changed by non-IT-staff though their meanings are different. Cybersecurity encompasses the ability to protect against cyberattacks. Cybersecurity is a broad range of legal, organizational, technical and educational means aiming at assurance of cyber-room protection.[9] It is the protection of computers, networks and both the internal and external communication. To work on information security means to assess risks and vulnerabilities. Working on information security means assessment of risks and vulnerability. This assessment is implemented into the management plan in order to reduce problems. The expression of "information security" was used for the first time by the US government. Since that time it has become a definition of technical and management measures which should ensure believability, control, integrity, authenticity, accessibility and utility of information systems.[10] The goal of information security is to protect information and IT-systems and their accessibility, integrity, believability, authentication and confidentiality, as well as update of IT-systems through installation of tools enabling detection and reaction on security incidents. Caution! We have to bear in mind that information security also relates to information of non-electronic character, i.e. security measures also aim at ensuring security of prints.[11] The definition of cybersecurity has not a broad spectrum. It is rather considered to be a part of IT-security. Cybersecurity is taken as the protection of data and systems in networks connected to the internet.[12] The goal of cybersecurity is to ensure the protection of cyber-room at the national level. We will take cybersecurity as a part of IT-security. As the aim of IT-security is to protect any form of information, whereas the aim of cybersecurity is only the protection of digital data**.** The fact that the expression of "cybersecurity" has not been defined in the Slovak Republic yet can be proved by the following text produced during the adoption of the Concept of Cybersecurity of Slovakia in The Years of 2015–2020:[13] "Cybersecurity has been not sufficiently considered yet. It can be proved by the fact there is no formally adopted correspondent terminology for this issue. The word of "cyber" is stipulated neither in generally binding legal regulations, nor in dictionaries of terminology."[14] Further non-defined expressions follow: cyber-room, cyber-risks, cyber-threats, critical infrastructure, critical information infrastructure, national infrastructure. If we further dealt with them, we would go beyond the borders of our educational intention.

9 Cybersecurity National Centre: Explanatory Dictionary of Cybersecurity, 3rd Edition /Národní centrum kybernetické bezpečnosti. Výkladový slovník kybernetické bezpečnosti - třetí vydání [quot. 2015-12-11] available on:<http://www.govcert.cz/cs/informacni-servis/vykladovy-slovnik/>

10 PC Magazine [quot. 2015-12-11] available on:<http://www.pcmag.com/encyclopedia/term/44936/information-assurance>

11 HUDEC, L.: Security Requirements for Equipment & Software for E-Signature, page 7 /Bezpečnostné požiadavky na zariadenia pre elektronický podpis. s.7 [quot. 2015-12-16] available on:<www.lnd.sk/hudec2003-1.rtf>

12 PC Magazine[quot. 2015-12-11] available on: <http://www.pcmag.com/encyclopedia/term/40643/cybersecurity>

13 Concept of Cybersecurity in the Slovak Republic in the years of 2015-2020, Meeting of the Government of the Slovak Republic /Concept of Cybersecurity of Slovakia In The Years of 2015 – 2020, Rokovania vlády Of the Slovak Republic [quot. 2015-01-09] available on: <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24702>

14 Web News: The Government adopted the Concept of Cybersecurity in the Slovak Republic in the years of 2015-2020 /Web noviny Hlavné správy, Vláda prijala Koncepciu Kybernetickej bezpečnosti Slovenska na roky 2015 – 2020 [quot. 2015-01-10] available on: <http://www.hlavnespravy.sk/vlada-prijala-koncepciu-kybernetickej-bezpecnosti-slovenska-na-roky-2015-2020/633726>

ROLE OF THE STATE AND NATIONAL STRATEGY

Information technologies are one of key powers which change the world to a better place of living. Equal positive changes can be brought by the IT to the world and work of public service. In the Slovak Republic various state authorities are responsible for information security. National Security Authority (NBÚ) is responsible for classified information. All other information including "non-classified", as well as the whole electronic environment, is controlled by the Ministry of Finances of the Slovak Republic**.** Due to informatisation of the society of the Slovak Republic and in order to ensure information in all fields comprised into the notion of "informatisation of society", the Ministry of Finances of the Slovak Republic, as a central state authority responsible for informatisation of society, established its own website.[15] Its task is to provide the updated information about the activities of the Slovak Republic and the EU in the field of informatisation of society, about the news in electronic public service (eGovernment[16]), about the activities of informatisation for citizens and businessmen, about supporting availability of broadband internet, as well as public special and professional texts, overviews and characteristics of fields of information society, as well as governmental documents and materials of NGOs, polls, statistics and information about events related to informatisation of society. The main document which started dealing with information security in the Slovak Republic was the "National Strategy for Information Security of the Slovak Republic"[17] stipulating the following main task of the Slovak Republic in the field of information security: to establish the platform of building the information society based on assurance of corresponding protection and believability of digital environment in the Slovak Republic. Based on this document the State is further committed to create organizational, personnel, material and technical, as well as financial conditions for the protection of national information-communication infrastructure and information systems of public service especially aiming at prevention, effective reaction on security incidents and sustainable level of information security in the Slovak Republic. The document which governs education in information security based on the national strategy is called "System of Education in the Field of Information Security in the Slovak Republic".[18] The document focuses on increasing awareness of information security as the basic prerequisite for creating the environment of using information-communication technologies. To promote information security, the Ministry of Finances of the Slovak Republic as a managing authority responsible for information security in Slovakia, makes a regular survey of the status quo of information security and checks the protection of information and activities in the electronic environment of a bright spectrum of respondents. The survey is made in organizations. Households have not been included yet. Such surveys have been made since 2011. According to the last survey,[19] which focused on the status quo of information security in the public administration, the problems in the Slovak Republic are the result of the current regulations and the generally low awareness of information security. As organizations, especially financial institutes, are afraid of losing their good

15 Ministry of Finances of the Slovak Republic [quot. 2015-12-12] available on: <www.informatizacia.sk>
16 eGovernment - is defined as electronic performance of public administration via ICT. eGovernment is a way of applying means and tools of information technology (especially of internet) aiming at improvement of public service for citizens, entrepreneurs and the whole society. [quot. 2016-01-02] available on: <http://portal.egov.sk/sk/content/egovernment>
17 National Strategy for Information Security of the Slovak Republic [quot. 2016-01-02] available on: <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=12150>
18 System of Education In The Field of Information Security in the Slovak Republic approved by the Government of the Slovak Republic on May 207th, 2009 [quot. 2016-01-02] available on:<http://www.rokovania.sk/ Rokovanie.aspx/BodRokovaniaDetail?idMaterial=6876>
19 Current Status Quo in the Field of Information Security in Public Administration in the Slovak Republic, Parliamentary Courier / Parlamentný kuriér/ CCXXVI. – CCXXVII. No. 2014 p. 50–51

reputation, the incidents occurring in the field of information security are not being reported. Another reason is not sufficient a level of professional skills of the staff of public administration, as well as of operators of critical elements of IT. The different levels of professional skills and knowledge build barriers for information and for sharing information. The details from the level of information security in the public administration are available on the website of the Ministry of Finances of the Slovak Republic (www.informatizacia.sk) and on the website of CSIRT.SK[20] (www.csirt.sk). To remain objective when taking into consideration the above survey, we should read the "Declaration on the Status Quo and Survey on Digital Literacy of Citizens" issued by the Slovak Information Society.[21] The Declaration states that surveys and statistics based on subjective self-evaluation cannot be a reliable basis for working-out a strategy for education at secondary schools and lifelong learning. Real verification and confirmation on digital skills can only be obtained through their objective verification based on standardly required scope of such skills in individual spheres of ICT-application.

LEGISLATION, NORMS, STANDARDS AND TERMINOLOGY

Legislation, norms, standards and terminology are the basic ICT-elements, which are irreplaceable for the effective and systematic protection of information with regard to the ICT-development.

Legislation

Informatisation of the society is an inseparable part of information security, and is governed at the legislative level of the EU and at the level of the Slovak Republic. In the Slovak Republic, there are laws, directives, rules, measures and other regulations and decisions which are supposed to be of limited or specific effectiveness if they solve a partial problem related to information security. As this permanent process is comprehensive with regard to implementation of electronic services which have an impact on the whole legislative framework of the Slovak Republic, it is necessary to consequently and regularly analyse individual legal regulations with the aim to achieve their accordance and to remove their discrepancies. For this reason and due to permanently changing rules, we wish to emphasize the importance and the weight of legislation in the process of implementation of information security. All activities leading to the above legislation are managed by the Ministry of Finances of the Slovak Republic. They are completely presented on its website.[22] As the EU-legislation is superior to the national legislation and though individual regulations are of different levels, these documents are published at the above website.[23]

Norms

Norms govern the procedure of information security management. "Best practices" can also be ranked to norms as a list of practical experience which can be applied. Among the

20 Computer Security and Incident Response Team (CSIRT) is set up of experts who strive to provide services required to treat IT security incidents, to remove their consequences and to enable renewed operation of information systems.
21 Slovak Information Society – Declaration on the Status Quo and Survey on Digital Literacy of Citizens [quot.2016-01-02] available on: <http://www.informatika.sk/blox/content/sk/aktivity/nazory#informatizacia>
22 Legislation in the Slovak Republic[quot. 2016-01-07] available on: <http://www.informatizacia.sk/legislativa-sr/684s>
23 Legislation in the European Union [quot. 2016-01-07] available on:<http://www.informatizacia.sk/legislativa-eu/683s>

most important norms, there is an internationally recognized norm - ISO 27000[24] - which stipulates the requirements for setting, introduction, operation, monitoring, examination, maintenance and improvement of the documented system of information security management, whereby overall risks of organization's activities are taken into account. The Norm defines conditions for introducing security measures which can be modified according to the needs of organizations or their parts. The purpose of this norm is to set and monitor the rules for information security and to apply them within the whole security. Supplementary norms to the above information security norm are permanently added in order to consider the specific fields of information security, its management and their specific issues. The extremely quick ICT-development is followed by the accelerated preparation of new norms, which are added to the "ISO/IEC 27000 family" as follows[25]

ISO/IEC 27003 - Information security management system implementation guidance;

ISO/IEC 27004 - Information security management — Measurement;

ISO/IEC 27006 - Requirements for bodies providing audit and certification of information security management systems;

ISO/IEC 27007 - Guidelines for information security management systems auditing;

ISO/IEC 27008 - Guidance for auditors on ISMS controls;

ISO/IEC 27010 - Information security management for inter-sector and inter-organizational communications.

We could list all of them up to the norm ISO/IEC 27037 - Guidelines for identification, collection, acquisition and preservation of digital evidence - which belongs to further norms of this family. Compliance with these norms and their correct application in practice lead to the certification of information security management aiming at increasing confidence among individual entities.

Standards

Individual standards aim at various aspects of information security in organizations. As stipulated under Act No. 275/2006 Coll. on Information Systems of Public Administration as amended, and with regard to informatisation of society, the Ministry of Finances of the Slovak Republic is obliged to determine standards. For this purpose, there was established a Commission for Standardisation of Information Systems of Public Administration under the Ministry of Finances of the Slovak Republic, which is responsible for designing and introducing new standards and changes or cancellation of the existing standards. The implementation of standards reduces the risks of occurrence of security incidents. For this reason, the Ministry of Finances of the Slovak Republic issued a Directive on Standards of IT-Systems in Public Administration, which stipulates the standards for IT-systems of public administration.

Terminology

Not only standards themselves but terminology as a codified use of words and expressions as well, is a significant part of standardisation. The reason is obvious – to enable and maintain interoperability. As mentioned above, a "notion" or a "definition" is a key element in the professional communication among the entities ensuring information security. Non-generally

24 Slovak Office of Standards, Metrology and Testing: STN ISO/IEC 27000 this international norm gives an overview and definition of systems of information security management, which set up a system of norms ISMS, and describes correspondent terminology and definitions. This international norm is applicable to all kinds of organizations (e.g. trading corporates, governmental agencies, NGOs. [quot. 2016-01-07] available on:< https://www.sutn.sk/eshop/public/standard_detail.aspx?id=118557>
25 CIS – Certification Security Information [quot. 2016-01-09] available on:< http://sk.cis-cert.com/System-Certification/Information-Security/ISO-27001/ISO-27k.aspx>

accepted expressions with identical definitions lead to miscomprehension not only in the field of education but also in the whole strategy for information security. It was the Ministry of Finances of the Slovak Republic which issued the first version of Methodical Guidance Note on the glossary of frequent expressions in the legislation and in other materials applied in the field of informatisation of society.[26] The Glossary comprises general expressions in its first version. For the future, the authors will add "optimized" general expressions (using quotes for specific goals) and address concrete spheres of informatisation.

SPECIAL FEATURES OF EDUCATION

ICT-development, knowledge and IT-skills require further support via education focusing on continuous acquisition of multiple skills of citizens. Well-educated people are one of goals and consequences of the modern society. It means in practice that recruitment of organizations focuses on well-skilled and stress-immune persons out of their organization, and at the same time, organizations educate their employees in accordance with their strategic interests and needs. At each time and in each society, education is a process during which persons being educated acquire knowledge, create skills and know-how, and develop their abilities and interests. Output of education is the level of education achieved, and the graduate's new abilities, skills, knowledge, opinions and standpoints. The basic attributes also feature the field of education of information security. Like any professional education, education of information security is marked by its own attributes. We have to bear in mind the fact that each person not only works with information but he or she can also influence its security. For the contents of this education, it is necessary to consider all aspect of information security regardless of the fact whether specific types of information or systems are to be protected. Education in the field of information security is made not only by the state but by other institutions as well. Due to a potential human error, organizations make various types of education in the field of information security. As an example, we can point out to the output of a survey which was made 11 years long by Computing Technology Industry Association (CompTIA):[27] the main failure in security incidents was human element. 80% respondents believed that this failure occurred as a result of absence of security knowledge and trainings or non-compliance with relevant security procedures. Further 51% organizations have confirmed this output during the last two years. Missing knowledge can also be a result of introducing cloud computing,[28] mobility and social media in organizations. Nevertheless, it is worrying that only a few organizations (21%) consider human error as a serious problem. End users use high-efficient appliances and business-class systems[29] often without being supervised by IT-professionals. On the one hand, such users can be able to control and use such sophisticated appliances and systems but, on the other hand, they are not sufficiently skilled and experienced in information security and therefore, they can hardly detect potential threats.

26 Methodical Guidance Note on the glossary of frequent expressions in the legislation for the field of Informatisation of Society Version 1.0 /Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti Verzia 1.0/ [quot.2016-01-05] available on: <http://www.informatizacia.sk/ext_dok-metodicky_pokyn_ glosar_pojmov/3482c>

27 CompTIA 11th Annual Information Security Trends [quot. 2016-01-05] available on: <http://www.slideshare.net/ comptia/comptia-11th-annual-information-security-trends

28 Cloud computing – is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid.

29 Business-class systems – computers offer more functions for professionals like fingerprints, software for remote administration of desk top and encryption tools. Operation system for professionals installed in working computers is better for specialists than for home versions.

Let us put the following question: Would there be any difference between education in information security and education in cybersecurity? Study programmes for these two fields could be similar. Education in information security (which could be called "information security") would give an overview on permanently changing proceedings and challenges which are faced by ICT. The main goals follow:

1. To apply best practical experience and effective procedures related to current security risks.
2. To create and implement the IT-environment in the system of "Defensive Computer Network" in all its basic forms under acknowledgment of individual security attributes.
3. To assess the existing security programmes and systems which can detect threats, and to learn how to prevent such threats.
4. To develop solutions and procedures to be used for maintenance of computer networks and security integrity.
5. To understand the elements and requirements of assurance of information systems as expected by IT-professionals.

As mentioned above, ICT is very strong and it is necessary to ensure professional education required for information security. It is also necessary to focus on risk assessment, which is currently a subject of interest of corporations and governments of individual states. Any education should be supported by practical trainings as theory without practice will always remain theory. Current security threats are various and one cannot adequately prevent them without immediate and correct reaction. It should be a coordination together with prevention, correct reaction and update of security incident plan or security incident series.

At this place, we can give an example of education in information security at the Academy of Police Corps in Bratislava, the Slovak Republic. Information security is a part of the study field of "Protection of Persons and Property" which is a field of the master's study programme "Protection of Persons and Property form the Aspect of Legal Security". During this study, students acquire a good level of knowledge of information security, audit of IT-security system and relevant legislative norms. They acquire knowledge of various forms of IT-protection (physical security, security regime, personal security, security management, management of access to information systems and data, activity and IT-access monitoring, audit, etc.). They acquire knowledge of how to protect sensitive data and classified information (anonymisation and pseudonymisation), which are electronically saved and processed in police IT-systems. In practice, the graduates will be able to apply tools which can help increase security of IT-systems and make security audit. The subject has the following thematic plan and contents:

1. Introduction into information security – meaning of information security, legislative norms and valid standards in the field of information security.
2. Security policy - exercises – security policy and its basic strategy in the organization, basic processes in security policy and basic documents on information security.
3. Organization of security – infrastructure of information security in the organization, secure access by third parties and outsourced security management [30] (the data are processed by another company or organization).
4. Classification and management of activities – exercises – inventory and classification of activities, data and classification of information, classification of environments and classification of communication segments.

30 Outsourcing – the transfer of components or large segments of an organization's internal information technology infrastructure, staff, processes or applications to an external resource such as an application service provider – Explanatory Dictionary and Terminology of IT-Communication /Výkladový terminologický slovník elektronických komunikácií/ [quot.2016-01-08] available on:< http://www.vus.sk/iecd/new/Vyklad_srch.asp>

5. Personal security as the security for labour definition and recruitment, educational process of users and improvement of their security awareness, reactions on security incidents and non-functionality, protection of persons and activities during terroristic acts and other threats.
6. Physical security and security environment – exercises - regime security and protected environments, security and protection of equipment and general measures.
7. Computing and networks administration – procedures of operation, capacity planning for resources of system and system acceptance, protection against malware, backup and archiving information, network administration, media security, media manipulation, information and software exchange and transfer.
8. The access control system – exercises – policy of access control, user access control, responsibility of users, rules for the use of network services, access control to the operating system, control access to applications and systems, monitoring access and use of systems.
9. Systems development and maintenance - safety requirements for information system, security in application software systems, cryptographic measures, security of system files, and security in development and support processes.
10. Plans for continuity of activities (emergency plans) - exercises - process of activity continuity control of society, continuity of activity and impact analysis, elaboration and implementation of plans for activity continuity, structure of plans for activity continuity, tests, maintenance and reassessment of plans of activity continuity.
11. Accord of demands for security policy – lecture + exercise – accordance with legal provisions, examinations of security policy and assurance of technical accord, system audit.

Education in other institutions of higher education and other institutions focusing on information could be demonstrated in a similar manner. Once more, we have to consider the fact that in spite of various providers of education in the field of information security, each of them should respect the valid legislation, standards and use of the same terminology. Education can only be effective when all above mentioned facts are observed.

EDUCATIONAL SYSTEM

Referring to increasing demands of ICT-users, it is necessary to increase their awareness in the field of information processing and using (the protection of digital environment, classified information, personal data, and sensitive data). We cannot ignore the fact that modern ICT enables laymen with no IT-education to work with sensitive data. Implementing education in the field of information security both at schools and out of schools, there has been worked out an educational system of IT-security in the Slovak Republic.[31] The aim is to identify groups of users of digital environment beginning with laymen and ending with specialists, as well as their mission in this environment with a goal to design corresponding contents and forms of education and increasing awareness. The material encompasses the whole digital environment of the Slovak Republic but it does not prepare the specialists for protection of environment defined under the Slovak Act No. 215/2004 Coll. on Classified Information Protection as amended, as it is a closed room. The starting point is the classification of persons who participate in the digital environment and the description of their educational needs. For the definition of categories, it is considered that each participant should acquire sufficient knowledge of information security enabling him or her to consequently carry out his or her

31 System of education in the field of information security in the Slovak Republic [quot. 2016-01-02] available on:<http://www.informatizacia.sk /informacna-bezpecnost/2999s#IB_system_vzdelavania>

duties. Each category covers contents of education resp. curriculum and, at the same time, the definitions of three levels of knowledge (A, B, C) for the categories of participants in the digital environment. A significant part of the education are the forms of education which are covered with professional education and higher education up to lifelong education. Specialists in information security can achieve higher education in all three grades: bachelor, master and doctor studies, and as a combination of higher education (classical and lifelong studies, specialized courses and trainings), trainings and courses in companies for professionals in practice who wish to requalify or upgrade their education in information security. The website of the Ministry of Finances of the Slovak Republic presents the materials from trainings and courses for target groups mainly designed for the participants of courses on information security which are made by the Ministry of Finances of the Slovak Republic. In accordance with the European Cyber Security Month (ECSM), they are available to the professional public.[32]

CONCLUSION

Currently we would hardly find an organization which would not save and backup its key information in some IT-system. Each entity aware of its information wealth cannot neglect the external or internal risks arising from the IT-system, and must deal with information security, whereas education remains the priority. An effective solution requires planning and strategic decisions, as partial investments without a good strategy are not effective in the long term. Cyber-room is a source of new threats for national and international securities. Potential cyberattacks present one of key threats for the current security environment in the Slovak Republic. Certain improvement in this field can be expected thanks to the "Action Plan for Cybersecurity in Slovakia", which is to be carried out by the National Security Authority. This central organ of state administration has been responsible for cyber security in the Slovak Republic since 2016 according to the amendment to the Act on Activities of the Government and Organizations of the Central State Administration.[33]

We have to bear in mind that we have to be prepared and ready to act, even though the Slovak Republic does not belong to the states which are targets of increasing cyberattacks.[34]

REFERENCES

1. Akadémia Policajného zboru v Bratislave, Centrum excelentnosti bezpečnostného výskumu ITMS: 26240120034. Záverečná správa z výskumu. Akadémia Policajného zboru v Bratislave / Kriminalistický a expertízny ústav PZ, Bratislava 2015. Available in the Library Akadémia Policajného zboru v Bratislave.
2. Current Status Quo in the Field of Information Security in Public Administration in the Slovak Republic, Parliamentary Courier / Parlamentný kuriér/ CCXXVI. – CCXXVII. No. 2014 p. 50–51 /Aktuálny stav v oblastiinformation security vo verejnej správe v SR, Parlamentný kuriér CCXXVI. – CCXXVII. Číslo: 2014/

32 Materials for education in the information security [quot. 2016-01-10] available on: <http://www.informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s>
33 § 34 of the Act No.575/2001 on Activities of the Government and Organizations of the Central State Administration as amended. [quot. 2016-01-06] available on: <http://www.epi.sk/zz/2001-575>
34 This study is a partial output from the project implementation: "Centrum excelentnosti bezpečnostného výskumu" kód ITMS: 26240120034 supported by the Research & Development Operational Programme funded by the ERDF.

3. CIS – Certification Security Information [quot. 2016-01-09] available on the internet: <http://sk.cis-cert.com/System-Certification/Information-Security/ISO-27001/ISO-27k.aspx>

4. CompTIA 11th Annual Information Security Trends [quot. 2016-01-05] available on the internet: <http://www. slideshare.net/comptia/comptia-11th-annual-information-security-trends>

5. Council of Europe, EU-Council /Európska rada, rada Európskej únie./ [quot. 2015-12-11] available on the internet: <http://www.consilium.europa.eu/sk/general-secretariat/corporate-policies/classified-information/information-assurance/>

6. EurActiv Information security will be governed by unified rules throughout Europe [quot. 2015-12-18] available on the internet: http://www.euractiv.sk/lisabonska-strategia/clanok/informacna-bezpecnost-bude-mat-celoeuropske-pravidla-024630>

7. HUDEC, L.: Safety Requirements for Equipment for Electronic Signature, p. 7 /Bezpečnostné požiadavky na zariadenia pre elektronický podpis/. [quot. 2015-12-16] available on the internet:www.lnd.sk/hudec2003-1.rtf>

8. Concept of Cybersecurity of Slovakia in the Years of 2015 – 2020, meeting of the Government of the Slovak Republic [quot. 2015-01-09] available on the internet: <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24702>

9. Legislation in the Slovak Republic [quot. 2016-01-07] available on the internet: <http://www.informatizacia.sk/legislativa-sr/684s> Act on Activities of the Government and Organizations of the Central State Administration

10. Legislation in the European Union [quot. 2016-01-07] available on the internet: <http://www.informatizacia.sk/ legislativa-eu/683s>

11. Methodic Guidance Note on the glossary of frequent expressions in the legislation for the field of informatization of society version /Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti Verzia 1.0 [cit.2016-01-05] available on the internet: <http://www.informatizacia.sk/ext_dok-metodicky_pokyn_ glosar_pojmov/3482c>

12. Ministry of Finances of the Slovak Republic [quot. 2015-12-11] available on the internet: http://www.informatizacia.sk/informacna-bezpecnost/

13. Ministry of Finances of the Slovak Republic [quot. 2015-12-12] available on the internet: <www.informatizacia.sk>

14. National Strategy for Information Security of the Slovak Republic /Národná stratégia pre informačnú bezpečnosť Slovenskej republiky/ [quot. 2016-01-02] available on the internet: <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=12150>

15. National Cyber Security / Centre Cyber Security Glossary – 3rd Edition /Národní centrum kybernetické bezpečnosti. Výkladový slovník kybernetické bezpečnosti - třetí vydání/ [quot. 2015-12-11] available on the internet: <http://www.govcert.cz/cs/informacni-servis/vykladovy-slovnik/>

16. Regulation No.55/2014 Coll. – Decree by the Ministry of Finances of the Slovak Republic on Standards for Information Systems in the Public Administration /Výnos Ministerstva financií o štandardoch informačných systémoch verejnej správy/ [quot. 2016-01-09] available on the internet:<http://www.informatizacia.sk/ext_dok-vynos_2014-55_standardy_isvs_s_prilohami/17060c>

17. PC Magazine [quot. 2015-12-11] available on the internet: <http://www.pcmag.com/encyclopedia/term/44936/information-assurance>

18. PC Magazine [quot. 2015-12-11] available on the internet: http://www.pcmag.com/encyclopedia/term/40643/cybersecurity

19. System of Education in the Field of Information Security in the Slovak Republic approved by the Government of the Slovak Repulbic on May 27th, 2009 /Systém vzdelávania v oblasti informačnej bezpečnosti v Slovenskej Republike/ [quot. 2016-01-02] available on the internet: <http://www.rokovania.sk/ Rokovanie.aspx/BodRokovaniaDetail?idMaterial=6876>
20. System of Education in the Field of Information Security in the Slovak Republic [quot. 2016-01-02] available on the internet:<http://www.informatizacia.sk /informacna-bezpecnost/2999s#IB_system_vzdelavania>
21. Slovak Information Society - Declaration on the Status Quo and Survey on Digital Literacy of Citizens /Slovenská informatická spoločnosť - Vyhlásenie k stavu a k zisťovaniu digitálnej gramotnosti u obyvateľstva/ [quot. 2016-01-02] available on the internet: <http://www.informatika.sk/blox/content/sk/aktivity/nazory#informatizacia>
22. The Spokesman Review [quot. 2015-12-02] available on the internet: <http://www.spokesman.com/stories/2008/jul/10/information-is-the-oxygen-of-the-modern-age-it/>
23. European Classified Information (EUCI) [quot. 2015-12-11] available on the internet: <http://data.consilium.europa.eu/doc/document/ST-6488-2015-INIT/sk/pdf>
24. Web News: The Government adopted the Concept of Cybersecurity in the Slovak Republic in the years of 2015-2020 /Web noviny Hlavné správy, Vláda prijala Koncepciu Kybernetickej bezpečnosti Slovenska na roky 2015 – 2020 [quot. 2015-01-10] Available on: <http://www.hlavnespravy.sk/vlada-prijala-koncepciu-kybernetickej-bezpecnosti-slovenska-na-roky-2015-2020/633726>
25. Act No.575/2001 on Activities of the Government and Organizations of the Central State Administration as amended [quot. 2016-01-06].

UDC: 343.533::004
004.491.22
004.056

CYBERCRIME INFLUENCE ON PERSONAL, NATIONAL AND INTERNATIONAL SECURITY WHILE USING THE INTERNET

Igor Cvetanoski, MSc
"Goce Delchev" University,
Military Academy "General Mihailo Apostolski", Skopje
Jugoslav Achkoski, PhD[1]
"Goce Delchev" University,
Military Academy "General Mihailo Apostolski", Skopje
Dejan Rančić, PhD
University of Niš, Faculty of Electronic Engineering

Abstract: The aim of this paper is to stress the danger of cybercrime activities in cyberspace and its impact on personal, national and international security in the 21st century. Insignificant approaches toward this phenomenom may lead to inpredictible consequences even for the state's security.

The new millennium brought information society growth which enabled the nations to be linked in the global cyber space that lead to fast data transfer throughout the world. Globalization of the cyberspace caused new risks and threats which are invisible to the eyes and stealthy to the ears. Cyber-criminals act conspiratorially through the cyberspace; they penetrate in the system privacy and conduct the crime so we are not even aware of becoming the victim of cybercrime attack. Cybercrime starts as personal, but it ends as international security threat.

During the research we will present this term which correlates to cybercrime: crime, cyberspace, cyberwar and etc. We will stress on the motives which encourage cyber-criminals to execute cybercrimes on individuals, private sector/business companies or state institutions. Furthermore, we will define categories and types of cybercrime. Also, there will be present the methods of cybercrime, such as: hacking, social engineering, phishing, pharming, denial of services attacks, distributed denial of services, malicious software usage, adware, steganography and etc. And finally, there will be present some examples of cybercrimes that occurred in the world in order to note that no state is immune to this 21st-century threat.

In the future, cybercrime will grow and become more complex, more serious and will cause more damage due to the development of information - technological society. Today, modern technology gives great opportunity to use the tools of cybercrime that are available online, so practically it is unnecessary to be a computer expert in order to create malicious software for crime activities in cyberspace.

Key words: cyberspace, cyber-criminals, malicious software, malware and virus prevention.

1 E-mail: jugoslav.ackoski@ugd.edu.mk.

CONCEPTUAL DETERMINATIONS OF RESEARCHING SUBJECT

The modern IT society enables global connection of the people through cyber space. Communications through cyber space enable rapid transfer of information, but they increase the risk to be compromised. Cyberspace as a new battlespace creates new threats, warriors and challenges in the 21st century.

Cyberspace consists of hundreds of thousands of interconnected computers, servers, routers, switches and fiber optic cables that allow you to operate their infrastructures and thus correct operation of cyberspace is the basis for the economy and national security. Provision of cyberspace is an extensive undertaking that requires coordinated action and commitment from all stakeholders of society - governments, states, local governments, private sector and citizens[2].

Nowadays, modern societies depend on cyberspace for normal system functioning, especially after the rising role of the Internet. The threat of cyber war and its alleged effects are a source of great concern for governments and armed forces in the world. The fact that several serious cyber attacks are carried out in moments while debating the exact definition of cyber war, can serve as an illustration of what can be expected in the real cyber war in the future. What is characteristic of cyber attacks is that rarely precisely identify the perpetrators of the attacks and even countries that committed those attacks. For these reasons, the perpetrators of cyber attacks are very easy to conceal to another user[3].

Perhaps the movie "Matrix" with Keanu Reeves in the lead role is one of the many stories about the future and the evolutionary process of cyberspace, about the evolution of the war, about the change of the perception of the man to the machine, about the technological development and the development of artificial intelligence, about imaginary switching roles between humans and machines, about the world in which machines manage people, about virtual world created by the progress of machinery using the possibilities of cyberspace and smooth mutual communication through the established network connections.

The scope of this research paper is cybercrime and the basis of its definition is that this type of crime includes any criminal act relating to computers, computer networks and computer systems. The Convention on Cybercrime 2001 of the Council of Europe in its preamble defines cybercrime as "activities that are directed against the integrity, confidentiality and availability of computer systems and data networks, as well as any misuse of these system networks and computer data" [4].

Responsible for cyber attacks are so called malicious hackers. They have a basic objective to penetrate into the computer, data network or computer system through cyberspace, with the ultimate objective, disruption of the stability of the system, taking over control of the system (the so-called zombie system), denial of services attacks, stealing of personal data, stealing of the monetary funds from their own accounts, propaganda, spying, changes to data, abuse of Critical Infrastructure and many other criminal activities with the help of malicious softwares (viruses, worms and etc).

---

2 Vuletic,D. *Cyber warfare as a form of information warfare*. Downloaded on 15th December 2013. http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-32.pdf.

3 Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler. *Democratic governance challenges of cyber security.*Downloaded on 15th December 2013. http://www.fbd.org.rs/akcije/POJEDINACNE/CYBER%20ZA%20WEBSITE.pdf.

4 ETS 185 – Convention on *Cybercrime*, 23.XI.2001. Council of Europe. Downloaded on 15th December 2013. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

It is difficult to understand the motives for committing cybercrime, however, according to some surveys the following grounds are very common:

- Political / religious
- Financial benefit,
- Idealistic (activities which are held only to prove the capabilities without the expectation of reward or a financial benefit)
- Curiosity, adventure (beginners who have not entered the criminal leads, but they do it for fame, without the knowledge and skills)[5].

One of the characteristics of cyber attacks is that it is difficult to identify the perpetrators of the attacks and even countries that committed those attacks.

CYBERCRIME METHODS OF ACTION

Cybercrime is in constant evolution; its forms are changing at high speed, while the types of cybercrime depend only on the aspirations of the attackers (malicious hackers). Cybercrime as crime has differentiated the following main elements:

- Story - what happened,
- Circumstances - as happened
- Mental state of perpetrators of crime is necessary for classification of crime and cyber criminal profiling.

Cybercrime, respectively its main categories can be grouped based on the role of the computer in the execution of the crime, where the computer can be:

- apparent target (unauthorized entry into the computer, data theft)
- means of attack (credit card fraud, sending spam and pictures)
- When connected with everyday crime (trafficking in drugs and people, child pornography, etc.)
- When it is the **base** of evidence for committing cybercrime.

Recent studies have shown that crime associated with computers is increasing every day, which refers primarily to the violation of intellectual property (unauthorized copying and theft of copyright) and piracy of software.

There are many types of cybercrime and some of them are:

- theft of computer services;
- unauthorized access;
- piracy software;
- disclosure, theft and alteration of computer data and information;
- extortion using a computer;
- unauthorized access to the database;
- misuse of stolen passwords;
- child pornography;
- transmission of destructive viruses;
- Industrial and political espionage[6].

5 Gjorgjijevic, N.(2011) Defending Cyberspace: International Law must address Internet – based security threats. *Per Concordiam. Journal of European Security and Defence Issues*, 2 (2), 21 – 27.
6 Milosavljevic, M. and Grubor,G. (2009). *Computer crime investigation - Methodological technological*

For attacking the systems, malicious hackers are using various methods of attack, but the most frequently used are:

- **Hacking** as activity that performs malicious hackers (generally including cyber criminals). The main goal of malicious hackers is to enter unauthorized in the system from the outside or from the inside, and to take unauthorized procedures for authorization and identification, to disrupt the proper functioning of the system, to steal data and information system and sale of stolen information etc. Malicious hackers can be rented from various companies to work as spies for some governments or they may have some connections with organized crime and terrorist groups and so on. The reasons for these actions are different: material gain, revenge, entertainment etc.[7].

- **Social engineering**, this method is using the weakest line of defense of any organization - people. As a new trend this term in foreign literature is known as **people hacking**[8].

- **Malicious software** is software that involves the use of viruses, worms, Trojans, spyware etc.

- **Attacks for access prohibition** (DoS - Denial of Services Attack) are used for blocking the system that is targeted to claim the huge demand for services per time, and the system is not able to answer, because of that it is completely blocked.

- **Fraud bank** card that is on the rise worldwide.

- **Phishing** attacks. These attacks are activities when unauthorized users using fake e-mail messages and fraudulent websites of financial institutions try to mislead consumers about the disclosure of confidential personal data[9].

SECURITY RISKS AND THREATS WHILE USING THE INTERNET

With the emergence and use of the Internet, the term security of computers and computer networks, gets wider, which includes: theft protection of data and network from the attackers known as malicious hackers. The trend of globalization has further impact on security in Information Technology (IT) sector. Undefined legal provisions on security risks and threats in the Internet space at a global level enable safe zones for offenders and malicious hackers. The large number of Internet users make difficult and impossible to search for violators of the laws, relating to the abuse of the Internet. The most common ways of endangering the computers over the Internet are:

- Downloading malicious software that is attached to the e-mail;

- Open ports on the personal computer - PC (mostly due to the already installed malicious software), which can take control of the computer, known as Distributed Denial of Services attacks - DDoS, Denial of Services - DoS, ARP fraud (Address Resolution Protocol (ARP) spoofing), SYN flood (SYN flooding) and the like;

---

base. Singidunum University – Serbia, 291. Downloaded on 15th December 2013. http://www.seminarski-diplomski.rs/biblioteka/Istraga%20kompjuterskog%20kriminala.pdf.

7 Graves, K. (2010). *Certified Ethical Hacker Study Guide*. Wiley Publishing, Inc., Indianapolis, Indiana, 392. Downloaded on 08th January 2014. http://files.laitec.ir/wp-content/uploads/2013/06/CEH-Study-Guide.pdf

8 Beaver, K. (2010). *Hacking For Dummies, 3rd Edition*. Wiley Publishing, Inc. 111 River Street Hoboken, NJ, 386.Downloaded on 15th December 2011. http://www.dummies.com/cheatsheet/hacking

9 CARNet Croatian Academic and Research Network. *Phishing attacks*. CCERT-PUBDOC-2005-01-106., CARNetCERT in association with LS&S.Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-01-106.pdf.

- Visiting suspicious websites (usually placed on free servers) which mostly through Java or ActiveX inserts malicious software on the computer;

- Installing and launching the suspicious programs that have been infected with malicious software;

- Security vulnerabilities in programs that are used on computer (operating system, browser, users of e-mail and so on) that ask daily update (download) of security accessories (update);

- Using the so-called patches (crack) that allow illegal use of software;

- Network identity theft (Phishing) which involves collecting personal data (username, password, number of credit cards, telephone number, etc.) from which the user is not even aware that they are using a fake website;

- Forwarding fake websites (Pharming) with the modification of the local DNS (Domain Name System) server computer that has previously been infected with malicious software;

- Reckless using of the services of social networks: Facebook, Twitter, LinkedIn, Myspace[10]…

When accessing the Internet, the computer sends a message to the appropriate web page and in return expects information for allowed access to it. Often, this feedback brings with it unwanted malicious software created by malicious hackers. Now, the firewall can't recognize what is there inside the packet transmitted in the network. This software thus starts to install on our computer, and can only be slight discomfort or a serious threat to us, our identity and sensitive financial information. Usually, the inconveniences are visible and easy to detect, while dangerous threats are invisible, silent and difficult to detect[11].

The malicious software (Malware) under the definition of NIST (National Institute of Standards & Technology) refers to "program that is often secretly deposited in the system in order to compromise the confidentiality, integrity or availability of the data, applications and operating system or trying another way to harass the victim." In other words, malicious software can be used to delete or destroy valuable information; to slow down the performance of the computer to a complete standstill or spying and stealing important personal data from the victim's computer [12].

Malware includes all malicious programs, such as computer viruses, worms, Trojan horse or Trojan, Rootkit, Backdoor, Spyware, Adware, Phishing, Pharming and others.

Viruses are malicious programs that infect a user's computer without his knowledge or consent in order to cause damage (deletion and destruction of data, programs and operating system) to the computer user. A computer virus is a program code that is placed into individual files of the application or system software. They usually consist of two parts: self-modifying code that allows propagation of the virus and the main code (payload) in which the contents can be harmful. The infection on the computer with viruses can be done through the Internet or through portable devices such as floppy disks, CD, DVD, USB flash drives etc. Polymorphic viruses are those who change their code whenever multiplied in order to avoid the chance to be detected by the antivirus program.

Worms are malicious programs that are written in the working memory of the computer and they remain active. Worms spread by placing identical copies on other computers, in that

10 Nikola, B. (2013). *Security risks and solutions for data protection*. Singidunum University – Serbia, 2013.Downloaded on 15th December 2013.

11 Understanding Internet Security. *What you need to protect yourself online.* 2004 Big Planet, Inc. All Rights Reserved. Big Planet is a registered trademark. Downloaded on 16th August 2014. http://www.bigplanetusa.com/library/bp/pdf/bpis_understanding_security.pdf.

12 The Cyber security handbook. *A cyber security guide.*Downloaded on 06th August 2014. www.NJConsumerAffairs.gov.

way they can in a short time infect a large number of computers. The range of possible damages ranging from causing damage to the operating system (OS), extinguishing the PC slowdown or work with network resources, to open and close the CD/DVD ROM, displacing the characters on the keyboard of the computer etc.

Trojan horses or **Trojans** spread so that site users open programs that are thought to originate from legal sources and background disabling anti-virus program and firewall, and thus allow access to the user's computer[13]. Trojans unlike other malicious software must be activated by hackers over the Internet. The most common operations that a hacker can perform on the computer that is infected with a Trojan horse are:

- Collection and theft of confidential information - passwords, bank accounts, etc.;
- Installing software (including other types of malicious software);
- Download, installation, deletion, creation and modification of files;
- Review of the user's desktop;
- Adding BotNet computer network (DDoS attacks);
- Collecting and downloading the text that is entered through the keyboard (keylogging) and
- Taking the resources of the computer system and its slowdown[14].

Spy programs (Spyware)

There are several definitions of spyware, but the two definitions described form the companies: "McAfee Inc." and "Trend Micro Inc." describe their true purpose and action. According to them spyware programs are:

- "Malicious programs that monitor and collect user data for different purposes" and
- "Malicious programs that send user data to a third party without the knowledge or consent of the user."

We distinguish two types of spyware:

- Legal spyware programs and
- Commercial spyware programs - illegal malicious programs.

Legal spyware programs are those ones that are installed on the computer by the owners of the company, aiming to network administrators be able to monitor the activities of employees.These programs are used for the protection of intellectual property, data and computer networks against threats, and parental supervision of children and juveniles who are present on the Internet (at the request of a parent). Other legal cases for using these programs are its installation for the needs of the competent authorities of the state to monitor terrorists, criminals and other individuals who are suspects that with their behavior and actions violate certain legal frameworks.

Commercial spyware programs are that kind of programs which companies use to collect information on the habits of users when viewing Internet content. These programs are illegal and are proper to collect user information easily. The greatest benefit of spywares has marketing industry, because they are often present and should be taken into account, especially when browsing the Internet, visiting unfamiliar websites, downloading programs from unknown authors etc. Spyware, according to their purpose, can be divided into the following categories:

13 CARNet Croatian Academic and Research Network. *Spyware programs.* CCERT-PUBDOC-2009-10-280. *CARNetCERT in association with LS&S.* Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-10-280.pdf.
14 Nikola, B. (2013). *Security risks and solutions for data protection*. Singidunum University – Serbia, 2013.Downloaded on 15th December 2013.

- Internet URL Loggers,
- Screen Recorders"
- E-mail Recorders,
- Chat Loggers,
- Keyloggers,
- Password Recorders,
- Tracking Cookies,
- Browser Hijackers,
- Modem Hijackers and
- PC Hijackers[15].

Rootkit programs

Rootkit (root- administrator and kit - equipment, tools) is malicious software that can be composed of several programs whose main task is to conceal the reason that the system is compromised, designed in order to surreptitiously take control over the operating system by other malware (eg. Keylogger program). Using the Rootkit does not have to be mean, but the term Rootkit is increasingly associated with undesirable behavior of the operating system and the malicious program. Contrary to what its name form can be implied, Rootkit is not assigning administrative privileges to the user, but provides access, move and modify system files and processes**.**

Backdoor programs

Backdoor is a program that is installed from the viruses, worms or Trojan horses (without the user's knowledge), which is used to bypass authentication (verification process the personal data of the user in the moment of application or connection of the operating system), with the ultimate goal to enable seamless and unauthorized access to the operating system. Backdoor is using the flaws and weaknesses of the operating system. Backdoor Trojans open the "side entrance" the embattled computer and allow unauthorized use of hardware and software resources of embattled operating system.

Adware programs

Adware (ad- advertising, advertisement and ware - programming package) is any software package, some malicious software, which starts automatically, displays or downloads advertisements from the computer while using or after installation. Computers have the ability to collect large amounts of personal data and transferred to third parties including companies and advertising networks. Industry for on-line advertising is big and competitive business, powered by buying and selling of personal data, such as Internet browsing behavior and the nature of the users. There are many ways to collect such information. One way is contracting with the websites of social networks (Social Networking)[16]. Another way is to set the so-called cookies on our search engine to monitor our behavior and interests on the Internet or make an agreement with the research teams of applications for smart phones - that can even use GPS - Global Positioning System to find our location[17].

15 CARNet Croatian Academic and Research Network. *Spyware programs.* CCERT-PUBDOC-2009-10-280. *CARNetCERT in association with LS&S.* Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-10-280.pdf.

16 Nikola, B. (2013). *Security risks and solutions for data protection*. Singidunum University – Serbia, 2013.Downloaded on 15th December 2013.

17 The Cyber security handbook. *A cyber security guide.*Downloaded on 06th August 2014. www.NJConsumerAffairs.gov.

Cookies, pop-ups and adware are tools for monitoring our behavior when we are on-line on the Internet and are used to promote various products. Many cookies are safe tools for the sole purpose of monitoring and collecting information from the Internet. In the most of the cases adware programs are made of pop-up ads that cause nothing else than unwanted nuisances. Problem is that malicious hackers and on-line criminals largely use these tools to access and enter our computer and collect our personal information without us being aware of it[18] .

Some of the data of the user who visits a website are detected through log files. These files register those data targeted at the creator of the website.

Phishing – catching a personal data

Phishing attacks include activities that unauthorized users using false messages in emails and fake websites of some financial institutions (eg. "Ebay", " Paypal", etc.) are trying to mislead the user revealing personal data. In this context primarily refers to data such as credit card numbers, usernames, passwords, PIN codes, etc[19] . Phishing attacks are carried out in several stages: design and preparation of the attack; carrying out the attack and gathering intelligence. Fake emails and web pages that are used for these attacks look very similar to the original. The thing that you can find these attacks is URL (uniform resource locator) address of the fake website. For example, if you visit the "eBay" then the final part of the domain in the URL address should end with: "ebay.com". Accordingly, websites that have the URL http://www.ebay.com http://cgi3.ebay.com are valid web pages, while http://www.ebay.vaidate-info.com and http://www.ebay.login123.com are fake web pages that can be used by phishers. If the URL contains IP (Internet Protocol) address, like 12.30.229.107, instead of the domain name, more than certain is that someone wants to capture (phish) personal data[20].

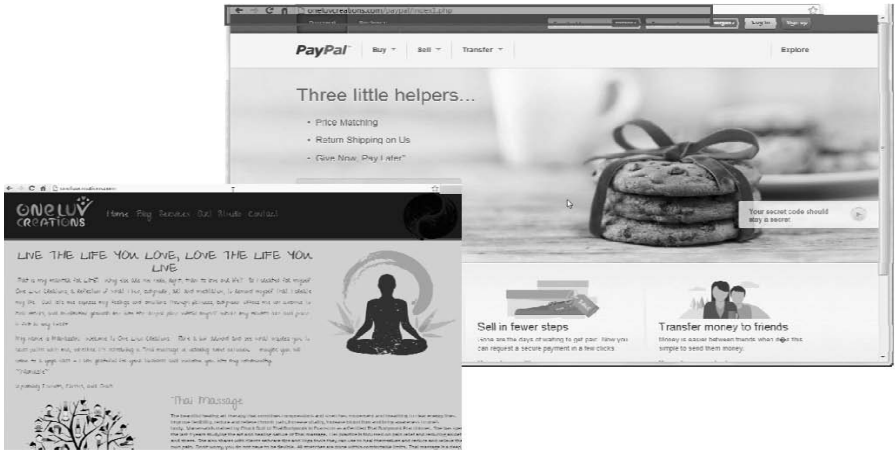


Figure 1: *PayPal phishing site hidden in legitimate site "One Luv Creations"*

18 Understanding Internet Security. *What you need to protect yourself online.* 2004 Big Planet, Inc. All Rights Reserved. Big Planet is a registered trademark. Downloaded on 16th August 2014. http://www.bigplanetusa.com/library/bp/pdf/bpis_understanding_security.pdf.

19 CARNet Croatian Academic and Research Network. *Phishing attacks.* CCERT-PUBDOC-2005-01-106., CARNetCERT in association with LS&S.Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-01-106.pdf.

20 Nikola, B. (2013). *Security risks and solutions for data protection*. Singidunum University – Serbia, 2013.Downloaded on 15th December 2013.

"The New New Internet", a web page for cyber security, in the past period has given a special emphasis to the malicious hackers who have lately been more active on social networking sites and activate phishing attacks by Instant messaging, Facebook, Twitter and other social networks[21] .

Table 1: *Website categories infected with phishing*

Website categories infected with phishing				
Rank	Category		Rank	Category
1	Free Web pages		6	Travel
2	Education		7	Shopping
3	Sports		8	Health & Medicine
4	Business		9	Real Estate
5	Computers & Technology		10	Fashion & Beauty

Pharmning programs

Pharming unlike Phishing directs users to fake websites without the user being aware of it. The phishing Web pages usually use the domain name for your address, while their exact location is determined by the IP address. The user gets to write the domain name into their Web browser and press enter; the domain name is converted into an IP address through DNS (Domain Name Server) server. Thus web browser connects to the server that IP address and takes data from the website. Once the user visits the website, DNS entrance on that side often remembers the DNS cache of computer user. Thus computer must constantly access the DNS server whenever the user wants to access the website.

One of the ways of Pharming is an e-mail that has a code of a virus that infects the local DNS cache user. For example instead of IP address 17.254.3.183 which essentially is the address of www.apple.com, it can be changed to another website by hackers. Pharmers – can infect some DNS servers, which means that any user who uses that server will be redirected to the wrong website. Usually most of the DNS servers have protection measures that protects from these attacks. That however does not mean that they are 100% immune to attacks by malicious hackers. These attacks can act on multiple users at once in cases when large DNS server is modified[22]. Methods pharming and phishing are the best known methods of identity theft and other personal data of the user. Categories of websites that were probably compromised with malware in 2013 are shown in Figure 4th[23].

Table 2: Websites categories infected with malware

Website categories infected with malware				
Rank	Category		Rank	Category
1	Travel		6	Education
2	Transportation		7	Search Engines & Portals
3	Business		8	Arts
4	Sports		9	Restaurants & Dining
5	Leisure & Recreation		10	Real Estate

21 The Cyber security handbook. *A cyber security guide.*Downloaded on 06th August 2014. www.NJConsumerAffairs.gov.

22 CARNet Croatian Academic and Research Network. *Online extortion*. CCERT-PUBDOC-2009-06-268. *CARNetCERT in association with LS&S.* Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-268.pdf.

23 Internet Threats Trend Report – October 2013. *Commtouch.* Downloaded on 17th August 2014. https://www.pallas.com/fileadmin/img/content/publikationen/2013-Q3_Commtouch-Internet-Threats-Trend-Report.pdf.

Scareware programs

The term Scareware marks several classes of programs for fraud, often with little or no profits that are sold to consumers because of some unethical marketing. These programs are made as to cause shock or perception of theft among users. The most frequently used tactic is convincing the user that the computer is infected with a virus so it is recommended to download antivirus program to remove the virus. Recommended antivirus is mostly commercial and users must pay their use. The term programs fraud is often used to describe a product while performing the desired operation and also produce many warnings for the purposes of the application of commercial firewall or programs for cleaning the registry (registry cleaner software). These classes of programs mark and often display continuous warning messages to users. Even more, some websites display windows with new ads (pop-up) or advertisements (banners) with text that emphasizes the user that the computer is infected with malware, and because of that they suggest scanning the computer by clicking on offered window. These programs are not linked with the installed malicious programs; they give false warnings, and are made as coming from the operating system. The user can infect his computer even if he presses the window to cancel or close the message.

Some types of programs that steal user's data are also ranked in the scareware programs because they shift the appearance of the background of the computer, they install icons (for the operating system Windows), and continuously inform the user that their computer is infected with some form of malicious software. Examples of fraud are SpySheriff. It is a program for stealing user data (spyware) posing as a program to remove these malicious programs.

Another form of scareware programs are so called joke programs (prank software) that are intended to intimidate the user to use the unexpected images, sounds or video messages. First distributed program of this type was for computer Amiga in 1991, and was called NightMare. This virus didn't take actions in the same time with booting the operating system, but in random selected period of time altered the entire background and burned horrible sounds. These viruses have recently been designed on that way that display window on which it is written, it will erase all data on the computer no matter of whether that action will be taken or not. However, the actual effect is that these malicious programs are used to intimidate the user, and never delete data from your computer.

Ransomware programs

These malicious programs are defined as programs that exploit the vulnerability of the personal computer in order to break their operating system and to encrypt those files. Once this happens the attacker keeps locked these files till victim's willingness to pay a certain amount of money. If the operating system has previously been attacked by a worm or Trojan horse, an attacker can easily penetrate in poorly configured operating system. In the most of the cases, during the attack usually false messages are used in order to detect the vulnerabilities of used antivirus program and to insert them in the operating system through the most vulnerable port of the system. The next step is contacting the user. The attacker sends an e-mail to the victim or a window appears on the victim's screen with an advertising message that requires encryption key to unlock the files. Very often instructions are given in accordance with the recover data. When the attacker using the tools of ransomware malicious programs takes control of the data, he will encrypt them with a sophisticated algorithm (Figure 2). The decription password is given to the victim in the moment when the certain amount of price is paid (Figure 3). The attacker informs the victim with instructions message for steps which should be taken to recover the data, which is located in the same directory as the encrypted data[24]. At the end

24 CARNet Croatian Academic and Research Network. *Online extortion*. CCERT-PUBDOC-2009-06-268. *CARNetCERT in association with LS&S*. Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-268.pdf.

of 2013 users of the operating system Windows faced such a threat known as "CryptoLocker", which once swept computer encrypt all personal files and folders so that users cannot access the same[25].

Figure 2 : *A "CryptoLocker" notification posted on infected PC*

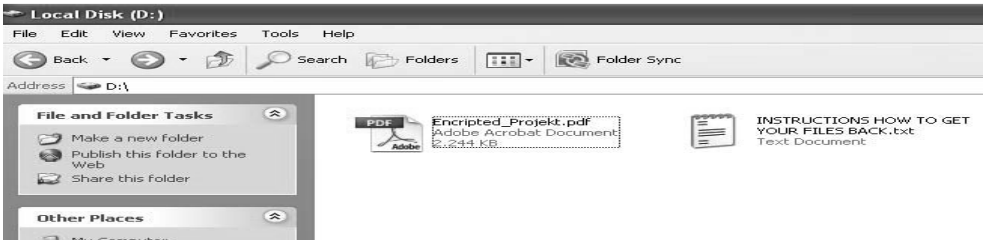


Figure 3: *Guidelines for data recover*

Steganography

Steganography involves concealing secret messages, but no communication between the two sides. This means that the process of steganography usually involves inserting a secret message in a transmission medium that in this case is used as a carrier and its primary role is concealment of permanent secret message. The carrier should be content that does not draw any attention to itself (image, text, audio or video, etc.). The entirety composed of a secret message and a holder where the message is located is called steganography medium or stego. Besides the use of steganography for good causes (protection of intellectual property rights, confidentiality in communications, etc.), very often it is used for illegal purposes as the malicious software transmission is, and could be used for computer endanger[26]. Today, there are many examples

25 New virus locks the data and required to pay $ 300. BusinessInsider. Downloaded on 04th January 2014. http://brkajrabota.mk/tehnologija/internet/30378-nov-virus-gi-zakluccua-komjuterite-i-barada-platite-300-dolari.

26 CARNet Croatian Academic and Research Network. *Steganography.* CCERT-PUBDOC-2006-04-154.

for steganography use in the process of secret communications between terrorist organizations. Other malicious programs not subject to the processing of this paper, that is necessary to be mentioned are: dialer (communicator, elector of numbers), DDoS (Distributed Denial of Service - distributed attacks for refusal of services), botnet network, exploit, keylogging, Boot viruses, hoax (fraud), scam, macro viruses, malware dropper and others [27].

Disgruntled insiders are employees of public institutions or private companies whose objectives are to cause damage to the system or to steal sensitive data for the company in which they are employed. According to the Federal Bureau of Investigation (FBI) in the United States, insider attacks are twice more likely than attacks from third parties[28]. In this context **social engineering** increasingly has been applied. This method exploits the weakest "line of defense" of any organization - people. As a new trend, in foreign literature this term is known as people hacking where the trust of people is abused for personal gains[29].

SOME EXAMPLES OF CYBERCRIME NOTICED IN THE PAST FEW YEARS

Security risks and threats, that are mentioned above permanently exist in the Internet space. For these reasons everyone who is using this space should be aware of the risks and threats that constantly lurk in the ether. Furthermore, there are a few examples of malicious programs that were popular in 2013.

For example, on September 6, 2013, the distributors of malicious software invented false news aiming to attract public opinion about the possibility of US air strikes against Syria. For this purpose messages have used the title "The United States Began Bombing" and were made to look like legitimate newsworthy Broadcasting station "CNN" ("The Cable News Network") of the United States. The trend of these campaigns is that they are becoming faster in real time. The real time to create attack with malware software from examples before Syria till the case in Syria was steadily declining.

In March 2013 when the new Pope was elected, first attack by malicious software started exactly after 55 hours of the election. In April 2013, after the bombings of the Boston Marathon in the US, after 27 hours, in order to attract public opinion the first malicious software attack had been implemented.

In the case of Syria the attackers did not wait, so the attacks were faster than the events on the ground. All this confirm that the Internet has a great power to attract public opinion. Nowadays, the past several military campaigns confirmed the motto "who attracted world public opinion on his side he won the war."[30].

CARNetCERT in association with LS&S. Downloaded on 16th December 2013. http://www.cert.hr.

27 Nikola, B. (2013). *Security risks and solutions for data protection*. Singidunum University – Serbia, 2013.Downloaded on 15th December 2013.

28 United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity," *Science* 326 (13 November 2009): 943-4; See Martin Charles Golumbic, Fighting Terror Online: The Convergence of Security, Technology, and the Law (New York: Springer, 2007).

29 Beaver, K. (2010). *Hacking For Dummies, 3rd Edition*. Wiley Publishing, Inc. 111 River Street Hoboken, NJ, 386.Downloaded on 16th December 2011. http://www.dummies.com/cheatsheet/hacking

30 Internet Threats Trend Report – October 2013. *Commtouch*.Downloaded on 17th August 2014. https://www.pallas.com/fileadmin/img/content/publikationen/2013-Q3_Commtouch-Internet-Threats-Trend-Report.pdf.

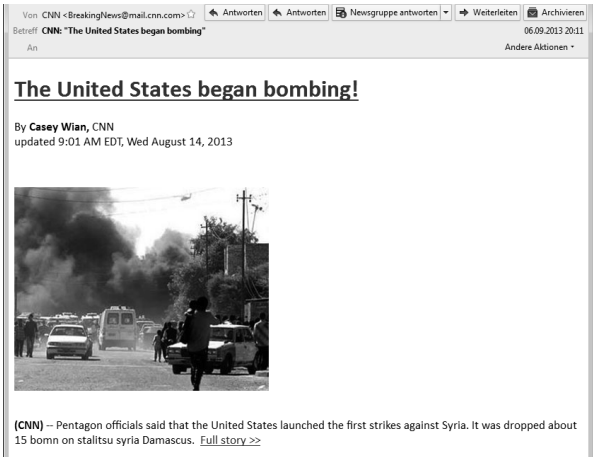


Figure 4: *Fake News Alert in the Name of CNN on Syria Conflict*

The campaign from the end of July 2013 is shown In Figure 5 below, which referred to the arrival of the baby - Prince George ("royal baby") in the UK. This malware campaign was initiated aiming to cause great interest. This news contrary to a previous had all characteristics of web malware software.

This news leads to a page with three hidden links to pages infected with malicious software. The script "<turncoat.js>" in its background activates "Blackhole Exploit Kit" without being noticed by the user. The only visible content on the page was the message "Conecting to server" (Figure 6). "Blackhole Exploit Kit" is one of the favorite tools that are commonly used by cyber criminals nowadays. It scans the target system and then downloads the most appropriate malware software depending on the operating system, browser type, PDF format etc.

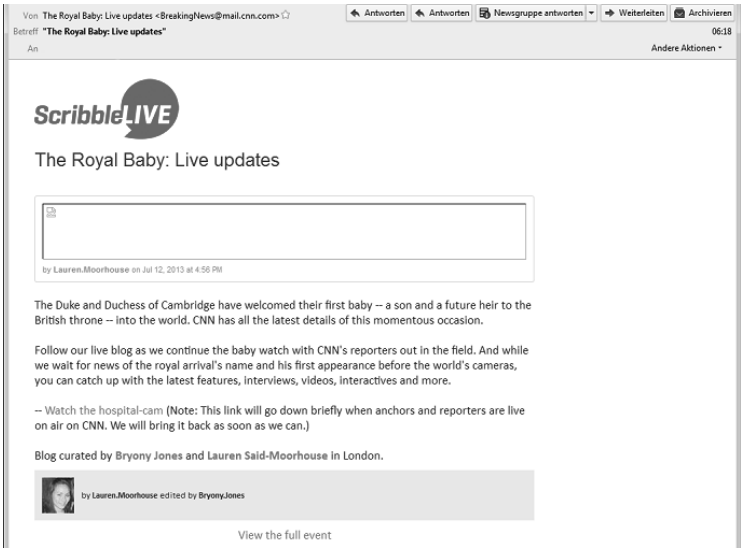


Figure 5: *Fake Royal Baby News Alert*

Figure 6: *Web malware*

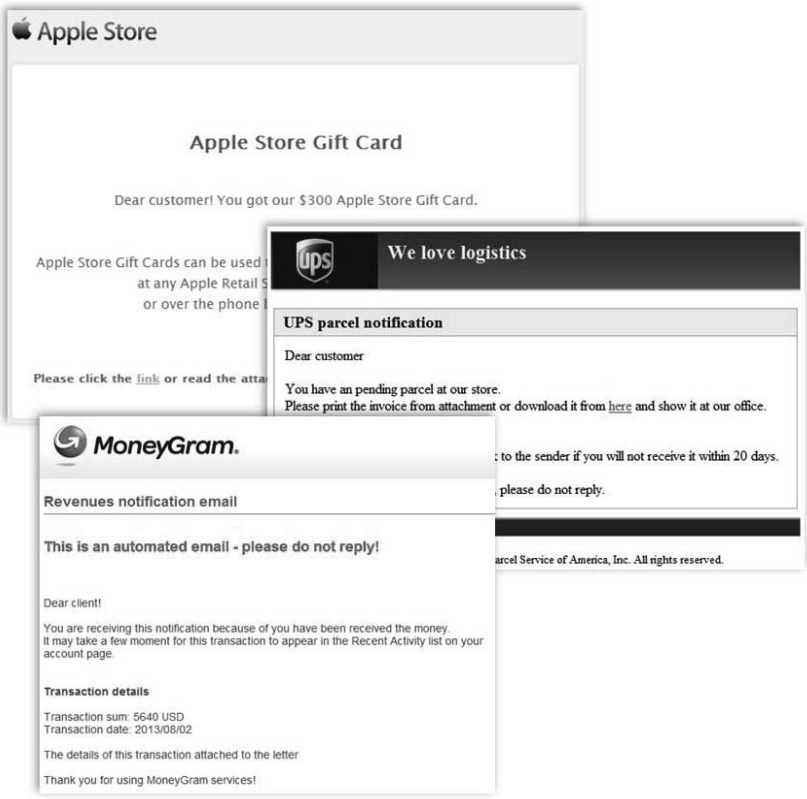


Figure 7: *Samples of emails with attached malware*

As an illustration, in May 2006 the main news in the newspapers in the United States was the theft of data from insurance of veterans. The chronology of this case is as follows: an employee of the insurance company in order to develop appropriate documents necessary for ensuring veterans to not break the given deadlines beyond the prescribed norms and safety rules, has put the relevant data on his notebook (laptop) and took the data to work at home. But in the meantime, portable computer had been stolen from his home with the data in it. The company estimated that if these data are found in the wrong hands can have serious consequences for the US and come to a complete collapse of the pension fund. Because of the seriousness of the problem they created large expert team, which decided to publish this

information through the media in order to point to the thief on the possible consequences (in order to convince the thief to destroy laptop). On the other hand, representatives of the IT sector of insurance company had undertaken all necessary measures to protect the data from possible abuse[31]. The outcome was such that luckily there were no consequences for the pension fund and the state after all, but because of negligence and breach of security procedures by one person were spent contingency funds, time and extra work for data protection.

The report "The high-tech crime" 2011 of the company Norton, which is designed for software solutions, estimated that consumers lost about 114 billion US dollars. The newspapers made a comparison and found that profits from cybercrime are equivalent to profit from the global drug trade.

During the month of February 2014 the Dutch police have arrested four Dutch people and one German, and it closed the trading in the so-called "Dark web - Utopia". These people were suspected of being involved in illicit drugs, credit cards that have been stolen, weapons, etc. in the above market. Two of those arrested were suspected of having established another web site called "Dark web" known as the "Black Market Reloaded". In the operation were found and seized the following things: personal computers, hard drives, USB sticks and 900 so called "Beatcoin" that had a value between 400,000 and 600,000 euros[32].

In June 2012 the FBI performed operation "Card Shop", in which 24 people from thirteen countries on four continents were arrested, for stealing and selling of credit card data. FBI succeeded to capture them due to the fact that they secretly placed online carding forum called "Carder Profit", who worked on the principle invitation only and was constantly monitored by members of the FBI. The users can buy or sell the number of stolen credit card, and also to advise in connection with the theft and use of that information. The stolen data were returned to the banks, which protected more than 400,000 victims of cyber crime and avoid loss of 205 million US dollars[33]. Assistant Director of the FBI of the USA, Janice K. Fedarcyk, said that: "From New York to Norway and Japan to Australia, Operation "Card Shop" was directed against sophisticated, highly organized cyber criminals involved in buying and selling stolen identities, used credit cards, forged documents and sophisticated hacking tools. Two-year-old secret of FBI investigation conducted on 4 continents is proof of commitment to eradicate rampant criminal behavior of the Internet"[34].

Computer crime unit from the Ministry of Interior from Macedonia was involved in this action. According to the FBI in Macedonia only the orders for searching and interrogation of two persons for whom there were grounds for suspicion that they are involved in cybercrime were accommodated. However, in this action coordinated by the FBI, there weren't arrested entities from Macedonia[35].

---

31 USAID / Project eGovernment. Ministry of Information. Metamorphosis (2010). *Fundamentals and development of e - government*.Downloaded on 13th February 2014. http://www.mio.gov.mk/files/pdf/Osnovi%20i%20razvoj%20na%20e-Vlada%202010%20-%20mk.pdf.

32 Sokolovski,D (2014r., February 3). *Dutch authorities turned off the online black market Utopia*. Internet portal IT. http://it.com.mk/holandskite-vlasti-go-izgasija-tsrniot-onlajn-pazar-utopia/

33 Halpern, S. (2013). *Are hackers heroes?* Forum for security and democracy. Edition views and signposts, number 3 March 2013. Downloaded on 15th December 2013. http://www.fbd.org.rs/akcije/POJEDINACNE/VIP3.pdf

34 U.S. Attorney's Office. Southern District of New York. (2012г. Јуни 26). *Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce 24 Arrests in Eight Countries as Part of International Cyber Crime Takedown*. The Federal Bureau od Investigation (FBI). Downloaded on 17th February 2014. http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown

35 Sokolovski,D (2012 june 27). *MI and the FBI together against cyber crime, 24 persons from 13 countries were arrested*. Internet portal IT. Downloaded on 15th February 2014. http://it.com.mk/mvr-i-fbi-zaedno-protiv-kompjuterski-kriminal-24-uapseni-od-13-drzhavi/..

During October 2012 there was a large police operation conducted around the country in Macedonia in which there were arrested a dozen entities. There were more criminal groups that were well organized and performed activities related to cyber crime and stealing credit cards. The investigation lasted a long time since the beginning of 2012 when it gathered the necessary information for the final execution of the arrest. The arrested entities from Macedonia were assisted by others from foreign countries[36].

In 2012, the Computer Crime Unit of the Ministry of Interior (MI) in Macedonia detects cybercrime attack which made damage and unauthorized entry into a computer system in public procurement for a hundred and fifty police vehicles. Namely, on September 3, 2012 Bureau for Public Safety – BPS filed an application with respect to other issues of a technical nature in the operation of the electronic procurement system in Macedonia in implementing electronic auction of MI for purchase of motor vehicles. Furthermore, from the analysis of the log files (logs) for access to the site it was established that increased traffic coming from 119 different IP (Internet Protocol) addressed from various countries of the world. Obviously the goal was an attack for prohibited access to the electronic system of BPS which was bombed with simultaneous claims of 119 different IP addresses that blocked the electronic system[37].

The number of criminal activities in the area of cybercrime that occurre worldwide and on domestic level is significantly higher than the above mentioned. The aim is to show that no country is immune to this modern threat nowadays, which is constantly changed in shape and capacity. Cybercrime like any other crime knows no borders, nations or individuals, but its well known environment is cyberspace.

SECURITY MEASURMENTS FOR PROTECTION OF SECURITY RISKS AND THREATS ON THE INTERNET

Security measurments show that it is recommended using known and reputable antivirus program which includes tools against spyware malware. It is necessary to install software patches and security updates daily. Moreover, these updates will protect our computer against new threats.

Firewall allows us protection from external attackers, while protecting our computer or network from malicious or unnecessary Internet traffic. This type of protection is especially important for users who are constantly connected to the Internet via cable or digital connectivity with modems[38].

Computer Security Solutions:

- Set a password in accordance with the standards;
- Installation, maintenance and updating of anti-virus program;
- Activation of automatic updates for antivirus;
- Setting personal security settings on the web browser;
- Controlling Internet connection;

36 *Arrests in Macedonia – Ministry of Interior cybercrime action.* (2012 October 2). Internet portal: Makfaks and Kurir. Downloaded on 15th February 2014. http://mkd-news.com/se-apsi-niz-makedonija-aktsija-na-mvr-protiv-kompjuterski-kriminal/.

37 *There was computer crime in bidding for police vehicles.* (2012 September19). Internet portal МКД. Downloaded on 15th Feruary 2014. http://www.mkd.mk/59923/crna-hronika/sepak-imalo-kompjuterski-kriminal-pri-naddavanjeto-za-policiskite-vozila.

38 The Cyber security handbook. *A cyber security guide.*Downloaded on 06th August 2014. www.NJConsumerAffairs.gov.

- Protection of the wireless network;
- Connect the computer to the switch port, if connect another computer then there will be no service;
- IDS - Intrusion Detection System.

Survey of the basic steps how to be smart on the Internet

1. Protection against malware and reduce the spam:
- You should never open the links in the e-mail message from an unknown source;
- No need to open an attachment from the email if you do not expect or do not know the sender;
- Antivirus scanning of attachments from e-mail prior to opening;
- Always delete e-mail in the spam without an opening;
- No need to give the address of the e-mails of people who do not know you.

2. Personal protection from fraud while being active in the Internet space:
- Mandatory checks if we visit a secure page;
- Using a secure way for e – banking;
- Never send information for the financial status via e-mail;
- Never respond to e-mail offering easy earnings;
- There should not be a transfer of money or give credit card information or bank account to any unknown people on the Internet.

3. Protecting the identity and privacy:
- Never share personal information via e-mail, SMS or through the pages of social networking with unknown people;
- Avoid using public computers or Wi-Fi hotspots for entering personal data.

Security of the social networks[39]:
- Adjust the privacy profile;
- Protecting the username with strong password;
- Discretion in accepting friends;
- Never click on suspicious links - even when they come from friends;
- Do not post information that may be sensitive to the family, such as: birthdays, address and the like;
- Do not post inappropriate and personal pictures of family or friends, or those which our friends asked not to be publicly published.

What you need to know is that we cannot install too many types of security software. Too many of these programs can affect the performance of the computer and the effectiveness of the software. Finally, you need to protect against unwanted e-mail messages or pop-up ads that claim to contain anti-virus program. They may not be open, to click on the given link or attachment. These messages which usually are Trojan horses waiting to infect your computer.

It is necessary to check private and security settings of web browser to our computers or mobile smart phones, which oftenly are bought with installed web browsers (Safari, Firefox, and Chrome, Internet Explorer or other). Search engines often come with default settings that provide a balance between the computer's security and functionality of web pages. Settings

39 Protecting Yourself Online. *What Everyone Needs to Know.* Commonwealth of Australia 2010. Australian Government. Copyright Administration, Attorney General's Department, National Circuit, Barton ACT 2600.Downloaded on 21st May 2014. http://www.ag.gov.au/cca.

set limits on the extent to which computers will enable Internet applications - such as cookies, ActiveX and Java - that help websites to perform important functions. If our search engine allows unlimited interaction cookies or other applications that monitor Internet activity, can easily be targeted, by contrast, if completely block these applications then the website will not function effectively. It is therefore necessary to find a balance, so for more detailed information it is best to visit the producer of relevant search engine where you can inform yourself for the setting of personal and security information[40].

CONCLUSION

Methods and forms of cybercrime are in constant evolution because they require continuous monitoring and studying by the authorities, their ability to adapt to the new environment and taking timely preventive measures to protect cyberspace. The new millennium, the Internet revolution, new ways of warfare, new enemies in the 21st century, new tactics and techniques of warfare, new leaders, new world order and a new world security card only confirm the role of security and intelligence in the modern world. Never forget, Information is the power.

Anyone who is looking for any information on the Internet is constantly exposed to security risks and threats from malicious software. The malicious software is located in the Internet space which is created, updated, upgraded, modified and distributed to target groups by malicious hackers. Motives for creating malicious software are of different nature (to espionage, crime, entertainment, etc.). One of the biggest dangers is disgruntled insiders within each organization. Searching of the Internet space with an open IP address is an additional security risk. Also, security risk means open access to the web page, while all our activities are detected in the browser history, cookie store and so on.

Cybercrime is increasingly appearing in more complex forms difficult to detect and prevent. The malicious software as one of the methods of cybercrime is accessible in cyberspace. Nowadays, it is practically unnecessary to be a great connoisseur of computer equipment or a good programmer in order to create malicious software for criminal activities, because many of the malicious softwares already exist on the Internet. Code of much malicious software is built and placed on a web site or forum for malicious hackers who waited on its use by any person who wants to create a cyber attack. Social engineering has always been a good tool for criminals to access information of a personal nature of the potential target for implementation of activities in the area of cyber crime. Information gathered through social engineering in many cases resort to negligence and accident.

Cyber criminals usually used the method phishing because they know that there are people who have the resources (computers) but lack of knowledge, they are reckless and curious, and therefore they often become victims of this method of cyber crime.

Protection against malicious software on the Internet is by constantly updating antivirus, installing and enabling a firewall, check the private and security settings of the search engines, password protection, raising awareness of using external memory devices (USB, CD, floppy disk, etc.), working with a hidden IP address, using concealed search (incognito) has no record of our activities in the browser history or in the cookie store and other measures to computer protection.

The possibilities for action of cyber criminals are huge and using all his methods. However, the biggest threat to the operation of cyber criminals in cyberspace will occur due to: low

40 The Cyber security handbook. *A cyber security guide.*Downloaded on 06th August 2014. www. NJConsumerAffairs.gov.

awareness of employees about the threats and risks in this area, ignorance, negligence and violation of safety rules and procedures. This means however that most cybercrime would be performed because of the people as a security risk.

The expectation in the future is that the attacks in the area of cyber crime are going to grow and become more complex, more serious, covered and to cause major damage due to the development of information - technological society, the greater opportunity to use the tools of cyber crime that is available online and because of the social status of citizens in society.

REFERENCES

1. Beaver, K. (2010). *Hacking For Dummies, 3rd Edition*. Wiley Publishing, Inc. 111 River Street Hoboken, NJ, 386. Downloaded on 15th December 2011. http://www.dummies.com/cheatsheet/hacking
2. Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler. *Democratic governance challenges of cyber security.* Downloaded on 15th December 2013. http://www.fbd.org.rs/akcije/POJEDINACNE/CYBER%20ZA%20WEBSITE.pdf.
3. Barry G.Buzzan (1983). *People, states and fear.* Skopje, 2010: Academic press,112.
4. Vuletic, D. *Cyber warfare as a form of information warfare*. Downloaded on 15th December 2013. http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-32.pdf.
5. CARNet Croatian Academic and Research Network. *Phishing attacks*. CCERT-PUBDOC-2005-01-106. CARNetCERT in association with LS&S. Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-01-106.pdf
6. CARNet Croatian Academic and Research Network. *Online extortion*. CCERT-PUBDOC-2009-06-268. *CARNetCERT in association with LS&S.* Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-268.pdf
7. CARNet Croatian Academic and Research Network. *Steganography.* CCERT-PUBDOC-2006-04-154. *CARNetCERT in association with LS&S.* Downloaded on 16th December 2013. http://www.cert.hr.
8. CARNet Croatian Academic and Research Network. *Spyware progras.* CCERT-PUBDOC-2009-10-280. *CARNetCERT in association with LS&S.* Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-10-280.pdf.
9. ETS 185 – Convention on *Cybercrime*, 23.XI.2001. Council of Europe. Downloaded on 15th December 2013. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
10. Graves, K. (2010). *Certified Ethical Hacker Study Guide*. Wiley Publishing, Inc., Indianapolis, Indiana, 392. Downloaded on 08th January 2014. http://files.laitec.ir/wp-content/uploads/2013/06/CEH-Study-Guide.pdf
11. Gjorgjijevic, N.(2011) Defending Cyberspace: International Law must address Internet – based security threats. *Per Concordiam. Journal of European Security and Defence Issues*, 2 (2), 21 – 27.
12. Halpern, S. (2013). *Are hackers heroes?* Forum for security and democracy. Edition views and signposts, number 3 March 2013. Downloaded on 15th December 2013. http://www.fbd.org.rs/akcije/POJEDINACNE/VIP3.pdf
13. Internet Threats Trend Report – October 2013. *Commtouch.* Downloaded on 17th August 2014. https://www.pallas.com/fileadmin/img/content/publikationen/2013-Q3_Commtouch-Internet-Threats-Trend-Report.pdf.
14. Industrial Control Systems Cyber Emergency Response Team (ICS – CERT). *Cyber Threat Source Descriptions.* Downloaded on 07th February 2014. http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions.

15. Milosavljevic, M. and Grubor,G. (2009). *Computer crime investigation- Methodological technological base*. Singidunum University – Serbia, 291. Downloaded on 15th December 2013. http://www.seminarski-diplomski.rs/biblioteka/Istraga%20kompjuterskog%20kriminala.pdf
16. Nikola, B. (2013). *Security risks and solutions for data protection*. Singidunum University – Serbia, 2013.Downloaded on 15th December 2013.
17. New virus locks the data and required to pay $ 300. BusinessInsider. Downloaded on 04th January 2014. http://brkajrabota.mk/tehnologija/internet/30378-nov-virus-gi-zakluccua-komjuterite-i-bara-da-platite-300-dolari.
18. Organized crime. Seminar work. Downloaded on 13th February 2014. http://www.maturskiradovi.net/forum/attachment.php?aid=2015
19. *Arrests in Macedonia – Ministry of Interior cybercrime action.* (2012 October 2). Internet portal: Makfaks and Kurir. Downloaded on 15th February 2014. http://mkd-news.com/se-apsi-niz-makedonija-aktsija-na-mvr-protiv-kompjuterski-kriminal/.
20. Sokolovski,D (2014г., February 3). *Dutch authorities turned off the online black market Utopia*. Internet portal IT. http://it.com.mk/holandskite-vlasti-go-izgasija-tsrniot-onlajn-pazar-utopia/
21. Sokolovski,D (2012 june 27). *MI and the FBI together against cyber crime, 24 persons from 13 countries were arrested.* Internet portal IT. Downloaded on 15th February 2014. http://it.com.mk/mvr-i-fbi-zaedno-protiv-kompjuterski-kriminal-24-uapseni-od-13-drzhavi/.
22. Protecting Yourself Online. *What Everyone Needs to Know.* Commonwealth of Australia 2010. Australian Government. Copyright Administration, Attorney General's Department, National Circuit, Barton ACT 2600. Downloaded on 21st May 2014. http://www.ag.gov.au/cca.
23. *There was computer crime in bidding for police vehicles.* (2012 September19). Internet portal МКД. Downloaded on 15th Feruary 2014. http://www.mkd.mk/59923/crna-hronika/sepak-imalo-kompjuterski-kriminal-pri-naddavanjeto-za-policiskite-vozila.
24. The Cyber security handbook. *A cyber security guide.* Downloaded on 06th August 2014. www.NJConsumerAffairs.gov.
25. USAID / Project eGovernment. Ministry of Information. Metamorphosis (2010). *Fundamentals and development of e - government*.Downloaded on 13th February 2014. http://www.mio.gov.mk/files/pdf/Osnovi%20i%20razvoj%20na%20e-Vlada%202010%20-%20mk.pdf
26. U.S. Attorney's Office. Southern District of New York. (2012г. Јуни 26). *Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce 24 Arrests in Eight Countries as Part of International Cyber Crime Takedown.* The Federal Bureau od Investigation (FBI). Downloaded on 17th February 2014. http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown
27. Understanding Internet Security. *What you need to protect yourself online.* 2004 Big Planet, Inc. All Rights Reserved. Big Planet is a registered trademark.Downloaded on 16th August 2014. http://www.bigplanetusa.com/library/bp/pdf/bpis_understanding_security.pdf.
28. United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity," *Science* 326 (13 November 2009): 943-4; See Martin Charles Golumbic, Fighting Terror Online: The Convergence of Security, Technology, and the Law (New York: Springer, 2007).

UDC: 004.65.056:616-089.84

ORGAN TRANSPLANT INFORMATION SYSTEM – IS THE DANGER FROM THE OUTSIDE OR INSIDE?

Saša Borović, MSc[1]
Dedinje Cardiovascular Institute, Belgrade,
University of Belgrade, School of Medicine

Abstract: In the well organized transplant programs, all transplantation centers have access to the central computer database. In this database, the transplantation centers enter information of their recipients along with the recipient profile and the donor profile. This is the basic principle of making the best match between donated organ and recipient. This paper elaborates potential criminal activities and malpractice regarding central computer database.

Keywords: central computer database, web application, malpractice.

INTRODUCTION

We live in times where modern information systems are involved in every aspect of human life. There is a need for computers in the role of deciding and choosing especially if we want an objective approach. Also, there is a large need for well organized databases that are easily accessed from all over the world. One of the most important aspects is security of data and personal information, identity and objective "jury decisions".

When transplant hospitals accept patients onto the waiting list, the patients are registered in a centralized, national computer database, and introduced into the network that links all donors and transplant candidates. After removal, a donor organ has to be transplanted within a few hours. A smooth running organization is of life-saving importance. Therefore the central office is manned by specially trained staff, 24 hours a day, and 7 days a week, supported by the computer information system.

In the area of health and medicine, a number of modern applications and databases can be found. In the need of new, modern technologies introduction in Serbia, professional team made a project and a final product.

Modern computer information system, as a final product, consists of a well organized database, web application, and a special protection and security. Main task was that process of registering and deciding, must be transparent and on a public world network, like internet is. Authentication of authorized personnel has to be very strong together with the encryption of communication and data transmitted. The exchanged data have to be protected because of the large number of persons involved in Cybercrime on illegal organ market, and data altering and counterfeiting.

The whole system is server oriented, the application is hosted and run on a server. Also, the computer database is hosted on a database server which can be hosted on a same computer like web application is, but it is advised that the separate servers manage database and web application, which communicates with a database.

1 E-mail: sborovic2001@yahoo.com.

A centralized, national computer database maintained on a hourly and daily basis, together with a modern, well organized web application is what was missing in Serbia, in our society.

This is a professional medical-engineering information system which is a basis of a modern healthcare and life saving of citizens of one country. Therefore, there are large number of examples of misusing and malpractice around this multi billion dollars area, which consists of transplant hospitals, medical personnel, governments and administrative personnel, computer databases and applications, donors and transplant candidates.

THE SITUATION IN THE WORLD

The whole system of donors and transplant candidates, together with transplant hospitals **cannot exist** without a modern computer information system. This is the practice and real situation in the world.

Two main systems, which were "compasses" of this system's development and building, are:

1) UNOS[2] (USA)

2) EUROTRANSPLANT[3] (Europe)

UNOS is United Network for Organ Sharing based in the United States of America. Their motto is: "Working together, Saving lives".

Their mission is to advance organ availability and transplantation to support patients through education, technology and policy development.

United Network for Organ Sharing (UNOS) is the private, non-profit organization that manages the nation's organ transplant system under contract with the federal government. In doing so, they bring together hundreds of transplant and organ procurement professionals and thousands of volunteers. This unique collaboration helps make life-saving organ transplants possible each day. Our system serves as the model for transplant systems around the world.

HOW ORGAN MATCHING WORKS

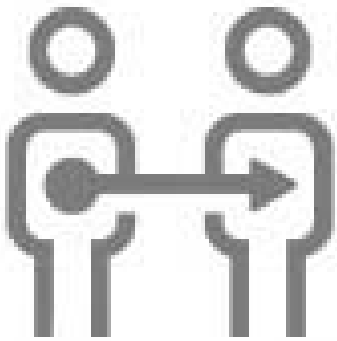


Figure 1: *Donor and a transplant candidate*

2 https://www.unos.org/
3 https://www.eurotransplant.org/cms/

When a patient is "added to the list," a transplant hospital adds a patient's medical information into UNOS' computer system. When a deceased organ donor is identified, UNOS' computer system generates a ranked list of transplant candidates, or "matches", based on blood type, tissue type, medical urgency, waiting time, expected benefit, geography and other medical criteria (UNOS 2016).

FACTS ABOUT DONORS AND TRANSPLANT CANDIDATES

- You can be a donor at any age.
- Celebrity or financial status are not factors in getting a transplant.
- Donation is possible with many medical conditions.
- All major religions approve of organ and tissue donation.
- **A national computer system and strict standards are in place to ensure ethical and fair distribution of organs.**
- A healthy person can become a living donor by donating a kidney, or a part of the liver, lung, intestine, blood or bone marrow.[1]

A national computer system and strict standards are in place to ensure ethical and fair distribution of organs, so the organs are matched by blood and tissue typing, organ size, medical urgency, waiting time and geographic location.

UNOS provides a vital link in the organ transplant process. Its policies and computerized network match donated organs with transplant candidates in ways that save as many lives as possible and provide transplant recipients with the best possible chance of long-term survival. The matching criteria developed by the transplant community, and approved by UNOS' Board of Directors, are programmed into UNOS' **computer matching system**. Only medical and logistical factors are used in organ matching. Personal or social characteristics such as celebrity status, income or insurance coverage play no role in transplant priority.

EUROTRANSPLANT's motto is: "Cooperating saves lives".

EUROTRANSPLANT is a non-profit organization based in Europe, that facilitates patient-oriented allocation and cross-border exchange of deceased donor organs. Active for transplant centers and their associated tissue typing laboratories and donor hospitals in eight countries, EUROTRANSPLANT ensures an optimal use of donor organs. EUROTRANSPLANT is responsible for the allocation of donor organs in Austria, Belgium, Croatia, Germany, Hungary, Luxembourg, the Netherlands and Slovenia, 8 countries in the Europe. This international collaborative framework includes all transplant hospitals, tissue-typing laboratories and hospitals where organ donations take place.

EUROTRANSPLANT AIMS

The aims of EUROTRANSPLANT are: As mediator between donor and recipient, EUROTRANSPLANT plays a key role in the allocation and distribution of donor organs for transplantation. The mission statement and goals of EUROTRANSPLANT express the foundation's main target: to ensure an optimal use of available donor organs. The allocation system is based upon medical en ethical criteria. Through conducting and facilitating scientific research, EUROTRANSPLANT aims at a constant improvement of transplant outcomes (EUROTRANSPLANT Manual 2016)

Statistical data[4]:

- 14,560 patients on the active organ waiting list on January 1, 2016.
- 10,808 registrations on the waiting list in 2015.
- 7,145 organ transplants from deceased donors in 2015.
- 134,6 million inhabitants in the EUROTRANSPLANT region

CENTRAL WAITING LIST IN OUR SYSTEM - SETNET

SETNET is the name of our system, **Se**rbian **T**ransplant **Net**work (Transplantaciona Mreža Srbije).

All transplantation centers within the national transplant system have access to the central computer database. In this database, the transplantation centers enter the general and medical information of their recipients along with the recipient profile and the donor profile. These profiles contain the characteristics of patients and donors (Figure 2).

Computer information system in SETNET network consists of:

- Hardware components (Servers on the Internet)
- Software components (Web application, RDBMS Database, TLS Protection and Secure Encryption)

Hardware components are Database server (Relational Database Management Server) and a Web server. Both servers can be only one computer.

Software components are copyrighted[5] Web application, Relational Database (MS SQL Server), https TLS (Transport Layer Security protocol) with custom made mathematical algorithms for encryption.

Web application is made in Visual Studio program environment, with program code written in C# and C++ programming languages. Web pages are dynamic web pages, in ASPX technology ASP.NET (Active Server Pages) with .NET 4.0, run at server.

Figure 2: *National computer database (proposed)*

Electronic network allows transplant professionals to register transplant candidates on the national waiting list, match them with donated organs, and enter vital medical data on candidates, donors and transplant recipients (Figure 3 on the next page).

4 https://www.eurotransplant.org/cms/index.php?page=home
5 Copyright, Saša Borović MD, Vladan Borović M.Sc.E.Eng., Authors

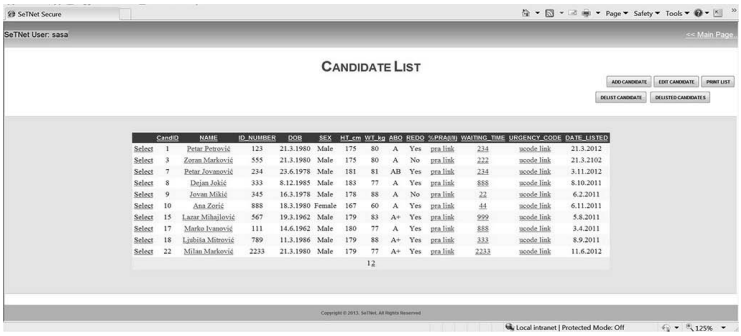


Figure 3: *Candidate list (main page)*

When the information is entered into the central database, the patient is put on the waiting list. At that point, the waiting time starts.

ALLOCATION

Following donor organs identification, the procuring organization accesses the computerized organ matching system, enters information about the donor organs, and runs the match program.

For each donated organ, the computer program generates a list of potential recipients ranked according to objective criteria (i.e. blood type, size of the organ, medical urgency of the patient clinical status, time spent on the waiting list). Each organ has its own specific criteria. The match list is generated by a complicated computer algorithm that takes into account all medical and ethical criteria.

After printing the list of potential recipients, the transplant coordinator contacts the transplant surgeon caring for the top-ranked patient (i.e. patient whose organ characteristics best match the donor organ and whose time on the waiting list and urgency status adhere to allocation policy) to offer the organ. Depending on various factors, such as the donor's medical history and the current health of the potential recipient, the transplant surgeon determines if the organ is suitable for the patient. If the organ is turned down, the next listed individual's transplant center is contacted, and so on, until the organ is allocated.

Once the organ is accepted for a potential recipient, transportation arrangements are made for the surgical teams to come to the donor hospital and surgery is scheduled. For heart, lung, or liver transplantation, the recipient of the organ is identified prior to the organ recovery and called into the hospital where the transplant will occur to prepare for the surgery.

The recovered organs are stored in a cold organ preservation solution and transported from the donor to the recipient hospital.

The allocation system is:

1. Objective: the match list is the same no matter which duty desk officer arranges the allocation

2. Reproducible: the same question will lead to the same answer

3. Transparent: every step in the process can be accounted for

4. Valid: the system is based upon valid medical and ethical criteria that are supported by consensus within the transplant community.

The match is based upon general principles of expected outcome, urgency and waiting time. Ethnicity, gender, religion, and financial status are not part of the computer matching system.

MALPRACTICE HAZARDS

Real-time, detailed communication is essential to coordinate the process of organ donation and transplantation. For many years, most information was shared by phone and fax. As information technology has rapidly evolved, transplant networks developed secure, online-based systems to place organs efficiently and collect essential data to improve the transplant field.

The system is designed for continual operation because any lapse in system availability could mean that transplant candidates lose an opportunity for a life-saving transplant. The system continues to adapt to emerging use of and need for newer technology such as mobile devices and tablets, and to integrate effectively with the increasing use of electronic medical records.

Entry to the computer data system is protected by personal passwords. To ensure as much privacy to donors and recipients, access to data in the system is limited by user rights. The computer based database is accessible over the Internet. This means that it is accessible everywhere there is an internet connection.

There are numerous Cybercrime possibilities. The most common and the most dangerous are:

- Revealing database usernames and passwords
- Changing passwords and important data in a database including patient data and records
- Tracking and sniffing connections on a database
- Sniffing Internet traffic and discovering secret database commands
- Discovering patient identity and medical data
- Deleting a database
- Altering patient urgency and priority
- Misusing private patient data in the area of organ black market in the world (Organ trade 2016), (Organ Trafficking 2016)
- Demanding a money compensation to illegally change urgency and priority of a patient

Each transplant center collaborating within national transplant network can enter, update and retrieve their own information of center, recipients, living donors and transplants.

Urgency statuses are used to classify transplant candidates on the waiting list and to prioritize patients in the thoracic organ match and allocation procedure. The urgency statuses reflect transplantability and medical urgency (Figure 4). The High Urgency (HU) status places the patient in the top priority of receiving the donated organ. The HU status is usually assigned by an independent team of auditors, where their decision is guided by well defined medical criteria (EUROTRANSPLANT Manual 206).

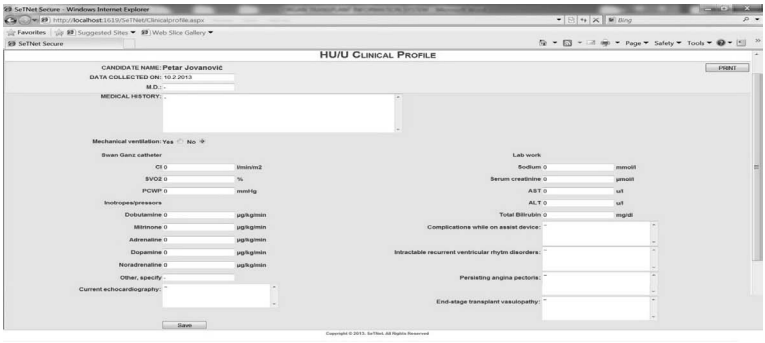


Figure 4: *HU/U clinical profile*

Proposing the patient for the HU status opens the possibility for manipulating the organ transplant allocation system in order to help the patients get donor organ more quickly. Doctors could exaggerate the severity of their patients' conditions so that they would be accorded higher priority for receiving organs, by manipulation of medical records. In this scenario, the effective manipulation of organ transplantation would necessitate falsifying medical records and manipulating medical tests. For example, flagging patients as requiring dialysis is likely to move them up the waiting list. Deliberately recording information known to be false constitutes serious misconduct. Tampering with actual medical samples to "make their conditions appear worse" is an extrapolation of the same falsification. Even the TV movies are dealing with that subject now (Why is Kollywood so taken up with organ transplant crimes? 2016). While this is in itself misconduct, the consequences of these actions may also be detrimental to a severely sick patient, by denying them organs, while benefiting another (Shaw 2013).

If we speak about Demanding a money compensation to illegally change urgency and priority of a patient, a real example happened in Germany during the period from 2010. till now, according to the numerous internet news (Connolly 2013), (Turner 2008), (Turner 2009), (Berglund, Lundin 2012).

MALPRACTICE PREVENTION

Obviously there are "inner" and "outer" possibilities for the crime, and the prevention should focus on both aspects.

Prevention of "outer" pathway means prevention of the Cybercrime. There are very important steps that must be implemented in a technical organization regarding computer information system, as follows:

- Implementing SSL *(Secure Sockets Layer)* v3.0 and TLS *(Transport Layer Security)* protocols for the security, authentication and cryptography, including custom made mathematical algorithms
- Nonstop, 24/7/365 technical surveillance on a database and web application users
- Using complex usernames and passwords
- Frequent use of a database backup and patient data check outs
- Monitoring the validity of patient identity

The "inner" pathway is completely depended on the medical profession. Tightly coordinated and monitored national transplantation system should incorporate regulative measures

to prevent this kind of crime. Professional (national and international) audits and controls, educated national coordinators and program CEOs are of crucial importance. Evaluation of each transplant program should be routine and transparent. Learning from the experience, national transplant regulatory bodies should be nongovernmental and non profitable.

CONCLUSION

Organ transplantation is the only medical therapy where benefit of the patient depends on the tragedy of another human. In the era of donor organ shortage, fare and efficient allocation is an imperative.

Public confidence and trust in medicine is essential and organ donation and transplantation are no exception. Willingness of members of the public to donate could be undermined by organ transplant scandals.[7]

Use of the modern technologies is the imperative of civilization. Therefore, multidisciplinary taskforce should be responsible to prevent any kind of misuse and crime.

There is a urgent need for a national computer database where the patients are registered, and introduced into the network that links all donors and transplant candidates.

This is a very important project in Serbia done by Serbian scientists, experts, based on domestic knowledge and "brains", in the area of Medicine, Electro-technical and Information and Communications Technology. Through the years of research and development, including experiences from Houston, Texas, USA, Brussels, Belgium, EU, Germany, Austria, this modern system came to life.

Prevention of Cybercrime can be done by strictly using a protected national computer system with strong encryption and strict standards in organizing the whole system. Security procedures must be obeyed and they have to be written and publicly transparent (**Organ trafficking: a protected crime**).

One big "Mass donor organ fraud" happened in Germany, European Union, in 2013., which can be a base how to prevent those malpractices and Cybercrime, together with how to fight them. There are even articles and information on prisoner killings for their organs (Killed for their organs 2016). Atrocities and crimes are made in our country, too (Organ Theft in Kosovo).

Several appearances of this SETNET network and system occurred on a national TV in Serbia, promoting the importance and necessity of the existence of such a system.

As mentioned in this paper, use of computer information system for managing donors, transplant candidates and transplant hospitals network, together as a whole functional system, is a must, and ethical and fair distribution of organs cannot be managed and successfully be done without a protected computer information system with encrypted, secure communication, data exchange and strong user authentication, proposed in this, SETNET network system.

REFERENCES

1. Connolly K. Mass donor organ fraud shakes Germany. The Guardian, 9th January 2013. http://www.guardian.co.uk/world/2013/jan/09/mass-donororgan-fraud-germany
2. Berglund S, Lundin S. . "'I Had to Leave': Making Sense of Buying a Kidney Abroad." In The Body as a Gift, Resource, and Commodity: Exchanges Organs, Tissues and Cells in the 21st Century, edited by Gunnarson M. and F. Svenaeus, 321–42. Huddinge: Södertörn Studies in Practical Knowledge, 2012.

3. EUROTRANSPLANT Manual. Chapter 6. https://www.eurotransplant.org (Available March 2016)
4. Killed for their organs, http://www.stoporganharvesting.org/ (Available March 2016)
5. Organ trade https://en.wikipedia.org/wiki/Organ_trade (Available March 2016)
6. Organ Trafficking: An International Crime Infrequently Punished
7. http://www.medicaldaily.com/organ-trafficking-international-crime-infrequently-punished-247493
8. (Available March 2016)
9. Organ trafficking: a protected crime
10. http://theconversation.com/organ-trafficking-a-protected-crime-16178 (Available March 2016)
11. Organ Theft in Kosovo, https://en.wikipedia.org/wiki/Organ_theft_in_Kosovo
12. (Available March 2016)
13. Shaw D. Lessons from the German Organ Donation Scandal. JICS 2013; 14:200-201.
14. Turner, L. "Commercial Organ Transplantation in the Philippines." Camb Q Healthc Ethics 18, no. 2 (2009): 192-96.
15. Turner, L. "'Medical Tourism' Initiatives Should Exclude Commercial Organ Transplantation." J R Soc Med 101, no. 8 (2008): 391-94.
16. UNOS, United Network for Organ Sharing, https://www.unos.org/ (Available March 2016)
17. Why is Kollywood so taken up with organ transplant crimes?
18. http://www.thehindu.com/news/cities/chennai/why-is-kollywood-so-taken-up-with-organ
19. transplantcrimes/article7532517.ece (Available March 2016)

UDC: 004.056.55
343.533::004

HIDING CYBERCRIME USING CRYPTOLOGY

Vladan Borović, MSc[1]
Ministry of the Interior of the Republic of Serbia
Nebojša Jokić, MSc
Ministry of the Interior of the Republic of Serbia

Abstract: This paper contains the description of secure systems, software applications and cryptology encryption/decryption methods that are used to hide cybercrime. Identity and actions done by the persons involved in crime on the Internet are being hidden from the public and police. Three main methods and computer applications are discussed together with real examples.

Keywords: cryptology, cybercrime, deep web, Tor

INTRODUCTION

In these modern times, with a numerous high quality technology products and a rapid technology development in the area of ICT, mostly fast software applications, criminals are using those modern applications and systems for their anonymous communication, file sharing, gathering of information, mostly on the Internet and large corporation networks, in one word, cybercrime. During those criminal actions, they remain hidden from the eye of the public and police. The most commonly used systems, software applications and techniques are deep web, Tor and SSL Tunnelling with custom made mathematical encryption algorithms.

METHODS OF HIDING

There are three main methods for hiding identity and actions on the Internet that are most commonly used by the persons involved in criminal acts. They are as follows:

- Deep (Dark) Web
- TOR (Anonymity network)
- SSL Tunnelling (TLS)

DEEP WEB AND DARK WEB

To enable devices on the Internet to communicate one with another, each one must have an IP address that represents its current unique identification. These addresses are assigned by ISP to which they are mapped, which temporarily sTores information which IP address is assigned to a certain point where the user is. In addition, the IP address does not necessarily indicate exactly a particular individual, but may indicate, exact or approximate, the physical location of the device.

1 E-mail: vladan.borovic@mup.gov.rs.

To establish communication between your device and another device on the Internet, and to be able to send information to another device or to seek and receive content from another device, it is not necessary to know its IP address. It is enough to know the global address (URL) of resource you want to access, and the network will get information about IP address from DNS servers.

The most common way to access any content on the Internet is to open a browser and type the name of the website you are accessing in the appropriate field, or click on a link to that page, and then the desired content appears on your screen. Your request is split into packets containing your IP address, which will serve the other side in communication to return the response to the right address. Your packages, of course, must include the IP address of the destination site in order for the request to be forwarded to the right place. Between you and the site with which you want to exchange packets there is communication network that ensures that packets are delivered to the desired address. The network directs the packets from node to node, until they reach their destination. The protocols used for packet routing perceive the entire path from the beginning to the end and calculate the best route. Sometimes it happens that protocol determines different paths for the packets from the same group, which does not affect the final outcome of communication and is invisible to the user.

In order to enable users to find the desired content, search engines use index sites content, including collecting, parsing and storing the information of a site. Indexing requires additional memory space and frequent updating, but the search for information is then many times faster.

[1]However, there are parts of the Internet that are not indexed because search engines cannot automatically access it. This includes subnets that require passwords or other credentials to gain access, databases that requires fees for access, and sites that require user interaction before accessing, parts of a very large database, the data that are generated in real time, and other parts of the Internet that are inaccessible from normal browsing. It is estimated that the Internet is indexed in the range from 3 to 15%, and it is considered that the size of the "invisible" network is 500 times larger than the visible. This part of the Internet in the jargon is called deep web, and also undernet, hidden web or invisible web.

There is also an invisible part of the Internet that cannot be accessed in the normal way, but only by using specialized applications that include anonymity, such as TOR (The Onion Router) or I2P services. The principle of operation of these services is that the packets travel through a predetermined path, not using standard protocols for packet routing. Each router on the path recognizes only the immediately preceding and immediately following router, so complete path of communication cannot be reconstructed at any point. Because of this method of communication, the user who wants to access certain content must accurately know its location.

However, there are activities on arranging this part of network in order to facilitate search and access. One of the search engines is Onion.city, which currently has about 6.7 million sites indexed.

This part of the Internet is very suitable for a variety of criminal activities, but it is also used by the users who do not want their communications to be monitored, such as political activists, journalists or whistle-blowers.

The part within the deep web that is used for a variety of criminal activity is called the dark web.

Many of criminal activities are recorded on the dark web, such as trade of soft drugs, cracked video games and other software, pirated music and movies, stolen credit card information. Also, there you can receive offer for illicit drugs, as well as for weapons, forged identity documents, child pornography and even professional killers.

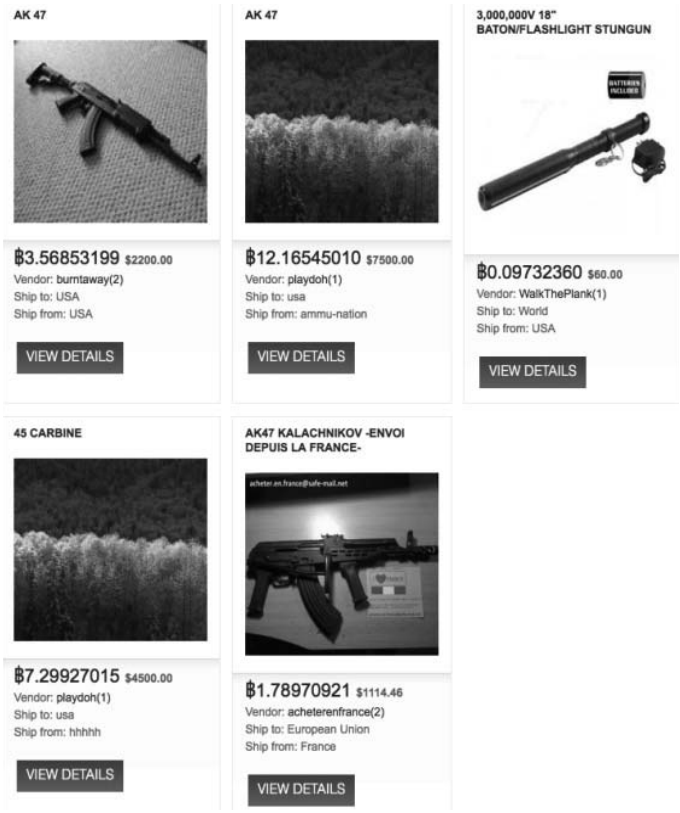


Figure 1: *Offer of weapons on the dark web*

For example, a US passport can be obtained for 700 Euros. Payment of goods and services is often in Bitcoins, in order to additionally hide the trace of transactions. [2]One of the most popular sites for selling drugs was the famous Silk Road, which is estimated to have a turnover of about 1.2 billion dollars and over one million users.

These networks are suitable for the placement of servers that control the malware. An example of this is the GameOver Zeus, a sophisticated malware designed for stealing bank accounts data and credentials. Computers infected by this malware are also becoming a part of a global botnet network, which had decentralized management, which means that command to the infected computer can be given from any other infected computers in the network. GameOver Zeus malware was used to distribute other malwares as Cryptolocker, which encrypts the contents of the victim's computer. This network was operational by mid-2014, when the FBI in cooperation with other agencies from 10 countries interrupt its work and seized servers for command and control of Cryptolocker scheme. A group of cyber criminals from Russia and Ukraine led by Evgeniy Bogachev was identified to be responsible for GameOver Zeus and Cryptolocker [3] malwares. It is estimated that GameOver Zeus malware infected over a million computers and that the damage from the removal of money from bank accounts worth hundreds of millions of dollars, while only Cryptolocker malware infected more than 230,000 computers, and recorded payments for ransom to unlock files are amounted to about $ 30 million in the period from September to December 2013.

Figure 2: *Cryptolocker screen*

It is obvious that this part of the Internet is very convenient for communication of criminals. For law enforcement agencies, Tor network and similar structures became a problem because it is quite difficult to determine the beginning and end of communication, which means that the final participants in the communication have a good ability to protect from disclosure of its current location. And if they have the option to hide even the content of communications, law enforcement agencies have rather a difficult task to come up with the necessary data.

The military and police are using encryption to protect their communication since ancient times. To protect their intellectual property, data encryption is used by business users. Why cannot the criminals do the same thing?

The FBI in its [4]bulletin from 1970 reported several cases in which they had to break a coded communication of criminals to reach the necessary information, but at that time the communication was not electronic, and criminals were using simple coding methods. Even in the late 20th century, the devices for encryption of voice traffic over telephone lines appeared on the market but they were expensive, as well as calling on the larger geographic distances. Global connectivity over the Internet has brought a drastic reduction in the prices of communication over long distances, and with it emerged new, free or relatively cheap options to hide communications. With that, the law enforcement agencies issued a series of difficulties in the course of their work. An additional problem was made by Edward Snowden, who revealed the ways in which the security authorities are coming to the content of communication of criminals and details about the program for the surveillance of communications named PRISM[5]. After Snowden published these documents, many criminal groups have changed the way of communication.

TOR (ANONYMITY NETWORK)

Tor is online software for accomplishing anonymous communication. It is free of charge and is constantly developed by the developer's community around the world. Enthusiastic and professional experts, engineers, programmers and mathematical experts are working on new versions developing new possibilities. Considering that, the persons involved in cybercrime are very protected and up-to-date just by using this software application.

The name Tor is an acronym derived from the name of the software project *The Onion Router. Onion routing*[2] is a technique for anonymous communication over a computer network. In an onion network, messages are encapsulated in layers of encryption, analogous to layers of an onion. The encrypted data is transmitted through a series of network nodes called onion routers, each of which "peels" away a single layer, uncovering the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.

Internet traffic from a person's computer is directed by the Tor through a free worldwide volunteer network that consists of more than seven thousand relays to completely hide a user's location and usage from anyone. If the police are trying to use network surveillance or traffic analysis, it cannot be effective on a user using Tor. Tor makes it difficult for Internet actions to be traced and connected to the user of Tor. This includes visits to web sites, online posts, file sharing, instant messages, and any other communication forms. Identity and Internet activities are kept from being monitored.

Technical aspect of the Onion routing is the encryption in the application layer of a communication protocol stack which appear they are nested like an onion, hence the name *onion*. The data are encrypted by the Tor, including the destination IP address several times, then sending it through a virtual circuit comprising successive randomly selected Tor relays. Each relay decrypts a layer of encryption to reveal only the next relay in the circuit, nothing else, in order to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address. If somebody is using a network surveillance that relies upon knowing its source and destination IP address, Tor eliminates the point at which the communicating peers can be determined.

Vulnerability and weaknesses of the Tor together with attacks against Tor are constant area of academic research which is also welcomed by the Tor Project and developers.

Statistics of web based Hidden Services in January 2015 is:[3]

- Drugs 15.4%
- Fraud 9%
- Hacking 4.25%
- Porn 2.75%
- Guns 1.4%
- Counterfeit 4.2%
- Gambling 0.4%

Tor software is used both for licit and illicit purposes. Hackers groups, criminal groups and law enforcement agencies sometimes use Tor simultaneously. Even governments of countries, such as the U.S.A., fund the research and development of Tor.

Tor is almost every day used in cybercrime and can be used for anonymous defamation, unauthorized news leaks of sensitive information and copyright infringement, distribution of illegal sexual content, child pornography sharing, sharing pirate software, selling controlled substances, selling drugs, weapons, and stolen credit card numbers, money laundering, bank fraud, credit card fraud, identity theft and the exchange of counterfeit currency, the black market.

2 https://en.wikipedia.org/wiki/Onion_routing
3 https://en.wikipedia.org/wiki/Tor_(anonymity_network)

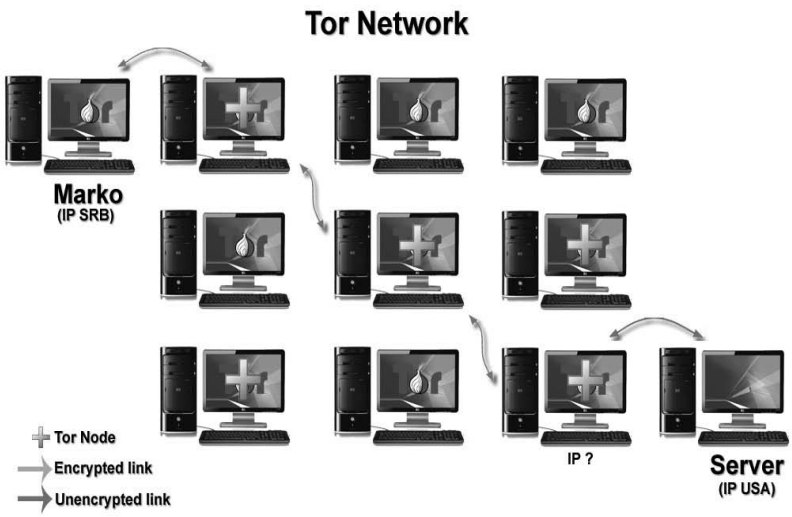


Figure 3: *Tor network*

In Figure 3 we can see the real example of Tor network configuration. As seen, all the computers, worldwide, use Tor software application for anonymity and actions hiding. Only the last computer, in the end on the right, does not have Tor software and it is an example of a common http server. The last computer in a Tor network communicates with http server over an unencrypted link with pages that are open to public. If it is the http server then even that communication is protected with at least ssl. Tor network with computers using Tor software can be in thousands in one hour.

From the Figure 3 Marko's Tor client with a computer in Serbia, with Serbian IP address given by the local ISP, picks a random path to destination server on the Internet. As guessed, green lines are encrypted links and communication, while red lines represent unencrypted links. That means if a link is encrypted then all the communication is encrypted and monitored by the Tor software regarding the level of security. If a link is unencrypted then the communication is open, in the clear or so called Clearnet.

So, as seen above, the IP address of a Marko's start computer with a Tor client in Serbia, is almost impossible to discover and positively found even if it frequently connects to a server in the U.S.A. because of the large "forest", a network of computers with Tor clients hiding their real IP addresses all over the world, and encrypting the traffic and communication. They usually change their IP address several times in a minute, while the communication remains undisrupted.

In real example even the famous Google cannot locate the real IP address of a start computer with Tor client searching the Internet, so the search engine displays the IP address of an end note in a Tor network, which may be, and usually is, thousands of kilometres away from a computer that initiated the search in Google or similar search engine. In that way the modern tracking and location discovering engines cannot discover and record the real IP address of a starting computer.

In Figures 4, 5 and 6 below, we can see the real examples of a modern Tor client.

Figure 4: *Tor client application*

In Figure 4 above, we can see the start window of a Tor client application, and also a warning that the application is out of date, it should be updated so the security risks are brought to a very low level. Tor software consists of a custom made browser, specially designed for Tor client and Tor network communication.

Figure 5: *Test of a Tor network settings*

In Figure 5 above, we can see the IP address which comes as a result of testing the network settings and proper functionality of a Tor application client and Tor network. **This is not the real IP address** of a start user i.e. Marko in Serbia. It is the IP address of a computer far away, which is the end node of a Tor network, as seen in Figure 6 on the next page, with all the nodes with IP addresses and hosting countries listed.

Also, there is an important warning that "Maximizing Tor Browser can allow websites to determine your monitor size, which can be used to track you. We recommend that you leave Tor Browser windows in their original default size." One of the very few weaknesses and leaks of the Tor client software application is that using other software leaks, weaknesses and faults the police can track down your IP or communication, while other faulty software is running together with a Tor client application.

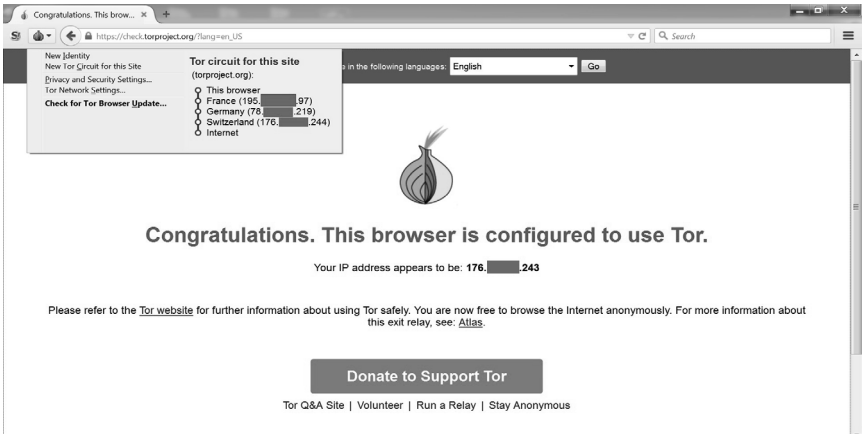


Figure 6: *Tor network nodes in a list*

As shown in Figure 6, there are 3 nodes listed with their IP addresses and the countries of origin, France, Germany and Switzerland, which is also the end node in Tor network, and is only visible by the requested http server for instance, or by the police tracking down the original, start user. The communication between nodes and start computer in Serbia are encrypted and concealed. The list above represents random path from the start user in Serbia and destination server in the USA which is contacted from Switzerland, and the communication goes through the USA, Switzerland, Germany, France and Serbia.

SSL TUNNELING (TLS)

This method is implemented in a software application STunnel which is a multiplatform GNU/GPL-licensed proxy encrypting arbitrary TCP connections with SSL/TLS.[6]

It is very important to mention that all web servers which use HTTP have a common weakness: all HTTP-traffic is transmitted in plain text and every bit of data in communication travelling between a web server (http) and a client (browser) can be intercepted and read by everyone. That means that whoever is in the chain of passing data to the final destination can read all the data. That also includes usernames and passwords which are encoded, and whose role is to protect web servers against unauthorized access, all are easy to reveal. Only encrypted traffic (HTTPS) between a server and a client can protect all the private data against reading and so called sniffing. By encrypting the traffic between a server and its clients, a sniffer by purpose is able to see which client's IP is exchanging the data with a certain web server at a certain time, but it is practically impossible to decrypt the transmitted data, as long as the sniffer does not have the important randomly generated private key. This is a very large security problem. But, there is a solution: Stunnel – it is a free, open source multiplatform SSL tunnelling proxy program, and it is designed to work as an SSL encryption wrapper between a remote client and local (inetd-startable) or remote server. It can be used to add SSL and TLS functionality to most commonly used inetd daemons like POP2, POP3, and IMAP servers without any changes in the code of the programs.

Transport Layer Security[4] (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols are in widespread use in applications such as web browsing, email, Internet faxing, instant messaging, and voice-over-IP (VoIP). Major web sites (including Google, YouTube, Facebook and many others) use TLS to secure all communications between their servers and web browsers.

The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications. When secured by TLS, connections between a client, i.e. web browser, and a server will have one or more of the following properties:

- The connection is private because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated at the start of the session. The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data are transmitted. The negotiation of a shared secret is both secure (the negotiated secret is unavailable to eavesdroppers and cannot be obtained, even by an attacker who places himself in the middle of the connection) and reliable (no attacker can modify the communications during the negotiation without being detected);

- The identity of the communicating parties can be authenticated using public key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server);

- The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

Stunnel uses OpenSSL or SSLeay libraries for cryptography. This means that Stunnel will be used to accept the client requests and establish an encrypted (HTTPS) connection, using SSL or TLS.

For example, one configuration that can accomplish a secure communication is STunnel with a HFS server which is enabled for https communication:

- Stunnel accepts requests from any IP in worldwide web on port 443 which is the HTTPS default port;

- Stunnel then connects to a HFS server on a chosen free port (i.e.44300);

- HFS server accepts requests on that chosen port in this example 44300;

- All the direct requests from clients to HFS on port 44300 have been blocked, except from 127.0.0.1 (localhost address), where Stunnel resides;

- The PC and drives where HFS, Stunnel and the data reside are secured against any unauthorized access.

There are number of algorithms for encrypting the data travelling through the STunnel. In a real example in Figure 7 below, some of them are listed (AES 256bit, RSA, SHA, ECDHE) with SSL version 3.0.

4 https://en.wikipedia.org/wiki/Transport_Layer_Security

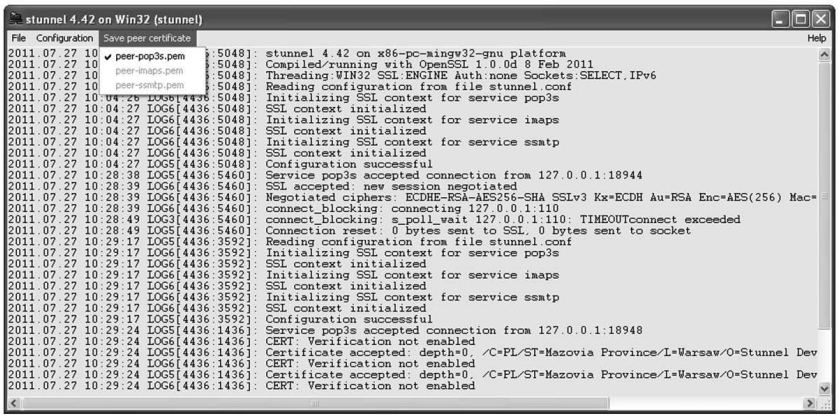


Figure 7: *STunnel software application*

During 2013 and 2014, a number of real experiments were conducted in the Ministry of Interior (MoI), Serbia, as a part of a security testing Project, in the restricted space, testing Tor and STunnel software applications, both on the public Internet network and on the Intranet, a private and protected MoI network. A number of applications were used to sniff the data traffic between clients and a server, trying to discover and retrieve IP addresses and passwords, together with the data transmitted, and with a decrypting techniques, and "man in the middle" computers.

The results were:

- The connections between computers were stable;
- IP addresses of clients and servers were undetected and concealed in a Tor network;
- Data and information exchanged were encrypted;
- Network attacks were detected by the STunnel application;
- SSL and TLS protocols were stable.

It is very important to mention that cryptography that was used to encrypt the data transmitted was **Custom made symmetric cryptography mathematical algorithm** (1024 bit). The original encryption algorithm in STunnel was replaced with a special modified testing MOI algorithm, with very strong mathematical methods inside. It was impossible to decrypt the data transmitted and read the information and IP addresses in a secure communication.

CONCLUSION

Technologies for encrypting and hiding communications and data exchanged on the Internet and other computer networks are developing and improving every day. Modern crime and persons are using those software applications and techniques to conceal their activities on the Net, thus hiding their data and identity. In that way it is very hard to retrieve and discover the real identity and communication of the data and files by the police.

Here comes the main reason why the modern technologies, like deep web together with Tor and STunnel software applications with implemented custom made encryption algorithms, are used in hiding cybercrime.

REFERENCES

1. Cyberoam blog: Are you ready to dive into the Deep Web?, Sophos Security, 2016 http://www.cyberoam.com/blog/
2. Donna Leinwand Leger (2014): How FBI brought down cyber-underworld site Silk Road, USA Today, 15th May 2014
3. Dorothy E. Denning and William E. Baugh, Jr.: Hiding crimes in cyberspace, Cybercrime, Routledge, 2000
4. FBI STories: GameOver Zeus Botnet Disrupted, 2014
5. How criminals have changed tactics after Edward Snowden leaks, The Telegraph, 2014
6. https://www.stunnel.org/index.html

UDC: 004.738.5:323.285
343.341::004

THE CHALLENGES OF CYBER TERRORISM

Katarina Jonev, MSc[1]
Hatidža Beriša, PhD[2]
University of Defence, Military Academy, Belgrade

Abstract: Over the past two decades, cyber terrorism has become one of the methods that terrorist groups have been using. Terrorists have increasingly started using information technologies and the Internet both as an instrument of the fight and as the target of the attack. The term is composed of a words 'cyber' and 'terrorism' and although it is widely used, there is still no globally uniformed definition. Furthermore, there are still no precise, enumerated acts that can be qualified as acts of cyber terrorism. The term refers to the pre-planned, politically motivated attacks against information, computer systems and programs, in order to provoke, above all, a sense of fear and uncertainty. Taking into account that it takes place in cyberspace, it can be understood that the terrorist act was planned, executed, or coordinated by computer networks and by using computers. Like any other form of terrorism, attack has political, ideological, religious, social dimension. The aim is to provoke panic and fear. One of the potentially most dangerous forms is an attack on the state's critical national infrastructure. Hostile groups around the world can potentially hack or illegally enter the computer systems that support national infrastructure and endanger the functioning of the system, shut it down, or change it.

Key words: cyberterrorism, cyber terrorists, terrorism, cyber propaganda, critical infrastructure

INTRODUCTION

Cyberspace is constantly under attack. Cyber criminals, cyber spies, state-sponsored hackers, individuals, are looking for a efficient way to penetrate computer systems in order to fulfill different objectives such as illegal financial gains, steeling private information, industrial secrets, sabotage, transmission of political messages. Vandalism of websites, disruption of the systems, changing data, violation of functioning, installation of viruses, worms, Trojan horses, are just some of the activities that disrupt security in the cyberspace.

Over the years, these resources have become an increasingly powerful tool for terrorists who are using them in order to achieve their objectives. The number of attacks in cyberspace is increasing. Some of them are on a more serious level and scope, some are weaker. States are more than concerned for their safety in cyberspace. Fear of attacks that could endanger the functioning of vital infrastructures, which increasingly relies on ICT technologies, is growing. That is why cyber attacks are among the top priorities in the national security strategies as a serious threat that could endanger the state.

At the same time, fear of cyberterrorism is growing[3]. Term itself became extremely popular in the last years. While the medias are constantly looking for exclusive news and do not hesitate to, at least once a week, announce cyber attacks to be acts of cyberterrorism, in front

1 E-mail: jonev.katarina@gmail.com
2 E-mail: hatidza.berisa@mod.gov.rs.
3 United Nations Counter-Terrorism Implementation Task Force (UN CTITF), Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes, 2009, (available at http://www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf), 12.11.2015

of IT experts and academics around the world, a more difficult task is to determine which attacks and acts can be characterized as cyberterrorism.

On the global level, academic and security experts still have not reached a unified definition or precisely defined acts that can be characterize as cyberterrorism. However, it is more than necessary to make a distinction between cyber terrorist actions and a simple use of cyber space by terrorists. It is not enough to put an equal sign between these two activities, since the situation is far more complex and complicated.

Our growing dependence on information technologies has created new forms of vulnerability that gives terrorists the chance to act.

Cyber terrorists and terrorists share the same political, ideological, religious motives but have a different effect. Cyber, as well as 'classic terrorism', aims to attack and intimidate civilians by using computers, computer networks and the Internet with the motive of spreading its ideals and political struggle[4]. The difference is negligible because more and more terrorists become cyber terrorists and use cyber elements to carry out attacks not only in the physical world but also in the virtual. However, while the 'ordinary terrorists' use traditional, kinetic weapons, cyber terrorists use information and communicational tools such as malware, viruses and computer worms[5] as well as omissions in operative systems and network devices. Cyberspace is more than attractive for terrorists, whose actions can protect their identity and the location of the attack at the same time reaching the goal - making damage to the system, transmitting a message and getting media popularity.

There is a problem for international community to complete the definition and interpretation of the notion 'cyber terrorism'[6]. The very concept is often misused or not well interpreted. The thin line between cyber vandalism (such is damage of websites), cyber incidents, cyber attacks (illegal intrusion into the networks), and the act of cyberterrorism often obscures the essence of the activity. Serious terrorist attacks on vital infrastructure of a country, such as, for example, dams, water systems, electricity, air traffic control, nuclear plants, which can lead to physical damage, destruction, and even death of people, can be considered a terrorist act. President Barack Obama has repeatedly stated that cyberterrorism is one of the most serious threats to national security, institutions and citizens[7].

DEFINING THE TERM 'CYBER TERRORISM'

There is neither a definition of terrorism on the global level, nor a universal definition of cyberterrorism. Cyberterrorism is an illegal act and presents the threat to the computerized systems, networks and information. As any other form of terrorism, it has political, ideological, religious and social dimension. The aim is to provoke panic and fear.

The first attempt to define term cyberterrorism was in 1998. The Report of the Center for Strategic and International Studies, defines cyber terrorism as "politically motivated attack of sub-national groups or the individuals on the computer systems, the computer programs and data that lead to violence against non-military targets[8]". Cyberterrorism can be defined as "the

4 Denning Dorothy: "Activism, Hactivism, Cyber Terrorism", Networks and Netwars, John Arquilla, David Ronfelt, eds, RAND, 2001, p.281

5 Daphna Canetti, Michael L. Gross, Israel Waismel-Manor Asaf Levanon & Hagit Cohen, Streaming Terror: Cyber-Terrorism and its Global Threat, p. 2

6 Taliharm Anna Maria:„Cyberterrorism in Theory or in Practice? "Defence against Terrorism Review, Vol. 3mNo 2, 2010

7 http://www.ibtimes.com/obama-says-cyberterrorism-countrys-biggest-threat-us-government-assembles-cyber-warriors-1556337,pristupila 23.11.2015

8 Center for Strategic and International Studies "Cybercrime, Cyberterrorism, Cyber Warfare, Averting and Electronic Waterloo", CSISM 1998

use of computer networks to shut down critical national infrastructure - such as the energy sector, transport, industrial plants, and to intimidate the government and the civilian population[9]".

Cyber terrorism is the form of terrorism that involves the use of computer "to cause a collapse in the public services and critical national infrastructure and also to cause a lack of public confidence in the institutions[10]". The definition of cyberterrorism can be interpreted as "politically motivated use of computer, either as a target or as a weapon of sub-national groups or clandestine agents who want to violently cause disturbance affecting the public and governments"[11].

A pioneer in the definition of cyber terrorism, professor Dorothy Denning[12]argues that a particular act can be characterized as cyber terrorism if "the attack results in violence against people or property, or make damage that will cause fear"[13]. According to Professor Denning "computer is the weapon of attack". Cyberterrorism can be interpreted as "a development phase of traditional terrorism[14]" and cyber terrorists are "people who are using computers to execute cyber attacks on national infrastructure[15]".

From the listed definitions, it can be concluded that cyberterrorism is the illegal act in which computer and the Internet are the weapons that are applied in order to endanger human life and national infrastructure. Attacks on computer systems and networks that can cause disruption in functioning, loss of life or injuries, are acts of cyber terrorism. According to security expert Gabriel Weimann, there are more and more reasons to be afraid precisely from these kinds of attacks[16].

Not every cyber attack is automatically the act of cyberterrorism[17]. The use of popular social networks, uploading photos, videos, vandalism of websites (such as changes in appearance of the home page), are some of the activities terrorists around the world use as the tactic. The Internet provided easier communication, either between members, or with 'public'. However, the propaganda of terrorists cannot be independently qualified as an original act of cyberterrorism.

On the other hand, the cyber space has allowed terrorists to enter our homes indirectly by creating an important psychological element to cause fear and helplessness[18]. An increasing number of theorists point out that terrorists will continue to use cyber space to achieve their ideological objectives. This includes the use of the Internet in particular, as a global media in order to spread their propaganda, for recruitment, data mining, gaining publicity, planning actions, easier communication.

9 Lewis, James. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats". December 2002
10 SooHoo, K., Goodman, S. and Greenberg, L.:"Information technology and the terrorist threat", *Survival*, vol. 39, no. 3 (autumn 1997), pages 135–55
11 Clay Wilson: Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, October 2003, p 7
12 Dorothy E. Denning is the professor of computer science at Georgetown University and Director of the Georgetown Institute for Information Assurance
13 Dorothy E. Denning Cyber Terrorism, published version of a paper appeared in Global Dialogue), August 24, 2000
14 Roland Heickerö, Cyber Terrorism: Electronic Jihad, Strategic Analysis, 2014 Vol. 38, No. 4, p. 554–565
15 See: Verton, D., *Black Ice: The Invisible Threat of Cyber-Terrorism*' New York 2003 and Awan I. "Debating the term cyber-terrorism: issues and problems", Internet Journal of criminology, 2014
16 G. Weimann, www.terror.Net: How Terrorism Uses the Interne', United States Institute for Peace, special report number 116, 2004
17 Denning Dorothy "Activism, Hactivism, Cyber Terrorism", Networks and Netwars, John Arquilla, David Ronfelt, eds, RAND, 2001, p. 21
18 Julian Charvat "Radicalization on the Internet" Defence against Terrorism Review Vol.3, N o. 2, F all 2010, p. 80

CYBER TERRORISTS OPERATIONS IN CYBER SPACE

We need to distinguish cyber terrorism from simple activities done by terrorists in cyberspace. Terrorists use the Internet as a global communication network to spread their propaganda, for easier communication, in order to recruit new members. These effects are only one of the instruments of action of terrorists but these are not a cyber attack that has aim to target the computerized systems[19].

Thus, we can conclude that activities of terrorists in cyberspace - such as uploading video and audio recordings, photographs, publication, news, blocking websites, spreading propaganda materials - could cause fear, terror, panic. Furthermore, they can raise the level of security and may have political background but these activities cannot cause death, injury or physical damage. Therefore, it is important to underline the difference between cyber attacks that can cause cyber terrorists and terrorist activities carried out in cyberspace.

The most common activities of terrorists in cyberspace are global in character, because the Internet is a global network that does not know borders between countries. Among other things, these activities include the following:

1. Propaganda – throughout websites and popular social networks
2. Financing group - online donations which are anonymous or by creating false humanitarian funds
3. Recruitment of new members - mainly young people
4. Easier communication among members - from hidden chat rooms and forums, throughout social networks, terrorists are communicating openly with their supporters
5. Cyber terrorist act - the attack on the state critical infrastructure

Terrorists use the Internet as an extremely efficient communication medium that provides ability to communicate with the public, supporters, sympathizers, members. Propaganda is the main activity of terrorists on the Internet. They are sending their political, ideological and religious messages, photos and videos, newsletters, to further popularize their principles, especially with younger population. It is well known that Osama Bin Laden communicated with the members of Al Qaeda through a laptop and a wireless network via encrypted messages. On the other hand, the Islamic State has made revolution when it comes to use of popular social networks such as Twitter, Facebook, Instagram, Youtube channels in order to spread their propaganda to a larger circle of people.

At the beginning of the new millennium, almost all major terrorist groups have their own websites dedicated to the work of the organization. These include, among others, Al Qaeda, the Tamil Tigers, Hamas, Lebanese Hezbollah, the Popular Front for the Liberation of Palestine (PLFP), the Basque ETA, and Irish Republican Army (IRA). On the websites, the organizations publish information related to the work and conscience, ideological messages, the group's activities and goals, important dates for the organization, biographies of leaders, as well as messages to enemies. Terrorists are using websites and social networks to promote their principles, to defend their doctrine, and to provide distorted idea about themselves to people around the world.

Access to the Internet is increasingly important for terrorists. Modern ways of communication have given terrorists the ability to facilitate the organization of groups, to plan and conduct the attacks. Supporters and members of terrorist groups can get via e-communication instructions on conducting attacks, necessary maps, instructions on making bombs and similar weapons.

19 Gabriel Weimann „Cyber Terrorism: The sum of All Fears" Studies in Conflict and Terrorism 28, Taylor & Francis Inc, 2005. p. 130

Moreover, terrorists successfully implement recruiting of new members using modern ways of communication. Terrorists take advantages of factors such as injustice, poor living standard and feelings of rejection, which often occurs to young people, in order to persuade them to join the group[20].

Terrorists are also creating online campaigns in order to collect donations and money to finance their activities. On Al-Qaeda website, it is possible to buy t-shirts, flags, CD and DVDs[21].

With the development of cyberspace, interest of terrorist for its abuse will grow.

IS CYBER TERRORISM A REAL THREAT?

Among academics and security experts term 'electronic Pearl Harbour' has become very popular. It is a term that describes potential, a surprise attack on the commands and control systems of critical infrastructure that could paralyze their operations[22]. Fear of such attacks is increasing, especially in highly developed countries.

In the previous years, hackers demonstrated weaknesses of the system by taking over sensitive information and control of the crucial services. In the future, terrorists could also start applying these methods. States, political groups, economical, military and national institutions, i.e. all those who are labelled as 'enemies', have become targets of cyber terrorists. This could be great threat to the states, international organizations and the security of us all.

The question is whether cyber terrorism nowadays is a real danger. We should bear in mind that to this day act of cyber terrorism has not occurred and that both the practice and theory are extremely divided when it comes to interpreting a cyber terrorist act. However, experts agree that the use of IT technologies in terrorist purposes is a real danger to the states.

Cyber terrorism is a threat to the international community as much as any other forms of terrorism[23]. Sufficiently trained terrorists are capable to attack the infrastructure of state by manipulating information or disordering information[24]. The power of terrorists to disrupt the economic system of a state by inserting erroneous information is potentially large. The target of cyber terrorists may be found in healthcare, government and military institutions.

In the developed countries, critical national infrastructure relies on operation and functioning of computers and ICT technologies and therefore it may be an easy target. If we take into account that the national infrastructure includes, inter alia: energy systems, nuclear power plants, dams, electricity and water supplies, transport traffic (such as air traffic control at airports), telecommunications networks, it can be clearly concluded that potential attack on these systems could have enormous consequences to the country and mostly to the civilians. The possibility that terrorists can attack the system, either through damaging its functions, alteration mode, or through the control systems, is frightening. Such an attack would also cause potentially enormous environmental catastrophe as well as the financial loss. The fact is that this will become more and more national, regional and global security challenge.

20 European Commission, Expert Group on Violent Radicalization, "Radicalization Processes Leading to Acts of Terrorism" (2008) (available at www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf.), pristupila interenetu 24.11.2015.

21Awan Imram: "Debating the term cyber-terrorism: issues and problems", Internet Journal of criminology, 2014 ISSN 2045 6743, p.9

22 Roland Heickerö "Cyber Terrorism: Electronic Jihad" Strategic Analysis, 2014 Vol. 38, No. 4, p.555

23Gábor IKLÓDY The New Strategic Concept and the Fight against Terrorism: Challenges & Opportunities, Defence against Terrorism Review Vol.3, No. 2, Fall 2010, p.5

24 Murat Dogrul, Adil Aslan, Eyyup Celik: "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", 2011 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 2011 © CCD COE Publications, p.30

An important element that must be taken into consideration is whether the attack on the infrastructure can produce potential damage that would cause death or injury to people. What is also a very important question is whether the motive of the attackers is exactly that - to endanger the functioning of the system, to provoke the death or injury of people, in order to convey a political message of terrorists[25].

To terrorists, cyber space provides an opportunity to attack the system and jeopardize its functioning, to manipulate with data, to make modifications or deletion. This is an efficient, effective and economical way of intimidation and demonstration of power of cyber terrorists.

CONCLUSION

Although the terrorists have shifted their action to cyberspace, they have not given up their traditional ways of struggle.

Cyberspace is a little paradise for terrorists. Anonymity is a major advantage. Minor financial investments are needed and a few keystrokes to send a message of hate. But it takes more than that in order to jeopardize functioning of the national infrastructure. The systems are protected and complex. Terrorists still have not demonstrated capabilities for a sophisticated cyber attack. States are becoming more aware of this issue and have already started creating their national cyber strategies as well as systems of defence.

Terrorists have not yet and will not for a long time in the future replace bombs with a keyboard. In the years to come and with the development of digital technologies, fear of experts, that the new generation of terrorists will be much more adept at using computers to launch attacks, is justified.

REFERENCES

1. Denning Dorothy., (2001) „*Activism, Hactivism, Cyberterrorism*", Networks and Netwars, John Arquilla, David Ronfelt, eds, RAND
2. Daphna Canetti, Michael L. Gross, Israel Waismel-Manor Asaf Levanon&Hagit Cohen: Streaming Terror: Cyber-Terrorism and its Global Threat
3. Taliharm Anna Maria., (2010),„*Cyber Terrorism in Theory or in Practice*?",Defence Against Terorrism Review, Vol 3mNo 2, 2010, http://www.ibtimes.com/obama-says-cyberterrorism-countrys-biggest-threat-us-government-assembles-cyber-warriors-1556337
4. Center for Strategic and International Studies „Cybercrime, cyberterrorism, cyberwarfare, AvertingandElectroinic Waterloo", CSISM 1998
5. Lewis, James.,(2002) " *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*." December
6. SooHoo, K., Goodman, S. and Greenberg, L.,(1997),„*Information technology and the terrorist threat*", Survival, vol. 39, no. 3
7. Clay Wilson Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, October 2003
8. G. Weimann., www.terror.Net: How Terrorism Uses the Internet', United States Institute for Peace, special report number 116, 2004
9. Julian CHARVAT "*Radicalization on the Internet"* Defence against Terrorism ReviewVol.3, N o. 2, F all 2010

25 Dorothy E. Denning "Cyber Terrorism", published version of a paper appeared in Global Dialogue), August 24, 2000

10. Gabriel Weimann., (2005) „*Cyberterrorism: The sum of All Fears*", Studies in Conflict and Terrorism, 28, Taylor&FrancisInc
11. European Commission, Expert Group on Violent Radicalisation, "Radicalisation processes leading to acts of terrorism" (2008).
12. AwanImram., „*Debating the term cyber-terrorism: issues and problems*", Internet Journal of criminology", 2014 ISSN 2045 6743
13. Roland Heickerö „*Cyber Terrorism: Electronic Jihad*" Strategic Analysis, 2014 Vol. 38, No. 4, str. 555 (http://dx.doi.org/10.1080/09700161.2014.918435)
14. Gábor IKLÓDY The New Strategic Concept and the Fight against Terrorism: Challenges & Opportunities, Defence Against Terrorism Review Vol.3, No. 2, Fall 2010
15. Murat Dogrul, Adil Aslan, Eyyup Celik "*Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism*", 2011 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 2011 © CCD COE Publications

UDC: 343.436
343.436::004(73)

STALKING AS A SOCIAL PHENOMENON WORLDWIDE WITH SPECIAL REFERENCE TO CYBERSTALKING IN THE UNITED STATES

Stojan Troshanski, MA[1]
Latif Latifi, MA[2]
Zafirco Pancev, MA[3]

Abstract: Stalking is a widespread social phenomenon. It existed in the past, but is especially evident in the present framework. The reason for this is the new lifestyle of people, the possibility of today's technology that contributes to communication among people to be more intensive. With the development of information technology in the early 90s, a new opportunity and a way for monitoring and terrorizing the victims of stalking emerged.

Given that stalking was incriminated for the first time as criminal behavior in the state of California in the United States, the authors of the paper will try to present statistical information of the rate of this type of crime. Furthermore, as a central issue, this research elaborates the cyberstalking as a special kind of stalking, which is widespread across the United States. This paper aims to point out the seriousness of the existence of cyberstalking which is a degenerative social phenomenon as a product of modern living. State institutions and non-governmental non-profit organizations are involved in the fight against stalking. The mission of these institutions and organizations is to detect new cases of stalking, as well as to provide assistance to their victims and to inform the general public about the threats and dangers that they may be faced with or that are related to stalking.

Through a comparative statistical analysis of the data available to the authors, the goal is to give an opinion for the trend of increasing the rate of this type of crime and whether and how to prevent new cases of cyberstalking.

Key words: stalking; cyberstalking; statistics; anti-stalking law; victim; crime;

INTRODUCTION

The modern world in which we live is filled with a variety of social actions that people take and are not incriminated worldwide. Some of these procedures are less worrisome, while some have greater impact on those affected by them. Stalking is a particularly worrying social phenomenon. Considering its character, it has more elements and typologies through which it can be recognized, and in some countries it is even incorporated into the national law as a criminal offense. As a social phenomenon it existed in the past, but today it is starting to be

1 stojantroshanski@yahoo.com
2 l.latifi@yahoo.com
3 zafircopancev@gmail.com

incriminating due to increased consequences it brings on. Victims often react in time, but often the reaction of the authorities does not give a positive result. Some of the victims even end tragically. The subject of this paper is stalking as a social phenomenon with particular reference to cyberstalking in the United States.

With the development of information technology, the space of the emergence of new crimes and new ways of performing the same open up. As a result, cyberstalking as a special kind of stalking shows a wide representation in the United States. The number of victims of stalking is getting bigger and bigger. As a social phenomenon which was declared as a crime in the early 90s of the last century, stalking still cannot be prevented despite the efforts of the state institutions dealing with this issue and the non-governmental-non-profit organizations that provide help and support to the victims of stalking. With the trend and methods of use of the Internet - communication technology in the last two decades, stalking cannot be prevented.

At the outset, this paper gives a variation of definitions of what exactly is stalking in its broadest form, giving some examples as the introduction to this social phenomenon which has worrying upsurge of galloping size. Furthermore, we will explain the typology of the crime in short and present statistical information referring to stalking in the US. The main part of the paper analyzes cyberstalking as a modern kind of stalking. The paper also includes the results from surveys conducted in the United States testifying the risk of the large presence of this crime. Statistical data are processed by the relevant government institutions in the US formed in order to analyze the situation in American society where stalking as a criminal phenomenon is a matter in issue. The final part of the paper offers certain ways and modalities that could help in the fight against stalking or cyberstalking as separate specie.

DEFINING AND TYPOLOGY OF STALKING

Scientists dealing with stalking define it in various ways. In the broadest sense today, cyberstalking involves monitoring, harassment or sexual harassment in general, violence which may occur in the workplace, threats of various types. In the region of Europe there is very little scientific literature about this topic. For the first time stalking is incriminated in 1990 by the state of California in the United States, with the introduction of Anti-Stalking Law. Immediately afterwards, this trend of incrimination continues in Canada and some European countries such as Belgium, Germany, England, Ireland.[4]

In the United States there are multiple levels of protocols through which this phenomenon is sanctioned.

Thus, the first interventional level is for early raising of human consciousness through detention of stalkers and their prosecution. The second level gives emphasis to the victim through measures / programs that are targeted at their social rehabilitation. The third level gives an emphasis to the stalker through various measures aimed to inform and warn him, by checking his criminal record, referral to counseling, his detention and surveillance, and all in order to prevent further stalking of the victim.

The origin of the term stalking comes from the typical hounding of animals during hunting in nature. The stalking can also be considered as old phenomenon too.[5]The recognition and determination of stalking had a way of simplifying and reducing the monitoring, harassment, sexual harassment, violence in the family, workplace violence, threats and serial

4 Vesna Nikolic-Ristanovic, Marina Kovacevic-Lepojevic, *December 2007,* Stalking: concept, characteristics and social responses, *TEMIDA*, *p.3*

5 Vesna Nikolic-Ristanovic, Marina Kovacevic-Lepojevic, *December 2007,* Stalking: concept, characteristics and social responses, TEMIDA, p.3

murders in order to understand the phenomenon in a broader sense today. This phenomenon must and cannot be linked to the phenomena with which that intertwines and equates.[6]In modern sense, transferred to interpersonal level, it can be understood as a systematic harassment and behavior of a person who persecutes another person. Because of its complex nature and variations that may occur, there is no precise definition of it. Stalking may include multiple acts done by the stalker which are not criminal offenses, such as sending messages by phone, by mail, standing in front of someone's house, etc. If we analyze the psychological state of the modern man, *Erich Fromm* says that man is alienated, lonely, overwhelmed by a sense of insecurity.

The first starting definition of stalking includes willful, malicious, continuous monitoring and harassment of a person by another person (stalker), thus compromising an individual's safety[7]. The basis of this definition is derived from the elements of the definition (repetition of the act at least twice, infringement of privacy of the victim, and the existence of evidence of threats or fear in it, and the possibility of stalking of the victim or a person close to her/him).[8]

The penalty provisions (Cal Pen Code 646.9 Stalking. 2008) of the Anti-stalking Law of the state of California sanctioned the following legal qualifications: "Any person who maliciously and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent of the person to install fear for his or her safety or the safety of his closer family is guilty of the crime of stalking, punishable by imprisonment up to one year or with fine up to one thousand dollars ($ 1000), or a combination of both types of punishments".[9] The penalty provisions (ALM GL ch. 265 43 Stalking. 2010)of the Anti-stalking Law of the state of Massachusetts regulates this in the following way: "The one who willfully and maliciously engages to organize series of acts during one period of time targeted at a specific person that seriously disturbs and causes considerable suffering and emotional stress, and makes the threat with the intent to place that person in fear of immediate death or bodily injury shall be guilty of a crime of stalking and will be punished by imprisonment in the state prison up to 5 years or a fine of up to $ 1000 or imprisonment in a penal or correctional institution up to 2 years or a combination of both sentences".[10]

Scientists, who are studying stalking as a phenomenon, are giving different definitions and each of them places emphasis on a certain element. Thus, *Jovanovic* adds a feeling of nausea that appears among the victim who is stalked, *Davis* and *Sheridan* indicate the special feeling of threat and harassment.

A stalker wants to establish full control over the victim's life and his/her way of behavior. A stalker is characterized by one feature - the persistence in the committing of the crime. In most cases stalking is usually a result of a previous narrow-associated emotional relationship between the stalker and the victim. That anger and rage that may appear at the beginning when the victim is aware that someone is stalking her/him often develops into depression, fear, desire for suicide. These symptoms are exhaustively enumerated in the special report on "The stalking criminalization in the United States" prepared by professor *Katrina Baum*, *Shannan Katalano* and *Michael Rand*, in 2009.[11]However, with the development of informa-

6 Vesna Nikolic-Ristanovic, Marina Kovacevic-Lepojevic, *December 2007,* Stalking: concept, characteristics and social responses, TEMIDA, p.3

7 Meloy, J. R. &Gothard, S. 1995, Demographic and clinical comparison of obsessional followers and offenders with mental disorders. American Journal of Psychiatry, 152, 258-263

8 https://www.ncjrs.gov/pdffiles/169592.pdf

9 http://www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-laws/criminal-stalking-laws-by-state/california#646

10 http://www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-laws/criminal-stalking-laws-by-state/massachusetts

11 https://www.victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0

tion technology, the method by which stalking is performed is changing. Today cyberstalking is often present among the celebrities. Rarely present modes of stalking are breaking into the home of the victim, criminal actions of various kinds against the victim or her/his relatives, etc. The dangerous consequence of stalking is that after its completion, the life of 1/3 of the victims changes completely. There are cases of agoraphobia too.

There are three forms (typologies) of the crime:

- stalking the person with whom the perpetrator (stalker) has already been in a relationship, regardless of the time in which the stalking began;[12]

- stalking the person with whom the perpetrator (stalker) wanted to realize a relationship (they were not in a previous relationship);[13] and

12 The case of stalking with tragic end is known in Belgrade, Serbia. It is a stalking which resulted in a tragic outcome. The victim was killed by the male stalker, and then he committed suicide. The stalker was a neighbor of the victim. He was a violent man. The victim who was named Slavica Rakulj (49) lived with her mother in the municipality of Zemun, Belgrade. The stalker, named Goran Milovanovic (50) killed the victim in a café in which the victim worked as a manager. The murder was committed with a gun when he fired four bullets into the victim's back, and after that committed suicide. There are additional details about the murder. Both the victim and the stalker were in previous emotional relationship, thus placing this case of stalking in the first kind of stalking of the person with whom the stalker had already been in a relationship, i.e. they had known each other before. The last words of the killer before he committed suicide reveal that he was obsessed with the victim: "Slavica, I cannot live without you". Further information revealed that the stalker had received restraining order forbidding him to approach the victim issued by the state judicial authorities.
Another case is an example of cyberstalking as a special kind of stalking. To protect the identity of both parties we will use pseudonyms. The stalker will be known under the name Trajče and the victim under the name Trajanka. This is the case that is well known to me and I was in direct contact with both persons. It is about my acquaintances from the past from the city X, who had been in relationship for several years. Both were very attached to each other, but the attachment of the male prevailed. After a period of time and a number of bickering, they ended the relationship. I (in the company of a few more people) was present at the moments when all argues between them happened. One day while I was sitting in a cafe bar with the alleged "stalker" (because it is not yet clear whether he actually stalked her, but there were elements of cyberstalking) he received a call from his former partner, in this case a "victim" asking him (as the stalker told me later) to leave her alone and not to push her on one of the social networks. It was about Facebook. I learned that he used a fake profile (previously the victim had blocked his Facebook profile) to supervise the profile of the victim on the Internet, and what she made after they had split. I think Trajče still loved Trajanka. The culmination was the moment when after a short time, Trajce received a call from the victim`s sister. During the conversation the sister of the victim informed Trajče that they had reported him to the police and delivered the victim's computer and all the messages that he posted to her on the Internet as evidence. I think the case ended there. Even the victim's parents interfered talking personally to Trajče, and I think that the situation calmed down then.
13 The famous American singer Rihanna was stalked in 2014 by a mentally disturbed man named Kevin Mekglin, aged 53. He threatened her through messages that he left on the entrance to her apartment in New York. In one of the messages he wrote that he was going to enter her apartment. According to the typology of stalking, this is a type of stalking when the stalker wants to make contact with the victim. This type of stalking involves stalkers suffering from schizophrenia or manic depression. The most extreme form is known as erotomania (dominated by women as stalkers).
Another victim of stalking was the famous Hollywood actress Nicole Kidman. She told the story of the man who stalked her when she was just 18 years old. The stalker was much older than her and followed her wherever she went on a daily basis. According to the physiognomic features of the stalker, she described him as a man with long gray hair. An interesting thing is that the police could not do anything then. Although the famous actress reported the stalker to the police, the police only advised her to be careful. The actress said that she had suffered incredibly terrible experience. In that period the stalking was not incriminated in the US legislation. Nicole Kidman was 18 years old in 1985, five years before the new Anti-stalking law was enacted in the US state of California. This kind of stalking can be placed in the typology as the previous case of the stalking of the singer Rihanna, with the difference that the case of Rihanna had legal outcome. As incredibly popular actress, Nicole Kidman was stalked again in 2001, but then she asked a restraining order for the stalker to be issued by the state authorities.
Another example of stalking involves a famous actress from the TV series "Friends" Jennifer Aniston. The stalker, a 24-year-old Jason Peyton, believed that they were "connected" and he wanted to marry her.

- stalking of a person although there is not the relationship between the perpetrator (stalker) and the victim.[14]

According to a Dutch study conducted on this issue which analyzed stalking as a crime, the result suggest that the stalking period takes approximately 33 months (3 years).

STALKING STATISTICS IN THE UNITED STATES

If the trend of stalking victims continues, then that is proof of the inadequate anti-stalking policy which has been conducted by state authorities in recent years. Considering stalking as a social phenomenon, a sort of degenerative phenomenon and a product of the modern society, it is criminalized for the first time in the United States. In addition, you will be referred to a number of statistics from the late 90s of the last century until 2015.The statistics is processed by the relevant government institutions in the United States established to analyze the situation in the American society.

"Stalking Resource Center", a program of the National Center for Victims of Crime in the United States aims to provide an organized, professional and effective systematic response to stalking and improve the safety of the victims of stalking. In fact, it is their mission.[15]Founded in 2000 with support from the Office on Violence Against Women in part of the Ministry of Justice, it allows familiarization with the legal remedies, multidisciplinary effort, familiarity with the technology used by stalkers when they pursue their crimes and has its own website that is timely and continuously upgraded and updated with new information from the field of the given matter. Of course, prior to the forming of this center, this problem was a subject of other research institutions in the United States in the past.

The first nationwide study in the US on the issue of stalking titled "Stalking in America: *Findings from the National Survey on Violence Against Women* - Research in brief" was conducted in 1998 stating that women are significantly more stalked than men in percentage, and most likely to appear as a stalkers are the former intimate partners.[16]Even then it is perceived that stalking is present much more than was previously thought. Thus, 8% of women and 2% of men in the US are sometimes stalked in their lives. Moreover 1 006 970 women and 370 990 men are victims of stalking annually. Therefore, stalking should be treated as a crime and threat to public safety and health. People aged 18 to 29 are the primary target of stalkers, which represents 52% of all victims.

Another survey conducted by the National Institute of Justice[17]from 2000 shows that the rate of incidence of stalking women who study on campuses is far higher unlike in previous surveys. Stalking defined as obsessive behavior causing victims to fear for their safety

After the actress filed a lawsuit, he was arrested by the police. He was forbidden to approach her home, workplace and car less than 100 meters. When the stalker was arrested, he was carrying a bag, duct tape and a message to the actress, and his car was all coated with the inscriptions: "I love Jennifer Aniston" which indicated that he was obsessed with that Hollywood star. All across America he left inscriptions that he loved Jennifer as his wife. Besides, he also had a police record. In the past he also physically abused his own mother. He had medical treatment with antipsychotics and was once convinced that he was in a relationship with Oprah, Jay-Z, Donald Trump, Courteney Cox, Nelson Mandela and Jennifer Lopez.

14 This type of stalking is different from the previous two because there is no desire to enter into an intimate relationship, but the purpose of the stalker is to harm or punish the victim (stalker sociopaths -predators).

15 http://www.victimsofcrime.org/our-programs/stalking-resource-center/about-us

16 http://www.caepv.org/getinfo/facts_stats.php?factsec=9; https://www.ncjrs.gov/pdffiles/169592.pdf;

17 National Institute of Justice, a research agency under the Ministry of Justice formed in 1968. It is authorized to support research that will improve and strengthen the criminal justice system and reduce or prevent crime. Additionally, the Institute has the authority to conduct evaluations of effects of the implementation of programs for criminal justice and in particular to highlight and identify those programs that have given significant effect or success.

occurred at rates of 156.5 per 1000 female students or 13.1%.[18]Women - victims of stalking reported being stalked 2 to 6 times a week. The three factors that are correlated and increase the risk of stalking women who are students at College are: living alone, spending a long time in night bars and clubs and being at the beginning of relationships, as opposed to a situation in which a woman is married and live with her intimate partner.

According to *Tjaden, P.* and *Thoennes's* full report on the prevalence, indices and consequences of violence against women that were also obtained in 2000, referred to the fact that between 85.4% and 93.6% stalkers were not prosecuted. About 40% of those processed by the system were sentenced, but only 56.3% of the convicted persecutors were sentenced to imprisonment. The rest were sentenced to pay a fine of 1000 American dollars.[19]The criminalization of stalking in the United States is based on the largest collection of data about stalking. The data are collected by the Additional victimization survey, a supplement to the National survey on victimization of crime sponsored by the Office on Violence against Women.

According to the study of the National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, more than 7 million women and 2 million men in the US have been stalked for a period of 12 months. Stalking affected 7% of women (one of 14 women) and 2% of men (one of 50 men) in the United States at some point in their lives. The study was published in the edition of the American Journal of Preventive Medicine in August 2006.

The Ministry of Justice, through its Office of Legal Statistics, issued a special report on "The stalking criminalization in the United States" in 2009, which was prepared by professors *Katrina Baum, Shannan Katalano* and *Michael Rand*. Stalking is widely prevalent and victims of stalking are facing drastic changes in their lives, fear for their safety and they are obliged to seek help from their friends and family members. Assessments are that about 3.4 million-[20]people testified that they had been victims of stalking for a period of 12 months in 2005 and 2006[21]. A half of these people had an unpleasant experience at least once a week, 11% were stalked for a period up to 5 years or more, and 1 of 7 victims changed their place of residence as a result of stalking.[22]The study showed that stalking on grounds of gender was present with 3: 1 for women in relation to men[23], and as far as the age of victims is concerned, the largest percentage of victims of stalking were between 18-24 years old. Furthermore, while women are stalked significantly by male stalkers (67%) than female stalkers (24%), the situation with male victims of stalking is different. Men are stalked by other men in the amount of 41%, and by women (43%)[24]. In the second case, the percentages are almost the same, unlike for women, who are the victims of stalking.

According to the way in which stalking is performed, the largest percentage, about 66% of victims of stalking were uncomfortably harassed through phone calls, 34% were under surveillance or spying, 31% received nasty messages by mail or over the Internet. The most upsetting fact is the percentage of the victims who did not report the stalking to the police promptly, and they accounted for 60%. For the number of the stalkers, the study shows that in 6 of 10 cases of stalking, only one stalker was present, while a much smaller number of the victims reported that they were stalked by two (18%) or three (13%) stalkers[25].

18 http://www.caepv.org/getinfo/facts_stats.php?factsec=9According to the National Institute of Justice. 2000. Sexual victimization of female students at college. Washington, DC: Department of Justice
19 https://www.ncjrs.gov/pdffiles1/nij/183781.pdf; http://www.caepv.org/getinfo/facts_stats.php?factsec=9;
20 http://crime.about.com/od/stats/a/stalkingstats.htm
21 http://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf
22 http://www.caepv.org/getinfo/facts_stats.php?factsec=9
23 Nearly 3 out of 4 victims knew the identity of their stalker.
24 http://www.caepv.org/getinfo/facts_stats.php?factsec=9
25 https://www.victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0

As regards cyberstalking, as a result of the development of modern technology, electronic monitoring of various types is used in 1 of 13 victims[26], most often devices such as digital video-cameras, bugging devices and the like.

Speaking about the ethnicity of the victims, the Asians and the inhabitants of Pacific Islands have lower rate of stalking (7 victims per 1000 persons) than white people (14 victims per 1000 persons) and black people (12 victims per 1000 persons). The biggest risk group refers to the people of two or more races (32 victims per 1000 persons).[27]

The number of victims of stalking varies from year to year, but is an indicator that this problem cannot be solved so easily. According to the official report of the National Center for Injury Prevention and Control, Centers for Disease Control and Prevention issued in 2011, the number of victims of stalking is similar compared to the 2006 report. According to the 2011 report, the number of victims of stalking amounted to 7.5 million. Nearly 3 of 4 victims knew the identity of their stalker, and it was usually their previous or current love partner. Accordingly, 61% of women and 44% of men were stalked by their former or current partner. A significant indicator is the data showing that 1/3 of the stalkers used to stalk in the past, meaning that they performed that crime several times, i.e. they stalked more than one victim. The mentioned data applies to the previous years as well with no significant changes.[28]

In 2012, Robin Hattersley Gray, executive director of the magazine "Safe Campus" which examines the public safety and security of the schools, hospitals and universities across the United States, based in Framingham, Massachusetts[29],published statistical data about the problem with stalking. In the section "Statistics persecution" the data showed that 6.6 million women and men in the US were victims of stalking annually[30]. The analysis revealed that 1 of 6 women and 1 of 19 men had such an unpleasant experience at least once in their lives. Many of them were even afraid for the lives of their loved ones and they believed that their loved ones could be killed by a stalker.[31]Furthermore, more than a half of the victims of stalking were people younger than 25 years of age, which again confirms the fact that young people are the most affected group of victims of stalking. About 2/3 or 66% of the female victims were stalked by their current or former intimate partner. Up to 10% of the victims reported that they had been monitored by using different monitoring systems, such as digital cameras and eavesdropping devices.[32]

"The Fact Sheet" of the Stalking Resource Center for the month of January 2015 published the following statistics: 7.5 million people were victims of stalking during the 12 month period; 15% of women and 6% of the male population at least once in their life had an unpleasant and disturbing experience and fear that it was possible their lives were in danger or the lives of their close friends or family members; 61% of women and 44% of the male population were stalked by a current or former intimate partner. The report emphasized the fact that almost a half of the victims of stalking were under 25 years of age; 11% of the victims were stalked in a period longer than 5 years.[33]

26 http://www.caepv.org/getinfo/facts_stats.php?factsec=9
27 https://www.victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0
28 http://www.victimsofcrime.org/docs/default-source/src/responding-to-stalking-a-guide-for-community-correctionsaf9bf82e2c3f4f608830756c920f85ec.pdf?sfvrsn=0
29 http://www.campussafetymagazine.com/site/about_campus_safets
30 http://www.victimsofcrime.org/docs/src/stalking-fact-sheet_english.pdf
31 http://www.campussafetymagazine.com/article/Stalking-Stats; http://sites.jcu.edu/vpac/pages/stalking/stalking-statistics/;
32 http://www.campussafetymagazine.com/article/Stalking-Stats; http://www.wgac.colostate.edu/stalking-statistics;
33 https://www.victimsofcrime.org/docs/default-source/src/stalking-fact-sheet-2015_eng.pdf?sfvrsn=2

The statistics provided by the bodies of the system only testified that the number of victims of stalking has been quite large in the last ten years. It may be noted that no serious steps have been taken in order to prevent this crime, and it is just sanctioned with a fine or imprisonment as a heavier type of legal sanction. It must be pointed out that it is necessary to find the cause of the occurrence of this kind of social phenomenon, not only to work on its consequences.

THE PREVALENCE OF CYBERSTALKING IN THE UNITED STATES

Global social networks with their role contributed to the creation of a new, unremarkable, technically perfected form of crime which is difficult to suppress because of its features that are difficult to spot. The most common types of virtual communication are disturbance through the internet, identity theft, and Internet fraud, manipulation of personal data and misuse of personal photos, interception and recording.[34] In its wider form, cyberstalking refers to stalking through all means of information and communication technology, not only through the Internet network. Cybestalkers rely upon the anonymity afforded by the Internet to allow them to stalk their victims without being detected. Stalking through the Internet is just one type of cyberstalking.

One of the first and broadest definitions of cyberstalking was given by *Paul Bocij* according to whom cyberstalking involves the use of information and communication technologies to abuse another individual, group of people or organization.[35]Most of the actions undertaken by cyberstalkers can be described as deliberately planned, systematically repetitive and too boring. Cyberstalkers have the feeling that they are anonymous and that if they got into a risky moment for them to be discovered, they could easily get away. In case of being caught, they declare that it has not been their intention and that they have not planned to go so far to intimidate the victim. The distinguishing factor between classical stalking and cyberstalking is the geographical element, i.e. distance between the cyberstalker and the victim. Although the cyberstalker can abuse the victim from a neighboring house, he can do that from a distant country, too. Through this method of stalking, the stalker and the victim rarely come into physical contact, so the police do not take further steps when the victim reports stalking.

Why do cyberstalkers stalk and what is their motivation? Mostly, they do it because of:

- *sexual motives:* they sexually harass the victim by sending messages of a sexual nature through the electronic communication systems. By doing so, they remain anonymous and are not afraid of physical retaliation;

- *love obsession*: cyberstalkers believe that the targeted person is a reflection of their life desires and dream about the person who would be ideal for them. Thereby, they do not accept *no* as an answer;

- *hate / vendetta* whereas, in this case there is no reference to the first motive, sexual motives / desires;

- *power of self-esteem and increased ego:* in this case, the victim is chosen at random. The motive of this type of cyberstalkers is to prove themselves and sometimes to prove to their friends that they have a real capacity to attract and win over a person.

34 Vida Vilić, March 2013, Stalking victimization through the Internet**,** TEMIDA, p. 151
35 Bocij, P.2004, Cyberstalking: harassment in the Internet age and how to protect your family. Westport: Praeger Publications, p.14

If online users continue with publishing their private information / data and details of their lives through social networks, then we cannot expect positive results in preventing cyberstalking in future.

This type of stalking is of the utmost interest to many organizations throughout the US. "WHOA" is a volunteer organization established in 1997 whose mission is to fight against Internet harassment through training of the Internet community in the US.[36] Its founder Jayne Hitchcock[37]is an expert on cybercrime and security. She draws attention of educational institutions, libraries, corporations and the general public to the problem of cybercrime and online security, and provides consulting services for several organizations, including the Ministry of Justice, Office for Victims of Crime, National Center for Victims of Crime and other organizations. "WHOA Kids/Teen Division"[38] is part of "WHOA" which specifically deals with the fight against online bullying, harassment and stalking of children and teenagers. By educating parents, teachers and the general public, and law enforcement agencies, this organization provides assistance to the victims letting them know that they are not alone.

In the early 2000s "WHOA" began to survey the victims of cyberstalking. The organization has statistical data for a period of 2000-2011. The questionnaires are filled out completely, but unfortunately they are not based on the total number of cases handled in the organization. "WHOA" receives 50-75 new cases of cyberstalking on a weekly basis. The total number of the processed cases is presented in the following table taken directly from the website of "WHOA":

Table 1: *Comparative Statistics (2000-2011).*[39]

WHOA (HALTABUSE.ORG)
COMPARISON STATISTICS 2000-2011

# OF CASES	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL	%
	353	256	218	198	196	443	372	249	234	220	349	305	3393	
VICTIM GENDER														
Female	87%	79.3%	71%	70%	69%	67%	70%	61%	71%	78%	73%	74%	2453	72.5
Male	13%	16%	28%	27%	18%	25%	28.5%	21%	21%	21%	27%	26%	788	22.5
UNKNOWN	0	4.7%	1%	3%	13%	8%	1.5%	18%	8%	1%	0%	0%	152	5
HARASSER GENDER														
Female	27%	32.5%	35%	38%	23.5%	21.5%	27.5%	30%	31%	35%	36%	33.5%	1021	30.25
Male	68%	58.6%	52%	52.5%	52.5%	43.5%	36.5%	39%	42%	45%	44.5%	40%	1615	47.5
Multiple/Gangs	0	0	0	0	0	2.5%	0	0	0	0	3%	0%	34	1.25
UNKNOWN	5%	8.9%	13%	9.5%	24%	32.5%	12.2%	31%	27%	20%	16.5%	26.5%	723	21
VICTIM AGE														
Under 18	0	0	0	0	0	1%	0	0	2%	0	.25%	0%	10	.5
18-30	54%	44.6%	50%	63.5%	48%	38%	40%	28%	35%	34%	41%	35%	1352	39.75
31-40	27%	26.2%	36%	25%	27%	25%	29%	24%	23%	30%	29%	33%	943	27.75
41+	19%	6.3%	2%	6%	23%	30%	28.5%	29%	32%	32%	27.5%	32%	862	24.75
UNKNOWN	62.5%	22.9%	12%	5.5%	2%	6%	2.5%	19%	8%	4%	2.25%	0%	226	7.25
VICTIM RACE														
CAUCASIAN	55%	60.6%	77%	75%	78%	73%	76.5%	66%	74%	69.5%	66.5%	82%	2398	70.5
HISPANIC	1.5%	2.7%	4.5%	6%	3.5%	5.5%	4%	4%	6.5%	3%	5%	6.75%	149	4.25
ASIAN	1%	4%	3%	2%	3%	4%	6%	5%	4%	8.5%	6.25%	3.75%	140	4
AFRO-AMERICAN	.5%	1.6%	3.5%	5%	3%	4%	2.5%	3%	3.5%	7.5%	6%	5.5%	126	3.5
NATIVE AMERICAN	1%	2%	1.5%	1.5%	1%	2.5%	1.5%	1%	2%	1.5%	1.25%	1.5%	53	1
EAST INDIAN	1%	.8%	1.5%	.5%	1%	1%	0	0	0	0	.25%	.5%	17	.25
UNKNOWN	0	28.3%	9%	10%	10%	10%	9.5%	24%	10%	10%	14.75%	0%	510	16.5

36 http://www.haltabuse.org/resources/stats/index.shtml
37 She herself was a victim of cyberstalking by the owner of the company, Jane once complained to the company's services. The cyberstalking began as follows: a cyberstalker began with sending messages in her name to many websites and certain persons. The ultimate goal of the cyberstalker was for Jane to be blamed for these actions. Although Jane filed a lawsuit against cyberstalking, this case was dismissed.
38 http://www.haltabusektd.org/
39 http://www.haltabuse.org/resources/stats/Cumulative2000-2011.pdf

VICTIM MARITAL STATUS*	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL	%
SINGLE	N/A	40.7%	48%	40.5%	44%	37.5%	46%	32%	31.5%	43%	45.5%	53%	1281	36
MARRIED	N/A	28.1%	32%	33%	28.5%	31.5%	29.5%	27%	18.5%	27%	28.25%	26%	858	25.25
DIVORCED	N/A	5.9%	7%	10%	11%	11.5%	10.5%	8%	11.5%	11.5%	11.5%	14%	312	9.25
LIFE PARTNER	N/A	2%	5%	8%	5.5%	4%	6%	3%	2%	2%	2.5%	4%	124	3.75
SEPARATED	N/A	1.2%	2%	2%	4.5%	2.5%	2.5%	1%	2%	2%	4.25%	2%	67	1.5
WIDOWED	N/A	0	.5%	1.5%	1%	1.5%	.5%	3%	.5%	.5%	0	1%	27	.75
UNKNOWN	N/A	22.1%	5.5%	5%	4.5%	11.5%	5%	26%	34%	34%	8%	0%	724	23.5

(*We didn't calculate this statistic until 2001)

RELATIONSHIP TO VICTIM	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL	%
YES	47%	45.3%	59%	58%	45%	49.5%	48.5%	44%	57%	61%	47%	59%	1680	49.25
NO	53%	44.3%	41%	42%	54%	50.5%	51.5%	56%	43%	39%	53%	125%	1686	49.75
UNKNOWN	0	10.4%	0	0	0	0	0	0	0	0	0	0%	27	1

IF YES, HOW?	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL	%
EX	25.5%	N/A	28%	57%	53.5%	33.5%	47%	31%	45%	43%	55%	56%	661	39.5
FRIEND	28%	N/A	16%	20%	9%	10.5%	12%	14%	6%	7.5%	7%	12.75%	207	12.5
WORK	0	N/A	9%	9%	6%	11.5%	6.5%	7%	6.5%	8%	8%	7.25%	113	6.75
ONLINE ACQAINTANCE	0	N/A	28%	7.25%	20%	26.5%	25%	27%	8%	22%	12%	7.25%	273	16.25
SCHOOL	0	N/A	1.5%	5%	6.5%	4%	5%	1%	.5%	4%	3.5%	1.5%	47	2.75
FAMILY	25.5%	N/A	4%	1.75%	5%	3.25%	4.5%	13%	8%	14%	6.5%	12.75%	140	0
ONLINE EX	0	0	0	0	0	5.5%	0	0	19.5%	0	0	0%	38	2.25
OTHER	21%	N/A	13%	0	0	1.25%	0	7%	6.5%	1.5%	8%	2.5%	201	20

HOW DID HARASSMENT BEGIN?	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL	%
EMAIL	39.5%	40.3%	47.5%	35%	41.5%	35%	31%	36%	36%	34%	34%	32%	1192	35.25
MSG BOARD*	17.5%	16.9%	14%	16.5%	13.5%	16.5%	16.5%	11%	11.5%	8.5%	9.5%	7%	460	13
IM	13%	5.9%	11.5%	17%	17.5%	16%	17%	11%	8%	13%	6%	2.75%	392	11.5
CHAT	15.5%	14.1%	7.5%	8%	5.5%	8.5%	7.5%	5%	5%	6%	2.5%	4%	266	8
WEB SITE	7.5%	6.3%	8.5%	7.5%	6%	3.5%	8%	6%	5%	7%	4.5%	10.5%	261	7.75
FACEBOOK	--	--	--	--	--	--	--	--	--	5.5%	16.5%	16%	115	3.5
PHONE	--	--	--	--	--	--	--	--	7%	2.5%	6.25%	0%	54	1.75
MYSPACE	--	--	--	--	--	--	--	--	5.5%	5.5%	4.5%	.5%	30	1
DATING	--	--	--	--	--	--	--	--	--	2.5%	1.25%	.5%	13	.25
CRAIGSLIST	--	--	--	--	--	--	--	--	--	2.5%	1.5%	.5%	14	.25
TEXTING	--	--	--	--	--	--	--	--	--	2.5%	4.5%	7.25%	42	1.25
GAMING	--	--	--	--	--	--	--	--	--	2.5%	.25%	2.5%	16	.5
OTHER**	7%	16.5%	11%	16%	16%	20.5%	38%	31%	22%	8%	8.75%	16.5%	538	16

*Includes Message boards, groups, usenet

**Includes auctions, blogs, Youtube, Twitter, hacking, mailing list, Juicy Campus, Ripoff Reports, keyloggers/virus, Formspring, Topix, Skype, Ustream, Yelp, ED)

DID IT ESCALATE ONLINE?*	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	TOTAL	%
YES	N/A	39.4%	34%	62.5%	40.5%	60%	44%	55%	71%	66%	79%	80%	2043	60.25
NO	N/A	60.6%	66%	37.5%	59.5%	40%	56%	45%	29%	34%	21%	20%	1350	39.75
OFFLINE THREATS?*														
YES	N/A	35.9%	34%	38%	40.5%	22%	22%	24%	25%	16.5%	26%	7%	731	21.5
NO	N/A	64.1%	66%	62%	59.5%	78%	78%	76%	75%	83.5%	74%	93%	2004	78.5
DID VICTIM REPORT IT?*														
YES	N/A	81.7%	78%	66.5%	66%	59.5%	72.5%	59%	70%	72%	61%	77.5%	1835	54.25
NO	N/A	18.3%	22%	33.5%	34%	40.5%	27.5%	41%	30%	28%	39%	22.5%	900	45.75

*We didn't calculate this statistic until 2001

The above presented statistics based on the 11-year research of this organization, as well as all 3393 processed cases of cyberstalking are as follows:

- as far as the gender of victims is concerned, women prevail with 72.5% compared to men (22.5%);

- as far as the gender of stalkers is concerned, 30.25% were female, 47.5% were male, 1.25% belong to the group / gang of stalkers from multiple persons of the opposite sex, and in 20% of stalking cases, the stalker is of unknown gender;

- as far as the age of victims is concerned, 0.5% are under the age of 18, 39.75% are 18-30 years old, 27.75% of the victims are 31-40 years of age, and 24.75% are above 41 years of age;

- as far as the race of victims is concerned, 70.5% were of Caucasian origin, 4.25% of Latin American origin, 4% of Asian origin, 3.5% of African-American origin, only 1% of the victims were of Native American origin, 0.25% were of Eastern-Indian origin, and in 16.5% cases, the racial origin of victims is unknown;

- as far as marital status of victims is concerned, 36% were unmarried, 25.25% were married, 9.25% were divorced, 1.5% of the victims lived separated from their spouse, and 0.75% of the victims were a widow / widower;

- as far as the relationship they had with the stalker is concerned, 49.25% of the victims stated that they were in previous relationship and 49.75% stated that they were not in any previous relationship with the stalker;

- as far as the last one is concerned, referring to the kind of connection they had with stalkers, 39.5% of the victims reported that they were their previous romantic partners, 12.5% were their friends, 6.75% were work colleagues, 16.25% were acquaintances through online networks, 2.75% of the victims reported that they knew the stalker from the school they attended, 2.25% were former friends online, while 20% were from all other types of connections;

- as far as the question about the beginning of harassment is concerned, 35.25% of the victims said they first started via email messages, 13% via instant messenger, only 3.5% were through Facebook (but this data of Facebook were analyzed for just 3 years, from 2009 to 2011, which means that there 3.5% refers to only 3 years compared to the 13% via instant messenger), 1.75% of the victims said they had been harassed by phone (these data of 1.75% are only from the period of 2008-2011);

- as far as the escalation of the harassment through online networks is concerned, 60.25% of the victims declared affirmatively while 39.75% answered negatively to this question, in 21.5% cases there were threats, and in 78.5% cases there were no threats through the online communications;

- to the question "Have you reported the harassment?", 54.25% of the victims said yes, 45.75% of them gave a negative answer, again indicating that nearly half of the victims of stalking, do not report the cases of stalking in time (data on this issue are collected from all years of the period of 2000-2011);

In order to make the representation of cyberstalking by states more visible, the same organization published the following data analyzed from 2001-2011:

Table 2: *Comparative statistics by country (2001-2011)*[40]

2001	**VICTIMS**		**HARASSERS***
CAL, NY, TEXAS	5.9%	TEXAS	5.5%
VA, FL	4.3%	NEW YORK	4.7%
MARYLAND	3.9%	CAL, IL, FL	4.3%
ILLINOIS	3.1%	MASSACHUSETTS	2.7%
MASSACHUSETTS	2.3%	ENGLAND	2.4%
2002	**VICTIMS**		**HARASSERS**
CALIFORNIA	13%	CALIFORNIA	7.5%
CANADA	5.5%	NEW YORK	4%
NEW YORK	5%	CANADA	3%
TEXAS	4%	IL, GA	2.75%
IL, GA	3.75%	MISSOURI	2.25%
2003	**VICTIMS**		**HARASSERS**
CALIFORNIA	14%	CALIFORNIA	7.5%
NEW YORK	8%	TEXAS, ENGLAND	4.5%
PENN, TX	5%	GEORGIA	3.5%
FLORIDA	4.5%	ILLINOIS, NY	3%
GEORGIA, CANADA	3.5%	MA, PENN, CANADA	2.5%

40 http://www.haltabuse.org/resources/stats/Cumulative2000-2011.pdf

2004	VICTIMS		HARASSERS
CALIFORNIA	13.5%	CALIFORNIA	11.75%
NEW YORK	7%	NEW YORK	4%
VIRGINIA	6.5%	VIRGINIA	3.5%
CANADA	5.5%	OHIO	3%
OHIO	5%	GA, IL, PA, TX	2.5%
PA, TX, MO, ENGLAND	3.5%		

2005	VICTIMS		HARASSERS*
CALIFORNIA	9%	CALIFORNIA	12%
CANADA	8%	TEXAS	5%
FLORIDA	7%	NEW YORK	5%
NEW YORK	5%	GEORGIA	3%
PENNSYLVANIA	4%	FLORIDA	3%
MICHIGAN	4%	PENNSYLVANIA	3%
OHIO	3.5%	ENGLAND	2.5%
GEORGIA	3.5%	CANADA	2.5%
VIRGINIA	3.5%	NEW JERSEY	2.5%
TEXAS	3%	OHIO	2%

2006	VICTIMS		HARASSERS
CALIFORNIA	10.5%	CALIFORNIA	7.5%
CANADA	7.5%	NEW YORK	4.5%
NEW YORK	7%	CANADA	4%
PENNSYLVANIA	5%	PENNSYLVANIA	4%
TEXAS	4.5%	TEXAS	4%
FLORIDA	4.5%	OHIO	2.5%
UNITED KINGDOM	4%	UNITED KINGDOM	2.5%
NORTH CAROLINA	4%	WASHINGTON	2.5%
WASHINGTON	4%	NORTH CAROLINA	2.5%
GEORGIA	3%	FLORIDA/GEORGIA	2.5%

2007	VICTIMS	
CALIFORNIA	9%	CALIFORNIA
NEW YORK	7%	NEW YORK
FLORIDA	5%	FLORIDA
ILLINOIS	5%	ILLINOIS
GEORGIA	4%	GEORGIA
UNITED KINGDOM	4%	TEXAS
PENNSYLVANIA	3%	CANADA/OHIO
WASHINGTON	3%	NEW JERSEY
CANADA	3%	UNITED KINGDOM
TEXAS/NEW JERSEY	3%	MARYLAND

2008	VICTIMS	
CALIFORNIA	14%	CALIFORNIA
NEW YORK	7%	NEW YORK
FLORIDA	5%	FLORIDA
TEXAS	4.5%	TEXAS
PENNSYLVANIA	4%	PENNSYLVANIA
NORTH CAROLINA	4%	NORTH CAROLINA
CANADA	3.5%	UK
MASSACHUSETTS	7%	CANADA
WASHINGTON	3%	OHIO
UK	2.5%	MASSACHUSETTS

2009	VICTIMS		HARASSERS
CALIFORNIA	13%	CALIFORNIA	9%
TEXAS	7%	TEXAS	5.5%
PENNSYLVANIA	6%	NEW YORK	4.5%
FLORIDA	6%	CANADA	3%
MARYLAND	5.5%	MARYLAND	3%
CANADA	5%	ILLINOIS	2.5%
NEW YORK	4%	MINNESOTA	2.5%
ILLINOIS	4%	NEW JERSEY	2.5%
VIRGINIA	4%	NORTH CAROLINA	2.5%
MASSACHUSETTS	2.5%	PENNSYLVANIA	2.5%

2010	VICTIMS		HARASSERS
CALIFORNIA	9.75%	TEXAS	8.5%
TEXAS	7.5%	CALIFORNIA	8%
NEW YORK	7%	NEW YORK	5.5%
FLORIDA	5.25%	CANADA	4.25%
PENNSYLVANIA	3.75%	FLORIDA	3.75%
CANADA	4%	ILLINOIS	3.5%
ARIZONA	3.75%	ENGLAND	2.75%
N. CAROLINA	3.75%	WASHINGTON	2.5%
WASHINGTON	3.75%	TENNESSEE	1.75%
MARYLAND	2.75%	PENNSYLVANIA	1.75%

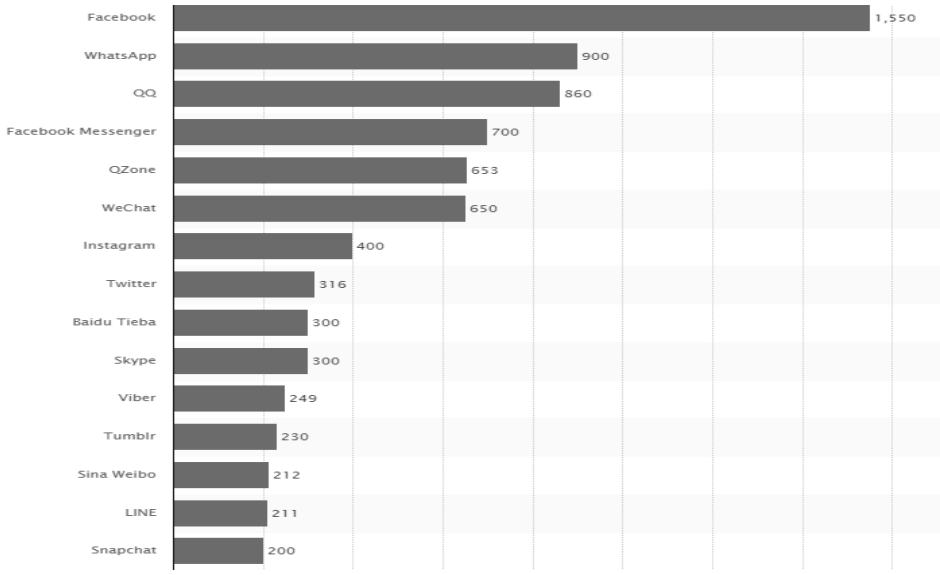
2011	VICTIMS		HARASSERS
CALIFORNIA	14.75%	CALIFORNIA	13%
TEXAS	8.5%	TEXAS	5%
FLORIDA	6.5%	PENNSYLVANIA	4%
NEW YORK	5.25%	NEW YORK	3.5%
ENGLAND	3.5%	FLORIDA	3.25%
PENNSYLVANIA	3.5%	ENGLAND	3%
N. CAROLINA	3.25%	N. CAROLINA	2.25%
WASHINGTON	2.75%	ILLINOIS	1.75%
MARYLAND	2.75%	OHIO	1.75%
VIRGINIA	2.75%	CANADA	1.75%

According to this processed information, it may be noted that the state of California has the highest rate of occurrence of victims of cyberstalking in average of 11.49% for the years 2001 to 2011. Texas, New Jersey, Virginia, Maryland, Illinois, Ohio, Tennessee, Pennsylvania, Massachusetts and others are in the group of states that recorded the lowest percentage of prevalence of cyberstalking.

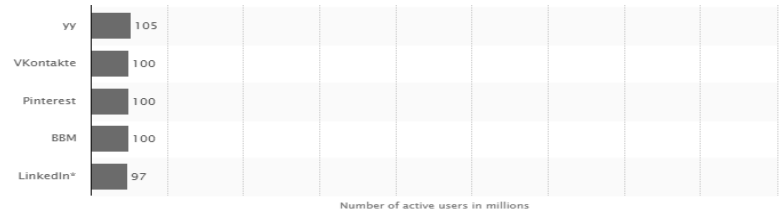
Individuals may be more vulnerable when on the Internet networks and act in a different way than they would behave in the real world. Everyone may access private information on the Internet, especially social networks, even on a daily basis. It increases the risk of many unwanted consequences. Speaking of this, it is good to mention the existence of the social network Facebook and its tool "check in" with which the user of this social network is able to check / mark exactly where someone is located at that moment. Users of this network can post photos, videos and articles. This can serve stalkers/predators to have insight on the location of their victim and his/her movement, with whom she/he hangs out and what she/he does. They can learn about the life of the victim in detail, especially if the victim is constantly active on that social network.

In 2015 Website "statista.com" ranked the leading social networks in the world for that year by the number of users:

Table 3: *View a leading social networks worldwide, ranked by the number of active users (in millions) in November 2015*[41]



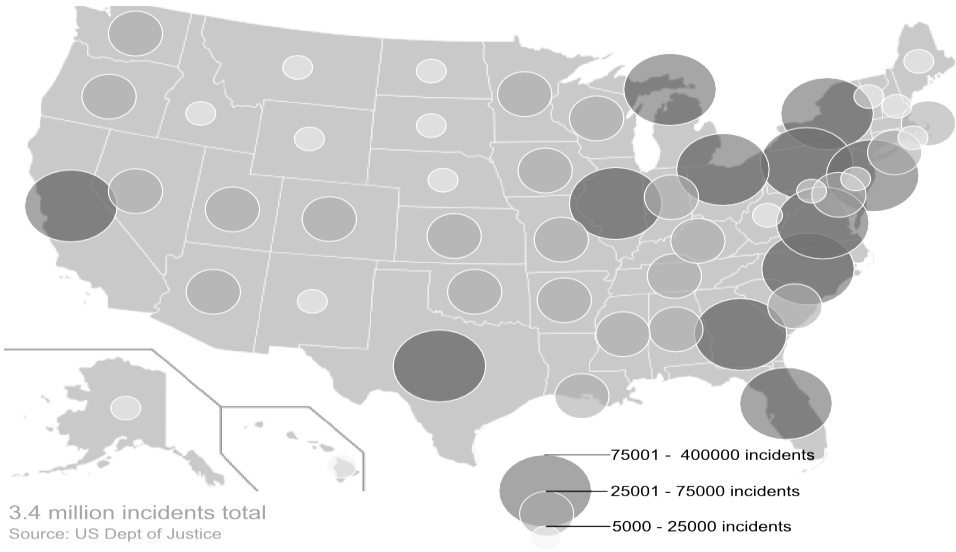
41http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/



According to this ranking, Facebook as a social network undoubtedly is in a leading position when compared with other social networks. This is a further indicator of risk in terms of cyberstalking, because in almost all cases the stalkers are orientated to find their victims through online social networks that have a large database of its users and large membership. The previously mentioned Facebook tool, "check in" can provide, if there is a case of cyberstalking which is still in the virtual world of Internet communication, a large and a real chance to be transmitted into the real world in terms that a stalker can find the victim's place of living. Thus, this cyberstalking would be transformed into a classic stalking of the victim and its cyber character would be removed.

According to Professor *Chris Piotrowski* from the University of West Florida and professor *Peter J. Lathrop*from from the Academy "Camelot" cyberstalkers tend to be highly educated, struggling with addiction to the Internet and over 16 years of age, and most of them are students. Statistics on cyberstalkers for the year 2011 marks the highest level. Around 74% of the victims were females, while 26% were males. The following picture presents how the Ministry of Justice mapped all incidents of cyberstalking for 2011:

Mapping the number of incidents of cyber-stalking for 2011 in the United States.[42]



Crime mapping is used by agencies / institutions of law enforcement and all in order to visualize and analyze the patterns of criminal incidents. Mapping crime, using Geographic Information Systems (GIS), allows crime analysts to identify crime hot spots along with other

42 https://bentj300.wordpress.com/

trends and patterns.[43]Spatial data analysis helps to analyze data and better understand why and not just where certain crime occurs.[44]

According to this mapping of number of incidents of cyberstalking for 2011, it is evident that the largest number of incidents of this type is located on the east coast of the US. The small yellow circles in the picture indicate the number of incidents of 5000-25000 cases; medium-sized orange circles indicate the number of incidents of 25001-75000 cases, while the largest circles in red indicate the number of incidents of 75001-400000 cases. According to the Ministry of Justice, the total figure for 2011 in the United States reached 3.4 million registered incidents of cyberstalking. Naturally, we should not abstract that "black statistics" because we do not know exactly how much it amounts to. If we take into consideration the survey of WHOA regarding the registration of cases of cyber-stalking, even a half of the registered victims do not promptly report the harassment to the competent authorities.

CONCLUSION

According to the statistics from the relevant institutions which are committed to the prevention and fight against stalking, we may conclude the following:

- stalking is a serious crime with annual statistics registered in the US of about 7 million victims;

- as victims of stalking by gender, women are more often represented than men;

- young people at an average of 18-24 years of age are the most endangered group of victims of stalking;

- it represents a danger for all, especially for the direct victims, regardless of gender, age, ethnic and racial background, religion;

- the developed programs to fight stalking that are implemented by government and non-governmental institutions in the United States provide some results, but the end result is still the fact that there is no progress in this crucial area in terms of prevention, data which are in favor of the thesis that these programs have a positive effect, but insufficient;

- despite the registered statistics, the "black statistics" remains which is not a part of the official research, and there is the danger of unreported cases, the exact number of which nobody knows;

- it is necessary to work on raising the general consciousness among people about the dangers of this phenomenon and its increasing incidence throughout the world.

As far as cyberstalking is concerned, we may see that stalkers "favorite" social Internet communication network in future may be Facebook, in terms of leading social network around the world because it has the largest number of users and has the richest database of personal user's data. Do not forget the tool "check in" which this social Internet network possess. As mentioned above, stalkers may use it in order to find the exact location of victims and the places where they usually go in real life.

In addition, we provide the following 5 principles / rules for protection against cyberstalking:

- do not publish your personal information and details of your private life on the Internet (real name, address, telephone number, marital status, profession / occupation, your personal Internet passwords);

- never use your real name in Internet communication;

43 https://en.wikipedia.org/wiki/Crime_mapping

44 The research of computer-based crime mapping began in 1986 when the National Institute of Justice (NIJ) funded project in cooperation with police in Chicago in addition to community policing.

- inform about the dangers of cyberstalking and modalities for broader prevention such as programs offered by governmental and non-governmental organizations;

- be very careful while communicating through the network with people who you do not know enough;

- if there is feeling of insecurity and discomfort during the Internet communication, disconnect from that Internet communication and talk elsewhere with other people.

These five principles / rules for preventing cyberstalking are in favor of the other thesis that if Internet customers continue to disclosure their private data and details of their lives through social networks, then we cannot expect positive results and suppression of cyberstalking in future. On the contrary, this trend will continue.

In case you became a victim of cyberstalking, proceed in the following order / steps:

- Step 1. Block the profile from which you have messages / calls written by the stalker. More social networks have an option to block the profiles. Facebook has this great tool, too. Mobile phones have the same option as well. Take this opportunity that technology offers you;

- Step 2. If the cyberstalker continues to disturb you and find other ways to get in touch with you, record the communication you had with that person. Never modify the content of the recorded communication; it can be used as evidence;

- Step 3. Following the second step, report the case to the nearest police station immediately. Furthermore, if you have the opportunity, report the incident to your service, telecommunications and Internet service provider.

Considering its complexity, stalking is different from sexual harassment, domestic violence, violence at workplace, voyeurism and other social phenomena. Stalking is a kind of harassment, but it does not mean that these two concepts should be used as synonyms. Although every case of stalking leads to harassment, every case of harassment does not lead to stalking. The similarity between these two phenomena is that both are systematic and continuous. Very often stalking is the result of the unsuccessful end of a relationship between a man and a woman. If so, male stalkers prevail. Millions of people are stalked in the US annually. This widespread criminal phenomenon causes social chaos among victims; they feel tremendous fear for their safety and often fear for their lives because of threats by their stalkers. The results of the non-governmental-non-profit organizations show that it is expected considering the today's lifestyle of people worldwide.

REFERENCES

1. Vesna Nikolic-Ristanovic, Marina Kovacevic-Lepojevic, Decembre2007, Stalking: concept, characteristics and social responses, TEMIDA, p.3-112
2. Meloy, J. R. &Gothard, S., 1995, Demographic and clinical comparison of obsessional followers and offenders with mental disorders. American Journal of Psychiatry
3. VidaVilić, March 2013, Stalking victimization through the Internet**,** TEMIDA, p. 151-162
4. Bocij, P., 2004, Cyberstalking: harassment in the Internet age and how to protect your family. Westport: Praeger Publications
5. Konstantinović-Vilić S. Nikolic Ristanovic, V., Kostic M. 2009, Criminology (third amended edition) Pelican Print Ltd. Stamparija, NIS Gornja Toponica, Nis
6. http://www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-laws/criminal-stalking-laws-by-state

7. Kaiser, G. 1996, Criminology, "Alexandria", Skopje,
8. From, E., 1984, A healthy society, Zagreb: Naprijed,
9. Journal of Psychiatry, 176, p. 206-209
10. Naomi Harlin Goodno, 2007, Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws,72 Mo. L. Rev.

INTERNET SOURCES

11. http://bjp.rcpsych.org/content/176/3/206
12. https://www.ncjrs.gov/pdffiles/169592.pdf
13. http://www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-laws/criminal-stalking-laws-by-state/california#646
14. http://www.victimsofcrime.org/our-programs/stalking-resource-center/stalking-laws/criminal-stalking-laws-by-state/massachusetts
15. https://www.victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0
16. http://www.victimsofcrime.org/our-programs/stalking-resource-center/about-us
17. http://www.caepv.org/getinfo/facts_stats.php?factsec=9; https://www.ncjrs.gov/pdffiles/169592.pdf;
18. http://www.caepv.org/getinfo/facts_stats.php?factsec=9
19. https://www.ncjrs.gov/pdffiles1/nij/183781.pdf; http://www.caepv.org/getinfo/facts_stats.php?factsec=9
20. http://crime.about.com/od/stats/a/stalkingstats.htm
21. http://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf
22. http://www.caepv.org/getinfo/facts_stats.php?factsec=9
23. https://www.victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0
24. http://www.caepv.org/getinfo/facts_stats.php?factsec=9
25. http://www.victimsofcrime.org/docs/default-source/src/responding-to-stalking-a-guide-for-community-correctionsaf9bf82e2c3f4f608830756c920f85ec.pdf?sfvrsn=0
26. http://www.campussafetymagazine.com/site/about_campus_safets
27. http://www.victimsofcrime.org/docs/src/stalking-fact-sheet_english.pdf
28. http://www.campussafetymagazine.com/article/Stalking-Stats; http://sites.jcu.edu/vpac/pages/stalking/stalking-statistics/
29. http://www.campussafetymagazine.com/article/Stalking-Stats; http://www.wgac.colostate.edu/stalking-statistics;
30. https://www.victimsofcrime.org/docs/default-source/src/stalking-fact-sheet-2015_eng.pdf?sfvrsn=2
31. http://www.haltabuse.org/resources/stats/index.shtml
32. http://www.haltabusektd.org/
33. http://www.haltabuse.org/resources/stats/Cumulative2000-2011.pdf
34. http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

35. https://bentj300.wordpress.com/
36. https://en.wikipedia.org/wiki/Crime_mapping
37. http://www.doiserbia.nb.rs/img/doi/1450-6637/2007/1450-66370704003N.pdf
38. http://www.sitel.com.mk/manijakot-koj-ja-progonuval-rijana-se-pojavi-pred-sudot
39. http://vistina.mk/2014/07/30/zapochna-suden-eto-protiv-manijakot-koj-ja-progonuval-rijana-sudijata-ne-znae-koja-e/
40. http://popara.mk/2011/zabava/soubiz/nicole-kidman-ja-raskazha-prikaznata-za-chovekot-koj-so-godini-ja-progonuval/
41. http://brkajrabota.mk/lifestyle/zivot/937-ja-progonuval-jenifer-anton-za-da-ja-ozeni-zatoa-sto-se-povrzani
42. http://daily.mk/zabava/uapseno-momche-opsednato-so-djenifer-aniston
43. http://www.telegraf.rs/vesti/1532730-goran-je-danima-pratio-i-proganjao-slavicu-najnoviji-detalji-krvavog-ubistva-i-samoubistva-u-centru-beograda
44. http://www.telegraf.rs/vesti/1531919-jezive-scene-u-centru-beograda-iznose-tela-ubice-i-konobarice-koja-je-usmrcena-s-cetiri-metka-foto-video
45. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/157898/consultation.pdf
46. https://www.stalkingriskprofile.com/what-is-stalking/stalking-legislation/international-legislation
47. http://www.victimsofcrime.org/docs/default-source/src/safe-haven-guide---stalking.pdf?sfvrsn=4
48. http://scholarship.law.missouri.edu/mlr/vol72/iss1/7

UDC: 004.738.5:621.39-182.3
343.533::004

MOBILE INTERNET CRIME AND ITS PREVENTIVE MEASURES

Qiang Fan[1]
National Police University of China,
Network Information Center, Shenyang

Abstract: With the development of wireless access technologies such as 4G and WiFi, and the popularity of smart phones, mobile Internet is changing the way of working and living. Mobile Internet brings convenience and efficiency to people, at the same time it provides new crime methods to the criminals. This paper introduces the concept of mobile Internet crime, summarizes the characteristics of mobile Internet crime, analyzes the form of mobile Internet crime, and puts forward some measures to prevent mobile Internet crime.

Keywords: mobile Internet; Internet crime; Internet security

INTRODUCTION

Internet is very popular in China nowadays. With the coverage of 4G network, by using the smart phones, tablet computers and other kinds of terminals to achieve the transmission of variety information, Internet has become a living way of modern people. From the cable to the mobile, the rapid development of the Internet has brought us more and more problems. Virus trojan, virtual property disputes, Internet financial fraud, phishing and other events constantly appear. According to the relevant statistical data, the current network crime is in the transition period, the target of network crime turns from the wired network to the mobile network, the new type of intelligent attack means continues to emerge, and the Internet crime is also changing in terms of type, form, quantity and so on.

THE CONCEPT AND CHARACTERISTICS OF MOBILE INTERNET CRIME

The concept of mobile Internet crime

To the understanding of mobile Internet crime, different scholars give their different definitions from different view. However, there is no authoritative definition at home or abroad. The present theoretical research gives the generalized concept of mobile Internet crime. That is all the cell phone-related criminal activities and bad behaviors. Some scholars consider that mobile Internet crime takes smart phones, tablet PCs and other mobile network terminals as the main crime tool, makes use of network communication function, network transmission function and other functions to commit illegal activities and behavior which harm society.[2]

1 58092638@qq.com
2 Wang Dawei, Yu Hongmei. A Preliminary Study on the Crime of Mobile Phones in China [J]. Journal of Chinese People's Public Security University, 2004, (03): 116-119.

The former concept focuses on using mobile phones to sending text messages, MMS and other ways to commit criminal activities; the latter concept focuses more on using mobile network terminal (smart phones, tablet PCs) to commit criminal activities on the Internet.

Characteristics of mobile Internet crime

The lower age and diversification of the criminal subject: Criminals involved in solved mobile Internet crime cases are very young, some of them are even school students, and they are becoming younger and younger. Young people easily accept new things. However, because of the lack of experience, they are easy to accept bad influence and to take part in crime. At the same time, the criminal subjects are not limited to be computer professionals, but from all walks of life. A criminal subject is diversified and complicated.

The criminal cost is low and the criminal tools are simple. Compared to the traditional crime, mobile Internet crime has the feature of small risk and large benefit, and its criminal tools are very simple, as long as an intelligent terminal (such as mobile phone, tablet PCs) and a network card is OK. As long as the criminals gently press a few keyboards, they can make the victims suffer huge losses.

Be cross regional and covert: Due to the characteristics of the mobile Internet openness, uncertainty, beyond time and space, the criminals need not face the victim, and the crime is often cross region. They usually plan a crime in a city A, commit a crime in a city B, and withdrawals in a city C, which makes the crime a strong concealment and increases the difficulty of crime detection.

THE MANIFESTATION PATTERN OF MOBILE INTERNET CRIME

Fraud crime by using mobile Internet to send mass SMS

Fraud crime by using mobile Internet to send mass SMS is the behavior when criminals fabricate non-existent facts or exaggerated facts and send the message to victims through smart phones, tablet PCs and other mobile Internet tools. They simulate the relatives' or acquaintances' phone numbers to make the victims believe that the message is in order thus cheating the victims' properties. The common methods of this kind of crime includes various designs of winning a prize in a lottery to lure victims to commit fraud, posing as an acquaintance to send text messages to ask for help to commit fraud, lying that their relatives have suffered from traffic accidents or kidnapping to commit fraud, pretending enrollment, recruitment, marriage to commit fraud, and selling low-priced smuggled goods to commit fraud, and so on.

Spreading pornographic information crime by using mobile Internet

The Internet function of smart phones, tablet PCs has matured, and the suspects of spreading pornographic information have found a new medium of communication from the Internet. Compared with the traditional obscene crime, smart phones, tablet PCs have the advantages of small volume, they are easy to carry, usually with a high-definition camera, supporting both audio and video transmission of computer communications and all kinds of obscene information; the capacity is small, the upload, browse or download of the pornographic information can be spread rapidly in the modern mobile terminals. Therefore, the activity and transaction mode of mobile Internet pornography crime completely breaks through the restrictions of time and space. And it can receive pornographic information or complete the transaction at any time and any place.

Spreading network virus crime by using smart phones and tablet PCs

The virus principle of smart phones and tablet PCs is the same as the one referring to computers, which is a kind of contagious and destructive procedure. The viruses can spread by the means of MMS, e-mail, web browsing, software downloads and Bluetooth transmission, causing the user crashes, shutdown, sending out spam e-mails, disclosure of personal information, automatic dialing a phone, SMS or MMS, and so on. Viruses can even damage the motherboard, chips and other hardware, so that users cannot normally use their devices. When the smart phones and tablet PCs get virus infection, the obvious performance is that the mobile tools run slow and often crash or have white screen phenomenon, the tools battery have serious consumption and they even automatically bulk SMS according to the mobile phone communication book, and reveal the user's privacy.

Financial crime by using mobile Internet

With the wide use of the mobile Internet technology in financial business activities, the prelude of the financial electronic has opened, and the consequences greatly promote the financial activities of automation and convenience, promote the great changes in the financial sector. However, it also causes the mobile Internet financial crime phenomenon. The crime is different from the traditional property infringement crime, which makes the Criminal Law face a huge challenge. Mobile Internet financial crime is a new type of crime in the background of the high development of modern network information technology.[3] Mobile Internet changes the way of people's life, at the same time, mobile Internet financial crime is also emerging endlessly. Mobile Internet financial crime has become one of the most important mobile Internet crimes with more than 20% annual growth rate.

PREVENTIVE MEASURES OF MOBILE INTERNET CRIME

To perfect legislation and strengthen international cooperation

Mobile Internet crime has caused a huge concern all around the world and is becoming a big problem that all countries should face together. More and more countries have added the terms of Internet crime in the laws and regulations. China lacks a sound legal system of Internet crime and the operability of relevant laws is not strong enough. Therefore, it is difficult to form a real system to fight and prevent mobile Internet crime. On one hand, we should strengthen the mobile Internet crime legislation and improve the network of the criminal justice system, in order to more closely fight against Internet crimes. And on the other hand, we should strengthen international exchanges and cooperation and establish the world legal cooperation mechanism to deal with the mobile Internet crime.[4] The transnational nature of mobile Internet crime requires that national legislation should pay attention to the international practice and joint, thereby enhancing the control of mobile Internet crime, and effectively preventing mobile Internet crime.

To introduce big data technology to strengthen governance

The development of big data technology has brought new ideas and means for mobile Internet crime management. Big data technology covers data fusion technology, data processing

3 Mao Dehua. The Means, Causes, Characteristics and Prevention of the Crime of SMS Fraud [J]. Journal of Railway Police College, 2004, (01): 75-78.
4 Chen Jiemiao, Zhang Yue. On the Improvement of the Legislation of China's Internet Crime [J]. Anhui University law review.2007, (01):210-219.

technology, information mining technology, and so on.[5] Take data fusion technology as an example, it integrates massive data such as search data, social data, logistics data and the public security business system, to screen abnormality, discover the suspect's network activity trajectory and investigate and solve the case by network DNA. Aiming at the phenomenon of difficult governance of mobile Internet crime in micro domino, and by using big data mining technology, we can take theme modeling, word frequency analysis and correlation analysis to the relevant information and status data in order to discover the potential mobile Internet crime.

To implement real name registration

With the embodiment of the application effect of various real name systems, we recognize that the fight against mobile Internet crime should start from the source. The reason that criminals rampantly obtain a lot of phone cards and network cards is because registration of real name system implementation of China's mobile phone cards and network cards is not in place. If the users' ID cards are required and examined carefully to open accounts when the users purchase phone cards and network cards, then this control of the mobile terminal will become one of the effective management measures to reduce mobile Internet crime.[6]

To strengthen the supervision of the mobile Internet industry chain

In the mobile Internet industry chain of ecological system, the telecommunication operators, mobile phones manufacturers, Internet companies and application service providers are in the core position. However, many equipment manufacturers, network service providers, research and design enterprises and software developers are in the downstream of the industry chain. At the same time, media, finance, electricity, education, health care, transportation and other industries have also joined, making the number of departments that are associated with mobile Internet increase, and it is difficult to clarify the boundaries of responsibilities. Therefore, we need to strengthen supervision, establish and improve the long-term monitoring mechanism, standardize the management process, strengthen the regulatory team and filter the bad information, software and function in time.

To improve the security awareness of mobile terminal users

We should strengthen the security awareness and technical support for the users of smart phones, tablet PCs and other mobile terminal, develop and install powerful anti-virus software of smart phones, tablet PCs. Individual users should develop good security habits such as off Bluetooth when not using, not opening strange MMS, not casually receiving micro channel, thus avoiding the use of the mobile Internet to bring their own major losses.

CONCLUSION

Mobile Internet crime is a new type of crime which appears with the development of science and technology, and it has become one of the most serious factors affecting the stability of the current society. At present, the laws and regulations, network security technology, and investigation measures related to mobile Internet crime are lagging behind. Therefore, there is a lot of work to do in order to reduce the incidence of mobile Internet crime. We should make mobile Internet play a positive role in the survival and development of human beings, improve the mechanism to combat mobile Internet crime in all aspects, and ensure the healthy development of the mobile Internet.

5 Zhang Chunyan. Public Security Governance in the Era of Big Data [J]. Journal of National School of Administration, 2014, (05): 100-104.
6 Han Hua, Liu Bing, Han Zhu. Analysis on the Phenomenon of Cellphone Crime and its Countermeasures [J]. Journal of Jiangxi Police Academy, 2007, (01): 68-70.

REFERENCES

1. Chen Jiemiao, Zhang Yue. On the Improvement of the Legislation of China's Internet Crime [J]. Anhui University law review.2007, (01):210-219.
2. Han Hua, Liu Bing, Han Zhu. Analysis on the Phenomenon of Cell Phone Crime and its Countermeasures [J]. Journal of Jiangxi Police Academy, 2007, (01): 68-70.
3. Mao Dehua. The Means, Causes, Characteristics and Prevention of the Crime of SMS Fraud [J]. Journal of Railway Police College, 2004, (01): 75-78.
4. Wang Dawei, Yu Hongmei. A Preliminary Study on the Crime of Mobile Phones in China [J]. Journal of Chinese People's Public Security University, 2004, (03): 116-119.
5. Zhang Chunyan. Public Security Governance in the Era of Big Data [J]. Journal of National School of Administration, 2014, (05): 100-104.

UDC: 004.738.5:316.624
343.85:343.542.1

STUDY ON NETWORK PORNOGRAPHY CRIME INVESTIGATION AND PREVENTION MEASURES

Hao Liu, MA[1]
National Police University of China, Shenyang

Abstract: With the continuous development of computer network technology and the popularization of mobile internet technology, network pornography crime runs rampant and causes severe harm to the society. It becomes an important task of public security organizations to effectively fight against and prevent this special form of crime at present. In this paper, by introducing the concept of network pornography crime, forms and characteristics of network pornography crime are summarized, and then investigation methods and prevention measures are proposed.

Keywords: network, pornography crime, investigation, prevention.

INTRODUCTION

Originating from Greek, the word pornography refers to the text or artwork describing the life of prostitutes. The concept of "pornography" is not explicitly stipulated in China's laws. Network pornography means the behaviour of making, selling and spreading pornographic information through the Internet. Network pornography crime refers to the behaviour of making, copying, selling and spreading obscene and pornographic information through the Internet for the purpose of profit or the severe behaviour of spreading obscene and pornographic information not for the purpose of profit, or the criminal behaviour of inducing, organizing and introducing prostitution.

CHARACTERISTICS OF NETWORK PORNOGRAPHY CRIME

High Elusiveness of Criminal Behaviour

As a new criminal type, network pornography crime possesses high elusiveness. Network pornography crime is completed by operating the computer network server. The doer can realize automatic spreading through the computer network by uploading pornographic information to the server, and the fund is often paid via online payment or short message payment. There is no need to have direct contact in real life.[2]

Low Crime Cost and High Benefit

In the fictitious network world, a pornographic image or a pornographic video can be reproduced into countless copies and spread across the whole Internet in quite a short time. Meanwhile, criminal offenders can obtain huge economic benefit by utilizing the quick payment mode and ubiquitous internet.

1 Email: liuhao8142@126.com
2 BI Yantao: "Control Measures for Network Pornography in Various Countries", Netinfo Security, the 8th issue of 2007.

Trans-Regional Nature

Different from other traditional crimes, network pornography crime won't be restricted by regions. As long as there is a computer connected to the Internet, the criminal is able to commit a crime and to reach the criminal purpose no matter where the criminal lives.

Interactivity

Users can download pornographic images according to their own taste, and spread the images through personal websites. Users with the same hobby can form a fictitious community easily. Based on the interactivity of network, pornographic information will be transferred to the network from all directions continuously.

EXPRESSION FORMS OF NETWORK PORNOGRAPHY

Network pornography shares some similarities with traditional pornography, and meanwhile it also has its own characteristics. Its major expression forms are as follows.

Pornographic Image

Pornographic image is the most widespread in the network, and it is also a type that can be obtained easily. Websites or users will upload and provide obscene and pornographic images, and other users can browse or download these images. The image formats include BMP, GIF, JPEG, PNG, etc.

Pornographic Text

The contents of pornographic text are almost the same with pornographic novels in reality, and the only difference lies in the media of presenting them. Pornographic text can often be seen on BBS or websites, and it can be directly browsed or downloaded.

Pornographic Video

The formats of pornographic video include MOV, MPG, AVI, RMVB, DAT, etc. Compared to pornographic image and text, pornographic video is more intuitional, barefaced and stimulating. Most pornographic websites provide online broadcasting or downloading services of pornographic video.

Network Pornography Interaction

Network pornography interaction has multiple forms, and typical ones include network pornography chat, network pornography video and network pornography game.

Pornographic Transaction through the Network

Due to the convenience of network, network transaction becomes increasingly popularized. Pornographic service providers directly conduct pornographic businesses on the Internet by utilizing the convenience of network.

Network Pornography Agent

As the sex medium and communication channel not involving pecuniary exchange, it will provide various kinds of information, covering one-night stand, looking for sex partners, collective pornographic travel, and sex partner exchange.

INVESTIGATION METHODS OF NETWORK PORNOGRAPHY CRIME CASES

Investigating the Crime Scenes and Collecting and Analysing Electronic Evidences

Network pornography crime stretches across physical and virtual spaces at the same time. It covers both tangible scenes (such as machine room and terminal room) and invisible scenes (information scenes, such as network space). After clues of network pornography crime are discovered, the crime scenes should be investigated as long as the conditions are met, and measures must be taken immediately to collect and analyse electronic evidences. In order to collect electronic evidences in network pornography crime cases, public security organizations can search the criminal suspect's computer system, computer room, storing area of original computer data, and other places related to the network pornography crime; moreover, they can detain related electronic data carriers. [3]

Analysing the Cases and Determining Temptation Investigation Strategies of Network Pornography Crime

Temptation investigation is one of the effective measures for public security organizations to uncover tough cases like network pornography crime. It means that the investigators disguise themselves as consumers to secretly obtain evidence through investigation at the initial stage of discovering the network pornography crime case. Investigators will enter the pornographic website and disguise themselves as consumers by applying temptation investigation means, so as to obtain trust from the webmaster and to acquire criminal evidence.

Tracing and Seeking Criminal Suspects through Monitors

Network pornography information will produce digital information in the spreading, copying and transaction process, including registration information of the pornographic website when registering the network domain name, IP address, records of accessing the server, and so on. Investigators can conduct monitoring and tracing by applying technological means, so as to know the identities of criminal suspects.

Arresting and Interrogating Criminal Suspects

After knowing relevant situations about the organizer and disseminators of network pornography crime, public security organizations in different places should take actions at the same time, so as to arrest all criminal suspects. The process of criminal behaviour can be known, and the correctness and reliability of criminal evidence can be verified by interrogating the criminal suspects. Besides, criminal clues not grasped by the public security organizations can be excavated, and the whole network pornography crime chain will be uncovered.

PREVENTION MEASURES OF NETWORK PORNOGRAPHY CRIME

The social cancer of network pornography has contaminated the whole network environment, and network pornography becomes widespread in the whole world by stepping over time and space. Nowadays, network has already become the first channel for people to

3 "On Collection of Criminal Electronic Evidences", http://www.lawtime.cn/info/shangwu/dzzj/20081116128.htm1, access time: 25 October 2012.

acquire pornographic information. Faced with such severe situation, comprehensive prevention measures should be adopted by referring to advanced experience and lessons in foreign countries and combining with domestic situations. Besides, the work in various aspects must be strengthened, so as to effectively prevent network pornography crime.

Perfecting Relevant Laws and Regulations

The Articles of China's criminal laws do not list out network pornography crime independently. Network pornography crime is a criminal behaviour to implement traditional crime by utilizing the computer network; network pornography crime should be listed out independently and brought into computer crimes. Laws and regulations of classifying network contents should be formulated. At present, most adult websites have no marks in China. Some adult websites will hint "no admittance for people under 18" before one enters them. However, no other measures are taken to stop an underage person from entering the websites. Such mark is just an empty slogan, and it does not play a positive role in network management. Therefore, laws should be formulated to restrain illegal behaviours.[4]

Strengthening Network Management

Firstly, government regulation should be intensified. China has adopted a series of measures to attack network pornography crime. For instance, information network security alarming website is set up, bad information reporting hotline is established, and reporting people are awarded. Besides, online cops are arranged to monitor the network at any time. There are more than 10 functional departments involving Internet management in China. However, these functional departments cross each other, their responsibilities are unclear, and the internal friction is severe. Therefore, special agencies should be established and the supervision for network must be increased in China by referring to overseas experience and combining with domestic situations.

Secondly, relevant management about website operation should be strengthened, and the living space of pornographic websites must be blocked. China should further intensify management for mobile operators, clarify safety responsibilities of mobile operators and information service providers that cooperate with them, and increase the punishment force, so as to create a green and healthy network environment.

Thirdly, self-regulation of the industry should be enhanced. In order to guarantee sound development of Internet in China, the Internet Society of China issued *Standard on Forbidding Spreading of Bad Information Involving Obscenity and Pornography on the Internet* in 2004, and this self-regulation standard has set up a barrier for spreading of network pornography crime. In addition, the Internet Society of China needs to formulate a self-regulation convention of Internet industry. Positive publicity should be highlighted, and website operators must be positively guided and organized to sign this convention. Executing agencies of self-regulation standard should be established, behaviours of violating the self-regulation convention must be disposed, and spreading of network pornography information should be effectively contained through self-discipline, self-management, self-education and mutual supervision.

Strengthening Technical Control

In order to effectively control network pornography information, some technological means must be adopted. Firstly, technology fire wall should be established to intercept overseas pornographic websites. China needs to strengthen research and development for core technology of information security, and to set up a technology fire wall developed by Chi-

4 Wang Daochun: "Discussion on Characters of Chinese Sexy Crime through Internet and Countermeasures of Improvement and Precaution", Journal of Shanghai Public Security Academy, the 3rd issue of 2005.

na independently. Secondly, network real name system should be implemented. In China, network real name system must be carried out, so as to clear the network where good and evil people are mixed up, and to effectively attack and prevent network pornography crime. Thirdly, special anti-pornography technology software should be installed to filter network pornography information. Pornographic websites can appear on the network only after gaining approval from network content service providers and network access service providers. Special anti-pornography technology software should be installed on the servers of network content service providers and network access service providers as gateway. In this way, network pornography information can be filtered.

Strengthening International Cooperation

As for why network becomes the hotbed for pornographic information, the borderless nature of network is one of the important reasons. This decides that the attack against network pornography crime should be completed by relying on international cooperation rather than depending on the effort of one country. When technical defence is strengthened, international cooperation should be conducted positively, and more bilateral or multilateral agreements and treaties can be signed with other countries. When conditions become mature, consistence should be reached with other countries in criminal legislation and judicial field of network pornography crime. This will help China fight against network pornography crime in virtue of the international judicial power.

CONCLUSION

As the product from development and application of network technology, network pornography is a new crime form produced with the continuous development of network. Investigation organizations should improve investigators' quality by referring to the experience of detecting traditional pornography crime cases and directing at characteristics of network pornography crime. Besides, the relationship and cooperation between network operators and banks must be reinforced. Meanwhile, a comprehensive system of attacking and preventing network pornography crime should be formed by relying on the force of extensive netizens and social organizations, so as to fight against network pornography crime more effectively.

REFERENCES

1. BI Yantao: "Control Measures for Network Pornography in Various Countries", Netinfo Security, the 8th issue of 2007.
2. "On Collection of Criminal Electronic Evidences", http://www.lawtime.cn/info/shangwu/dzzj/20081116128.htm1, access time: 25 Oct. 2012.
3. WANG Daochun: "Discussion on Characters of Chinese Sexy Crime through Internet and Countermeasures of Improvement and Precaution", Journal of Shanghai Public Security Academy, the 3rd issue of 2005.

UDC: 343.85:343.37(510)
343.85:343.53(510)
343.533::004(510)

A RESEARCH ON CHINA'S ECONOMIC CRIME PREVENTION AND CONTROL MECHANISM IN THE INTERNET ERA

Liu Dan, PhD[1]
National Police University of China,
Department of Economic Crime Investigation, Shenyang

Abstract: In the era of mobile internet and extensive data, recent cybercrimes of disrupting the order of market economy have the characteristics of informatization of crime means, networking of crime tools, internationalization of crime, industry of crime pattern, and electronic transactions involving crime funds in China. China's economic crime prevention and control is facing increasingly severe ordeal and new challenges. It is important to research on economic crime prevention and control mechanism in the Internet era to maintain economic security of the Internet, to create a safe network environment, and to enhance the level of public services. The network economic crime prevention mechanism includes the supervision mechanism, cooperation mechanism, social mobilization mechanism and other operating mechanisms in China. At the same time, the organization's leadership mechanism, planning mechanism, evaluation mechanisms and other security mechanisms are included. The improvement governance mechanism of economic crimes includes the mechanism of information collection, analyzing, coordination, decision-making under emergency situation, case investigation, releasing information, governance evaluation and other governance mechanisms in China.

Keywords: economic crimes, Internet era, prevention, governance, mechanism

INTRODUCTION

Cybercrimes of disrupting the order of market economy in China refer to behaviors that violate the laws and regulations of Chinese market economy and disrupt the socialist market economic order and seriously harm the development of the market economy based on information network. It is important to research on economic crime prevention and control mechanism in the Internet era to maintain the economic security of the Internet, to create a safe network environment, and to enhance the level of public services.

CHARACTERISTICS OF CYBERCRIMES OF DISRUPTING THE ORDER OF MARKET ECONOMY IN CHINA

After the application of computer network to Chinese commerce, network marketing and network trade, Internet banking and other Internet economy was booming. Accompanied by the development trend of China's online shopping market popularization and globalization and mobility, confrontation between the third-party online payment and bank card payment coexists in the field of mobile Internet, and the rapid development of all kinds of Internet

1 Corresponding author: E-mail: sunshine_dan@126.com.

applications. When the Internet provides unprecedented convenience for people and where people's dependence degree on the Internet is higher and higher, a large number of the factors that induce economic crimes are present. In the era of mobile Internet and extensive data, recent cybercrimes of disrupting the order of market economy have the characteristics of informatization of crime means, networking of crime tools, internationalization of crime, industry of crime pattern and electronic manipulation of crime funds in China. Economic crime prevention and control of China in the Internet era is facing a more severe test and new challenges.

Firstly, the means of cybercrimes of disrupting the order of market economy have become more intelligent. Compared with the traditional economic crime, the typical features of the means of network economic crime are more technical, professional and highly intelligent. Despite the increasing efforts of China's public security organs to combat network economic crime and to enhance the web public awareness of prevention, the new techniques of network economic crimes merged. For example, criminals disguised as a regular bank website or regular third-party payment site or utilized bulk short message service device or voice over internet protocol network phone to cheat others' credit card accounts and passwords and use their credit cards[2]. Through third-party payment platform, investors' funds are directly remitted to the net loan company or individual account, and then the net loan company transfers the funds to the financing side. Because of the back-to-back transaction between investors and financing sides, the net loan company easily evolved from the original intermediary into shadow banking and intercepted the investors' funds to form cash-pooling.

Secondly, the representation of cybercrimes of disrupting the order of market economy has been diversified. The criminals are in collusion with each other to provide convenience of committing the crimes of producing and marketing fake or substandard commodities, infringing on intellectual property rights, falsely making out special invoices for value-added tax, pyramid selling, illegal operating, illegally taking in deposits from the general public, unlawfully raising funds, defrauding by means of credit cards, defrauding money or property during the course of signing or fulfilling a contract, defrauding insurance money and defrauding by means of financial bills based on information network and so on. In 2012, the Ministry of public security of the People's Republic of China carried out a detection operation, launching an all-out attack on all kinds of economic crimes. During the detection process, 799 operations were carried out, involving the use of network technology that the Ministry of public security deployed and the economic crime investigation bureau of the Ministry of public security supervised. Public security organs of the involved region respectively filed the cases, many public security organs took joint action and completed their investigations and destroyed the entire crime network.

Thirdly the perpetration of cybercrimes of disrupting the order of market economy has become increasingly concealed. Due to the network nature of virtual reality and openness beyond time and space, China's network economic crime has a feature of high concealment. With the aid of a virtual network platform, criminal gang members carried out clearly different criminal activities and individually contacted real-time through the network. By modifying the internet protocol address and other technical means, some criminals provided false web sites and hid their identity. Through the network or telephone remote operation, some criminals set up the web server outside and committed the crimes. Through repeated anonymous login, some criminals went straight to the target of the crime in the process of receiving the network information. Having designed the computer program of intrusion, some criminals touched the

2 Lang Jun-yi. On the criminal risk and prevention and control measures of the three-party payment under the view of internet finance, Taking the crime of bank card as the angle of view. Public Security Science Journal, 2014(6), pp. 30.

keyboard and then committed the crimes at any moment on any computer. After committing the crime some criminals promptly destroyed the records stored on the computer and even system log records on the server in a timely manner.

Fourthly, the social harm of cybercrimes of disrupting the order of market economy has become more serious. In recent years, with serious harm to the people and property security, national economic security and social harmony and stability, network economic crimes increased significantly and major cases frequently happened, involved numerous objects and victims of crime throughout every province in China, and criminals can easily broke through the geographical restrictions. For example, in 2013, the Ministry of public security decided to carry out a special action against illegally produced medicines and marketing fake commodities. It organized the public security organs of 29 provinces and autonomous regions of China to carry out 3 centralized detection actions, and destroyed more than 400 criminal gangs, involving the amount of 220 million RMB, shut down more than 140 illegal websites and web shops, arrested more than 1300 suspects[3]. To give another example, on the pretext of electronic commerce of the direct-purchase official net, some criminals in Jiangxi province developed more than 120 thousand distributors and more than 6700 thousands ordinary members and carried out pyramid selling involving the amount of 640 million RMB by the means of charging entry fee[4].

Fifthly, the area of cybercrimes of disrupting the order of market economy has become more trans-regional due to internationalization. Because of the network characteristics of connectivity, international and trans-regional, beyond original regional and inter regional boundaries, the network economy crime in China presents the international trend. For example, in 2014 the Ministry of public security deployed public security organs of Guangxi, Guangdong, Fujian province, successfully cracked a major case of manufacturing and selling fake world cup team jerseys, seized more than 150 thousand sets of different kinds of counterfeit sports clothing, and involved the amount of more than 30 million RMB. These fake jerseys eventually flowed into many clothing market stores or online shops and terminal retail links, and some were even exported to Africa and Central Asia and other countries and regions[5]. The crime did not only directly damage the consumers' legitimate rights and interests, but also seriously affected China's international reputation.

OPERATING MECHANISM OF CHINA'S NETWORK ECONOMIC CRIME PREVENTION AND CONTROL

China's economic crime prevention and control is faced with more severe ordeal and new challenges. Operating mechanism are in the process of devising a way to exert the special forces of public security, mobilize all kinds of organizations and the masses of the society, stimulate the active power and restrain the negative forces. The operating mechanism of China's network economic crime prevention and control includes the supervision mechanism, cooperation mechanism, social mobilization mechanism and other operating mechanisms. The operating mechanism has the characteristics of diversity, flexibility and operability.

3 Ten major economic crime cases announced in 2013. http://cpn.cpd.com.cn/n17159841/c21550094/content.html.
4 Ten golden cases on the system of China's economic crime investigation in 2013. http://www.cpd.com.cn/epaper/rmgab /2013-11-28/05b-1.html.
5 The ministry of public security successfully commanded to crack a major case of manufacturing and selling fake world cup team jersey. http://www.gov.cn/xinwen/2014-07/01/content_2710456.html.

Supervision mechanism refers to the process and way to comprehensively supervise all aspects and total process of China's network economic crime prevention and control that includes the work in striking, educating, managing, constructing, reforming and so on. The supervision mechanism is an important guarantee of widening the clue to network economic crime cases, improving the detection rate of criminal cases, playing the role of penalty deterrent and ensuring judicial justice. The supervision is required to do a good job in the supervision of the masses and supervision of public opinion and judicial supervision. Firstly, it is necessary to widely publish the telephone hotline number for reporting network economic crimes, to stipulate the procedures for accepting and handling report clues to verify the criminal intelligence, to obtain the clear case clues, to examine the actual situation and sources for a certain range of people one by one, to analyze, research, judge evaluate, realize reward cash, implement incentive measures, encourage the masses to expose crime clues and compress living space of network economic crimes. Secondly, it seeks to increase the supervision strength in coordinating and guiding the investigation of major cases of network economic crimes in key areas, seize the important clues of major cases of network economic crimes, trace them back to their source, and destroy the gangs and crime dens. Thirdly, they are to invite reporters to the criminal scene to track the typical cases of network economic crimes, and expose new techniques and trends of economic crimes. Lastly, they should openly hear the network economic crime major cases and announce the verdict, and thus ensure a deterrent effect of Criminal Law.

Collaboration mechanism refers to the process and way to carry out the duties of related departments and institutions between China and foreign countries, cooperate on network economic crime prevention and investigation and control. Firstly, break the shackles of fighting the enemy separately and the boundaries of countries, regions and departments. Secondly, cooperate in the releasing criminal information, researching legal qualitative opinions and preventive measures, constructing propaganda network on preventing and controlling the economic crimes, arresting criminal suspects and so on. A professional network economic crime information collection mechanism should be established. Expand the source of information of network economic crimes, establish national network economic crime information collection system, organize and coordinate the activities of information exchange in the whole country. The above criminal information mainly includes the facts and details from the public security organs, the standing committee of the people's congress, the publicity department, the government office, the courts, the security department, the foreign affairs section, the development and reform commission, the education department, the financial section, the railway department, the transportation department, the civil aviation department, the industry information department, the business department, the culture department, the industrial and commercial department, the administration of press, publication, radio, film and television, the banking regulatory commission, the administration of customs, the taxation administration, the administration of quality supervision inspection quarantine, the food and drug administration, the administration of foreign exchange, the human resources and social security, the telecommunication company, China post and related departments and social organizations. In addition, some criminal information is from the industry associations, enterprises and the people. There are four main types of network economic crime intelligence information. The first type is the early warning information about new methods of committing network economic crimes. The second type is the information about victories: information about the of acceptance of cases, filing cases, detection, the end of investigation, suspects involved in the cases, involved institutions, involved money and property and so on. The third type includes the clue information about fugitives involved in the cases, analyses of gang members, bulletins on assistance in the investigation and so on. The fourth type is associated information about financial institutions' account information and credit system blacklist, eco-

nomic investigation into key personnel, abnormal information on commodity business platform, company registration and related information. Thirdly, carry out joint action against network economic crimes, and strengthen communication and contact with foreign police organizations, jointly organized seminars of prevention and control of the network economy crime, exchange the experience in handling cases.

Social mobilization mechanism refers to the process and way to mobilize the whole society, especially the grass roots organizations and the people, to participate in the prevention and control of network economic crimes. It is an important guarantee to enhance the awareness of the prevention and control of the people, and to improve the ability of the whole society to prevent and control network economic crimes. Firstly, people's governments at all levels and their relevant departments and all kinds of news media should provide free prevention and emergency handling propaganda of network economic crimes. Make full use of newspapers, radio, television and other news media and the internet, micro channel platform, short message service platform, select the methods of establishing network economic crime prevention and control website, or holding press conference, or issuing propaganda brochures, posters, promotional CD-ROM, or showing publicity pictures, or explaining advisory services or other popular forms. Secondly, the focus of publicity includes the provisions of criminal law and other laws and regulations about network economic crimes, the common sense of preventing and controlling and reporting network economic crimes, the economic crime victims' experience, the achievements in the special campaign and centralized government action of network economic crimes and so on. Thirdly, actively promote the propaganda network construction of prevention and control of network economic crimes covered the urban community and rural areas. Attach importance to propaganda in the key regions with a high network economic crime rate. The object of publicity mainly focuses on the social vulnerable groups easy to be infringed by the network economic crimes. Then, create a good atmosphere for the whole society to prevent and control network economy crimes.

GUARANTEE MECHANISM OF CHINA'S NETWORK ECONOMIC CRIME PREVENTION AND CONTROL

Guarantee mechanism is the process and mode of unified organization and leadership, careful planning, effective emergency treatment. Perfect guarantee mechanism provides a solid foundation for prevention and control of the network economic crime, ensures to carry out prevention and control scientifically, effectively and smoothly. Guarantee mechanism includes organization's leadership mechanism, planning mechanism, evaluation mechanisms and other security mechanisms.

Organization and leadership is the highest level of management system of prevention and control of the network economy crime, which is the determinant in the network economic crime prevention and control work. Firstly, establish a leadership system that are constituted by the central, the provincial, the city and the county (district) level, that implement comprehensive coordination, grading responsibility and regional management. Recommend for the establishment of joint conference on preventing and controlling network economic crimes under the state council, the provincial, the city and the county (district) level, that is the highest form of organization of preventing and controlling network economic crimes at the above 4 level governments. The joint conference is mainly responsible for the leadership of the state council and provincial, city and county (district) government and reflecting their work progress, putting forward some suggestions related to prevention and control work, organizing and coordinating the relevant departments to do a good job of attacking and preventing network economic

crimes, and carrying out the vocational work. According to organizations and work responsibilities of the member units, prevention and control work that includes legislative design, legal amendment, institution improvement, regulatory law enforcement, special rectification, industry regulation, law enforcement cooperation, criminal justice, publicity and education, overseas cooperation, cross-border exchanges should be determined by the joint conference.

Through formulating the scheme to prevent and control network economic crimes and response plans of network economic crimes of emergency, corresponding planning mechanism can be constructed. The prevention and control scheme refers to the plans and strategies drafted in advance to prevent and control the network economic crimes, which includes the long-term blueprint and short-term action guide. About the long-term blueprint, strategy directions, long-term goals, main steps and major measures of prevention and control of the network economic crimes should be mentioned. And the short-term action guide refers to the direction of the campaign, recent target, the specific steps and concrete measures. The program for the prevention and control of network economic crime is as followed, determining the long-term, medium-term or short-term objectives of the network economic crime prevention and control, analyzing the subjective and objective environment of the network economic crime prevention and control, analyzing the resources including human resources, financial resources, material resources, technology resources, information intelligence and so on, amending the target determined by situation change of network economic crime prevention and control, formulating and implementing strategies and tactics for prevention and control, monitoring or evaluating the suitability, adequacy, schedule, efficiency, effectiveness and impact of the schemes or plans of network economic crime prevention and control. Considering the elements of space distribution, power allocation, the use of means, measures selection in formulating the scheme of network economic crime prevention and control, six major relations should be correctly understood and properly handled. One is the relationship between macro scale and micro scale. It is not only attach importance to the prevention and control in a wide social range, but also attach importance to the key places and key personnel admonished and controlled. Two is the relationship between the current and the long-term. The current situation of network economic crime prevention and control and future development trend predicted scientifically should be considered. Three is the relationship between prevention and control of mass force and specialized power. It is not only attach importance to mobilize the masses to participate in the prevention and control network economic crimes, but also attach importance to give full play to specialized forces of the public security organs and related sectors. Four is the relationship between traditional means and high technical means. Flexible use of economic crime investigation means and research and development of high technical means would be applied to. Five is the relationship between the crackdown and lenient. Crack down on network economic crimes and educating and saving the criminals should be paid attention to. Six is the relationship between education and training. Correcting people's bad psychology and improving people's ability and skills of preventing and controlling network economic crimes should be considered. Establish the thoughts on preventing and controlling at higher stages, long-term operation, combination of mass force and specialized power, science and technology determining the outcome, temper justice with mercy and people-oriented. Fight a three-dimensional campaign, a lasting campaign, people's campaign, a high technology campaign, a most difficult campaign and a high skills campaign.

Evaluating mechanisms of preventing and controlling network economic crimes is the process and mode that is according to certain criteria, using scientific methods, examining effectiveness and efficiency of prevention and control, analyzing and evaluating value. Evaluating mechanisms is the basis for the prevention and control network economic crimes, which is the only way which must be passed to reform the organization leadership of preventing and controlling, promote making scientific planning and system and efficient operating mecha-

nism. Determining the comprehensive evaluation index system of preventing and controlling network economic crimes is the core issue of the evaluating mechanisms. Whether or not scientific and reasonable, the index system is directly related to the quality of the evaluation. In the process of establishing the comprehensive evaluation index system of preventing and controlling network economic crimes, the principles of the comprehensive, scientific, objective, operational and practical should be adhered to. For example, the total evaluation index of the comprehensive evaluation index system of early warning mechanism can be divided into four main evaluation indices, including the operating mechanism index, the guarantee mechanism index, the supervision mechanism index, early warning results and benefit and effect index. Multi level of the current comprehensive evaluation index system for preventing and controlling network economic crimes is the complete embodiment of the social system engineering of the prevention and control. Fuzzy comprehensive evaluation method should be selected as a comprehensive evaluation method for preventing and controlling of network economic crimes. Fuzzy comprehensive evaluation method combines quantitative analysis with qualitative description. Through the selection of comprehensive evaluation index and the establishment of comprehensive evaluation result set and index weight set of network economic crime early warning, use the fuzzy distribution method to the total evaluation value, and take the normalized evaluation index as the evaluation result of network economic crime early warning work.

CONCLUSION

At present, China is in a crucial period of reform and opening up and in a critical period of economic development. With the massive access of users and intelligent terminals, the development of the Internet and cloud computing and other technologies and applications, the trend of commercialization of network attacks, Internet economic security risks have become increasingly prominent[6]. Internet economic crime prevention and control is playing a more important role in the advance speculation on the development trend of network economic crimes and prevention, investigation into the network economic crimes. By capturing the network economic crime phenomena while still in the latent state and deeply analyzing the nature and law of the network economic crime prevention and suppression, we can undertake a comprehensive study on the prevention and control of network economic crimes.

In the research of Internet economic crime prevention and control, four principles should be adhered to, including the scientific nature of the guidance law of the network economy crimes, the pertinence of the characteristics and cause of the current network economic crimes, the systemic of comprehensive measures of network economic crimes which has the characteristics of a completely functional and flexible mechanism, the effectiveness of the prevention and control of harm arising from the expansion of network economic crimes. For providing theoretical support and practical guidance, we need to use a system method and empirical analysis method, and to effectively operate network economic crimes prevention and control mechanism so as to prevent, control, and combat network economic crimes.

REFERENCES

1. Criminal Law & Criminal Procedure Law. China Legal Publishing House, 2007, pp. 48-100.
2. Feng Shu-liang. Comparative study on the crime prevention between China and foreign countries. Chinese People's Public Security University press, 2003, pp. 133-173.

6 CNNIC (China Internet Network Information Center). The thirty-fifth statistical report on the development of China Internet Network. http://www.cac.gov.cn/2015-02/03/c_1114222357.html.

3. Liu Kun, Zhang Guang-chong. Research on the gathering mechanism of economic crime investigation. Journal of Shanxi Police Academy. 2015(4), pp 67-71.

4. Lang Jun-yi. On the criminal risk and prevention and control measures of the three-party payment under the view of internet finance——Taking the crime of bank card as the angle of view. Public Security Science Journal, 2014(6), pp. 27-32.

5. Ten major economic crime cases announced in 2013. http://cpn.cpd.com.cn/n17159841/c21550094/content.html.

6. Ten golden cases on the system of China's economic crime investigation in 2013. http://www.cpd.com.cn/epaper/rmgab /2013-11-28/05b-1.html.

7. The ministry of public security successfully commanded to crack a major case of manufacturing and selling fake world cup team jersey. http://www.gov.cn/xinwen/2014-07/01/content_2710456.html.

UDC: 343.533::004
343.985

CROSS-BORDER ACCESS TO DATA AS A WAY TO COLLECT ELECTRONIC EVIDENCE

Milana Pisarić[1]
University of Novi Sad, Faculty of Law

Abstract: Cybercrime is a phenomenon with prominent transnational, global dimension which imposes to prosecution authorities the need for gathering electronic evidence and catching perpetrators located in the territory of other states. The consequence of the expansion of information technology as a tool and subject of the offense is that the competent authorities of one country cannot, without cooperation with the competent authorities of another country, effectively combat this form of crime. Although obtaining evidence through mutual legal assistance plays an important role in the investigation of high technology crime, as the mechanisms for mutual assistance are slow and in some cases non-existent, the current issue is whether and under what circumstances the competent authorities of one country can legally take actions outside the borders of their own country, including the situation that the evidence is stored in the "cloud", which could be anywhere, and if they can directly access the computer data stored in computer systems/networks abroad via computers at the territory of another state, especially when there is a need for urgent action.

Keywords: cybercrime, investigation, electronic evidence, cross-border access to data, remote search.

TRANSNATIONALITY OF CYBER CRIME

Traditional understanding of information security which sets in spotlight an isolated computer system is not adequate in the circumstances of digital and wireless connection. The concept according to which the computer data is stored in a particular computer system in a particular place and within one country is becoming less relevant because the location where the computer data is stored in unstable and unclear. Networked world has become a big "playground" for the perpetrators of crimes against the confidentiality, integrity and availability of computer systems and data, of cybercrime in general. The challenges of technological progress before the prosecution authorities are reflected in the increased volume of data stored, processed or transmitted through a computer network, use of multiple devices to access data, facilities perpetrators have to hide the traces of activity and preserve anonymity, the utilization of computers of innocent persons or remote information structures for the execution of cybercrime, the use of cloud computing that store electronic evidence in the servers in different locations or websites whose IP addresses are constantly changing.[2]

The above mentioned factors cause difficult detection of offenses and perpetrators and therefore it is necessary to find a mechanism by which the authorities would be able to pro-

1 E-mail: mpisaric@pf.uns.ac.rs.
2 G. Laykock, "New Challenges for Law Enforcement", *European Journal on Criminal Policy and Research* 1/2004, 42.

vide electronic evidence that is unstable by nature and scattered in different jurisdictions. Implementation of the measures and actions for access to electronic evidence includes identifying specific locations in which computer data are stored. If the required information is located on the territory of another State, the competent authorities of one country cannot undertake evidentiary actions in the territory of another state in accordance with the principle of territorial sovereignty. Standard procedure in this situation involves the activation of cross-border cooperation between the competent authorities and mutual legal assistance. As the mechanisms of mutual assistance are slow and in some cases non-existent, the current issue is whether and under what circumstances the competent authorities of one country can legally take actions beyond the borders of their own country (including a situation where the evidence is stored in the "cloud" which could be anywhere), and directly access the computer data stored in computer systems/networks abroad via computers in the country, especially in the case where there is a need for urgent action.

NEED FOR EXTENSION OF TERRITORY PRINCIPLE OF CRIMINAL INVESTIGATION

The state is interested not only to criminalize extraterritorial conduct that produces a significant impact within its territory, but also to create the possibility that its competent authorities investigate these illegal behaviours by taking cross-border access and remote search of computer system/network that are outside the boundaries of its territory. Authorities in some countries are authorized to broaden the initial search to a computer system and storage devices that are on the territory of the State, if it is probable that the data necessary to demonstrate the high technology crime are stored in that second computer system or part of a computer system and if they can be accessed or in some other way become available through a computer system which is the object of the original action.

The question is whether the authorities would be entitled to extend an initial search to the other computer system if it is located in another state. If due to the transnational nature of cybercrime and the possibility of spatial distances between the offender and the victim, after a lengthy investigation with a lot of technical details, the prosecuting authorities would find that the computer of the offender is abroad, given that the authorities take action only within the territory of their country, the only way the necessary evidence is obtained and the person is arrested would relate to the use of mechanisms of mutual legal assistance in criminal matters, as required by the rules of public international law.

However, given the ineffectiveness of such mechanisms in terms of longevity of procedure, on the one hand, and the nature of the data to be processed, stored and transmitted via the Internet and the need for emergency response in cyberspace, on the other hand, would it be justified for the purposes of criminal proceedings for cybercrime, even if there is no international agreement that would allow international cooperation in collecting evidence, to give the authorities the power under certain conditions and in certain cases to access and search the computer systems and networks, which are located on the territory of another State, or to take certain actions and measures to collect the data even beyond the borders of their territory. This radical approach is not widely accepted because the majority of states are not ready to give up their sovereignty and to accept the competent authorities of other states to undertake certain investigative actions on their territory.[3] Once the competent authority determines that the necessary data are stored in a computer system/network that is located abroad and, after

3 M. Goodman, S. Brenner, „The emerging Consensus in on Criminal Conduct in Cyberspace", *International Journal of Law and Information Technology* 2/2002, 178.

observing the territories of which state the system/network is located, the authority checks whether there is adequate basis with the relevant country for mutual legal assistance and for triggering the mechanisms of international cooperation.[4]

However, the need to regulate access to computers, computer systems and computer networks in another country and search the data stored, processed or transmitted in them stems from the fact that in the Internet environment, due to the nature of the global computer network and connectivity of computer systems that are in different countries, it is quite possible to imagine a situation in which the competent authorities of one country, by taking certain evidentiary actions are not aware that their search includes the data in computer systems located in other countries, which may cause the violation of the territorial sovereignty of states if these actions were taken without prior notice, or consent of the other state.[5] As in cyberspace nation-state borders and jurisdiction of state authorities may have blurred frames, it may happen that the authorities access the stored data through electronic networks and that in doing so, they are not able to assess whether a particular computer data is stored in a computer that is physically located in their territory or in the territory of another country.

Unilateral access to the computer data stored in a computer system in a foreign territory without the need of the request for mutual legal assistance is a complex issue that requires a review of the rules of public international law concerning the sovereignty of the state, on the one hand, and is connected to the protection of the rights of individuals in terms of guarantees in accordance with national regulations, on the other hand.[6] For this reason it would be important that there are explicit rules of international law which would regulate the possibility of cross-border access and search of computer systems and networks abroad, instead of *laisee faire* practice.

This issue has been on the agenda since the late 1980s. It is mentioned in the form of "direct penetration" of the competent authorities in the territory of another state in the Recommendation on criminal offenses related to computers in 1989[7] and in the Final report of the European Committee on the problems of crimes from 1990.[8] These principle ideas are embedded in the Convention on Cybercrime,[9] but not in the sense that the competent authorities of a State are allowed to extend the search of a computer to a computer system located in the territory of another state which through a computer system within their boundaries can be accessed via the Internet or other computer networks, but in the case of a need for this, it is mandatory to involve the appropriate mechanisms for mutual legal assistance in criminal matters (in the sense of Article 31 of the Convention). However, in accordance with Article 32 of the Convention, which regulates cross-border approach as an exception to the territorial principle, the competent authorities of a State may, without making a request for mutual assistance to other Contracting State, *under certain conditions* unilaterally access to the *specific data* stored in computer systems in the territory of another state. Specifically, based on the above-mentioned article which regulates *Cross-border access to stored computer data with consent or where publicly available*, the competent authorities of the Contracting States, without first obtaining permits and notifying other States parties, are entitled to:

4 S. Brenner, J. Schwerha, "Transnational evidence gathering and local prosecution of international cybercrime", *John Marshall Journal of Computer and International Law* 3/2002, 356-358.
5 P. Bellia, „Chasing bits across borders", *University of Chicago Legal Forum*, 2/2001, 39-40.
6 In addition to legal demands, one should not ignore the lack of established and scientifically proven methodologies for data collection in this way. More on this, E. Kenneally, „Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection", UCLA Journal of Law and technology 5/2005,17.
7 R*(89)9 on Computer-related Crime, http://www.oas.org/juridico/english/89-9&final%20Report.pdf.*
8 *European Committee on Crime Problems,* Final Report, http://www.oas.org/juridico/english/89-9&final%20Report.pdf
9 Council of Europe Convention No. 185 on cybercrime, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

a) Access to computer data which are otherwise available to the public (open source), regardless of where the data is located geographically (e.g. the competent authorities can access and download the data stored on the web site without an obligation to notify the state in which the host computer system is), or

b) Access or receive the computer data stored abroad through a computer system in its territory, if they obtain a lawful and voluntary consent of the person who has the legal authority to make the data available through that computer system (e.g. if the person, whose e-mails are by service providers stored in another country or who intentionally keep information in a computer system in another country, would voluntarily allow the competent authorities to access the data).

Lawful and voluntary consent means that some binding request against a person was not versed which contains coercion or demonstration of the consequences for failure to act on the request, nor that the person is deluded, while the *consent* of a person is determined under the regulations of the country to whom the authority is given, or which conducts the cross-border access. As the first known case in which the cross-border access to abroad computers is realized is *United States v. Gorshkov*. In the investigation of offenses which two suspects using computers in Russia carried out against American companies in 2001, the FBI fraudulently obtained passwords to access computers of the suspects and came to the incriminating material which was used for the prosecution.[10] However, just this kind of conduct is recognized as a negative example in the literature, because the cross-border access is allowed only if there is consent. Whether the person is legally authorized to submit data is assessed according to the regulations of the state on whose territory is the computer which was cross-border approached. The important thing is the issue of where the person is when giving the consent or access to the data. There are two situations: the person is in the territory of the State whose authorities seek trans-border access or is located abroad, in which case it is necessary to keep in mind whether collecting and disclosing information to foreign government authorities without the mediation of local authorities is punishable, even due to the need to conduct criminal proceedings.[11] It is noteworthy that in this way it can be only accessed to strictly defined computer data that are clearly located, and that it is not allowed in terms of vague data, whose location is not identified. Also, single-side access to the data does not include the obligation of the State to inform another State of the actions taken in accordance with this article, but such a possibility is not excluded. Except in the cases provided for in Article 32 of the Convention, the competent authorities of one country are not allowed to access computer data stored in the computer system in the territory of another state, but only have the ability to send a request pursuant to Article 31.

So, there are two situations in which there is a need for electronic evidence stored in computer systems abroad, and whose circumstances cause the different treatment by competent authorities: A) The competent authority has taken control of a computer that is connected to the Internet and has the authority to access the sites or computers that are located in the territorial jurisdiction of another state on the basis of domestic law or a combination of domestic law and the provisions of Article 32 of the Convention on Cybercrime;[12] B) Electronic evidence is found in the "cloud" - for example, e-mail messages are not saved in the home computer of a suspect, which was confiscated, but are stored elsewhere on a remote server, for example, in the United States.[13] In this sense, we can distinguish direct trans-border access and trans-border access via electronic communications service providers.

10 N. Seitz, „Transborder search: a new perspective in law enforcement?", *Yale journal of law and technology* 7/ 2005, 24-25.
11 J. Goldsmith, „The Internet and the Legitimacy of Remote Cross-Border Searches", *The University of Chicago Legal Forum* 103/2001, 12.
12 L. Huey, Rosenberg R., „Watching the Web: Thoughts on expanding police surveillance opportunities under the Cyber-crime Convention", *Canadian Journal of Criminology and Criminal Justice* 10/2004, 600.
13 M. Wittow, D. Buller, „Cloud Computing: emerging legal issues for access to data, anywhere, anytime", *Journal of Internet Law* 1/2010, 3.

DIRECT TRANSBORDER ACCESS TO DATA

Regardless of the solutions retained by the Convention, the countries are overcoming the aforementioned difficulties in the investigation of cybercrime acceded in different ways. Some assume that their authorities have the ability to conduct cross-border computer search, so they use a computer in their territory to access and view the computer data stored abroad, if it is justified by the need of concrete criminal case. In the basis of the idea to permit cross-border searches of computers, in the sense the competent authorities are authorized to gain direct access to the cross-border, is the "virtual presence" of information in the national territory, while they may be viewed on a computer within the limits of their competence. In this way the act and the Serbian authorities, although there is no direct legal basis for it, which we believe would be justified if the Criminal Procedure Code would foresee such a possibility. For example, In Belgium in 2000 Law on IT crime adopted, in relation to which in Belgian Code of Criminal Procedure[14] article 88ter was prescribed, on the basis of which the investigating judge may extend the order on search of computer system, that allows the authorities of the Interior to access another computer system wherever it may be. The investigating judge extends the order including the remote computer system if it is necessary to ascertain the truth and other investigative measures are not adequate to achieve that goal, or there is a clear risk that evidence may be lost (the condition which is fulfilled whenever volatile data in a computer network are concerned). Giving this authority, the police does not have complete discretion in terms of coverage of a computer system, because the investigating judge limits in the order the search to specified parts of the computer system which can be accessed via the initially searched computer. If the circumstances indicate that the required electronic evidence is found in a computer that is in another state, the data that are accessed are copied. The investigating judge informs the Ministry of Justice through the Office of the Public Prosecutor's Office about this action, and the Ministry notifies the state on whose territory the computer system covered by the extended search is located.

However, the unilateral regulation of cross-border access to the computer does not solve the problem of exterritorial action and can be considered not only contrary to the principles of territorial sovereignty, but also useless and counterproductive for achieving the legitimate aims of the criminal proceedings, because even though cross-border searches of computers may be legal in one, in another country they could constitute a criminal offense in terms of unauthorized access to a computer system. Thus, in Spain the realization of remote access to the computer can only be based on the prior approval of the court at the reasoned request of the prosecutor with regard to serious offenses, unless other actions would not be able to collect necessary evidence (character of special investigative action) but this possibility is explicitly prohibited in respect of computers that are located abroad.[15]

The legislator of individual states is of the view that cross-border access to a computer that is located abroad and which can be accessed from their territory, is an issue that can be resolved only in accordance with the international agreements between countries. Thus, the Norwegian Criminal Procedure[16] does not provide for the ability to access a computer system that is on territory of other countries via computer on domestic territory, but assumes that measures of expeditious preservation of data (referred to in Article 29 and 30 of the Cybercrime Convention) aims at securing electronic evidence until the request for assistance

14 COE, *Transborder access and jurisdiction: What are the options?*, 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf, 32.
15 J. Pradillo, Fighting against cybercrime in Europe: the admissibility of remote searches in Spain", *European journal of crime, criminal law and criminal justice*, 19/2011, 382-383.
16 *Lov om rettergangsmaten i straffesaker (Straffeprosessloven) 53/2006,* http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf.

to the competent authorities of another state are sent and acted upon. A similar solution is contained in the Dutch Code of Criminal Procedure,[17] providing that there is a possibility of extending the search to another computer if it can be accessed through the computer that is the subject of the search action and if it is within the country's borders, while access to computers outside the territory of the Netherlands is not allowed in terms of the provisions of the Criminal Procedure Code, but only by the application of the rules of public international law or through ordinary mechanisms for mutual legal assistance (Article 552h). However, in *Bredolab* case in 2010, in which a network of botnets was created (using 143 servers whose host was the provider of electronic communications services in the Netherlands, while the attack was initiated from abroad) that infected over 30 million computers in several countries, after taking over botnets and servers, the Dutch police shut them down, and sent an automated message to all infected computers. Similarly, in the case of *Descartes*, the police approached servers (*TOR: The Onion Router*) which were not located in the Netherlands, and in which the images of child pornography were stored - that data was copied, and then removed from the server.[18] Although the court has been previously informed about these police actions, such conduct could be considered as illegal access to computers within the meaning of provisions of the Act.

An interesting solution is contained in the Portuguese law on cybercrime[19] relating to international cooperation of competent authorities in order to investigate the offenses related to computer systems and computer data, as well as for the purpose of collecting electronic evidence unrelated to the type of criminal offense. It is specifically provided that all forms of cooperation are pursued with respect to Law no. 67/98 on the transfer of personal data (Article 20). On the occasion of the application of the competent authority of another country to enable them to access the data stored on computer systems located on the territory of the country, it is envisaged that the Portuguese authorities undertake search and seizure of the computer data at the request of the other country, but only in situations where it may be carried out in accordance with the national legislation, and if there are circumstances that indicate that the requested information could be destroyed or altered, the authorities are obliged to act as expeditiously as possible. However, Article 25 provides that the competent authorities of other State may, without prior authorization by the Portuguese authorities: 1. Access the data stored in a computer system located in Portugal, if such data are publicly available, and 2. Receive or access through a computer system on their territory the data stored in Portugal, provided that there is a legitimate and voluntary consent of the person authorized in accordance with the law to make this information available. In terms of cross-border access to the computer data stored in the computer system beyond the borders of Portugal, Article 16 of the Act is important, which applies to cross-border seizure of the computer data which are accessed in accordance with Article 15. The computer search is done on the basis of court orders in order to find certain computer data in a given system, and if during the search it is obvious that the requested data resides in another computer system, even outside the territory of the state, but which can be lawfully accessed via searched computer, by an order, the initial search may be extended, by giving authorization to the competent authorities to remotely search the other computer system. This procedural action is ordered by the public prosecutor, and the authorization issued by the investigating judge is required if the computer data or files which are to be seized contain personal or intimate information on individuals and

17 Wetboek van Strafvordering, http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html.
18 *The effectiveness of international cooperation against cybercrime: examples of good practice,* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp;
19 *Lei do Cibercrime*, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0631906325.pdf;

thereby could jeopardize their right to privacy. Seizure of the data can be in different forms: by subtracting the physical device containing the data, copying of the data, preserving the integrity (without copying or removing), and permanent removal of information or blocking the access to the data.

CONCLUSION

After analysing the legal texts of individual countries, we may conclude that direct cross-border access can practically be realized in several ways:

A. In carrying out the search of the premises, the police come across a computer that is turned on and after obtaining necessary passwords from a person in a lawful manner, gain access to the computer data that are stored in the remote computer system. In terms of the possibility to remotely search the computer system, two situations may be distinguished: in some countries the police can achieve remote access even if it is obvious that the computer is located in the jurisdiction of another country (e.g. in Finland, Lithuania, Portugal, the USA), while in other countries further searches are only permitted if the person's consent is provided pursuant to Article 32 b of the Convention (e.g. Germany, Sweden, the Netherlands) where the person's consent, as a condition of the legality of the actions, cannot be replaced even for the reasons of extreme urgency (hence, collected electronic evidence could not be used in criminal proceedings).

B. Police lawfully obtains the passwords required to access the computer data stored in remote computer systems which are accessed through their computer system. This possibility exists in some national legislations even in a situation when it is obvious that a remote computer is located outside the territory of the state, and thus collected electronic evidence can be used in court (e.g., Finland, Norway, Sweden, Portugal).

C. Cross-border access to a remote computer is achieved by using special software (key loggers, sniffers, etc.) or other technical means, unless it is not obvious in the jurisdiction of which state the computer is located. If, however, it is clear that the computer, in which the requested data is located, is outside the territory of the state, this option is not allowed (with the exception of Japan).

D. During the investigation the police obtains legal and voluntary consent of persons on the basis of which they gain access to the computer data that can represent electronic evidence and which are stored in the computers in the jurisdiction of another country. The police may in some countries access and secure (take/copy) the necessary computer data, regardless of where the person giving consent is - whether on the territory of the State from which cross-border search is conducted or on the territory in which the remote computer is located (e.g., Finland, Portugal, Sweden). Whether the person has the legal authority to grant access to these data, is however estimated on the basis of regulations of the state in whose territory the data is stored (e.g., Finland, Portugal, the United States).

REFERENCES

1. Bellia P., „Chasing bits across borders", University of Chicago Legal Forum 2/2001, 35–101
2. Brenner S., Schwerha J., "Transnational evidence gathering and local prosecution of international cybercrime", John Marshall Journal of Computer and International Law 3/2002, 347–395.

3. COE, Transborder access and jurisdiction: What are the options?, 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf,

4. Council of Europe Convention No. 185 on cybercrime, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

5. European Committee on Crime Problems, Final Report, http://www.oas.org/juridico/english/89-9&final%20Report.pdf

6. Goldsmith J., „The Internet and the Legitimacy of Remote Cross-Border Searches", *The University of Chicago Legal Forum* 103/2001, 1-16

7. Goodman M., Brenner S., „The emerging Consensus in on Criminal Conduct in Cyberspace", *International Journal of Law and Information Technology* 2/2002, 139-223

8. Huey L., Rosenberg R., „Watching the Web: Thoughts on expanding police surveillance opportunities under the Cyber-crime Convention", *Canadian Journal of Criminology and Criminal Justice* 10/2004, 597-606

9. Kenneally E., „Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection", UCLA Journal of Law and technology 5/2005, 1-35

10. Laykock G., "New Challenges for Law Enforcement", *European Journal on Criminal Policy and Research* 1/2004, 39-53

11. Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0631906325.pdf;

12. Lov om rettergangsmaten i straffesaker (Straffeprosessloven) 53/2006, http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf.

13. Pradillo J., „Fighting against cybercrime in Europe: the admissibility of remote searches in Spain", *European journal of crime, criminal law and criminal justice*, 19/2011, 363–395

14. R*(89)9 on Computer-related Crime, http://www.oas.org/juridico/english/89-9&final%20Report.pdf.*

15. Seitz N., „Transborder search: a new perspective in law enforcement?", *Yale journal of law and technology* 7/ 200, 22-50

16. The effectiveness of international cooperation against cybercrime: examples of good practice, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp

17. Wetboek van Strafvordering, http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html;

18. Wittow M., D. Buller, „Cloud Computing: emerging legal issues for access to data, anywhere, anytime", *Journal of Internet Law* 1/2010, 1-5.

UDC: 005.52:343.9
004:343.9.018

PREDICTION OF CRIME COMPUTER COMPARISON STATISTICS

Venezija Ilijazi[1]
Vera Tanasijević
Ministry of the Interior of the Republic of Serbia

Abstract: CompStat (short for "Computer Comparison Statistics"), is a performance management system designed for the collection and feedback of information to reduce crime and achieve other police department goals. This process originated with the New York City Police Department and is now being adopted by many law enforcement agencies throughout the world. CompStat emphasizes information-sharing, responsibility and accountability, and improving effectiveness. CompStat includes four generally recognized components: timely and accurate information or intelligence, rapid deployment of resources, effective tactics, and relentless follow-up.

The CompStat model is a goal-oriented strategic management process within a performance management framework that synthesizes analysis of crime and disorder data, strategic problem solving, and a clear accountability structure. Ideally, CompStat facilitates accurate and timely analysis of crime and disorder data, which is used to identify crime patterns and problems. Based on this analysis, tailored responses are implemented through rapid deployment of personnel and resources. An accountability structure is key to ensuring the analysis is acted upon and the responses are implemented correctly as well as assessing whether responses are effective in reducing crime and disorder.

The primary purpose of our proposals is to challenge policy makers, practitioners, and scholars to reconsider the current relationship between CompStat and community policing and conceive of more innovative approaches to their co-implementation.

Keywords: Information technology, prediction of crime, analysis of crime, strategic management, requirements.

INTRODUCTION

CompStat is a "strategic performance management system" designed for the collection and feedback of information on crime and related quality of life issues.[2] Compstat (short for "Computer Comparison Statistics" or for "Computerized Statistics") was primarily designed to reduce crime and achieve other police department goals. Nowadays, it represents a dynamic approach to crime reduction, quality of life improvement, and personnel and resource management. The Compstat process can be summarized in one simple statement: "Collect, analyze, and map crime data and other essential police performance measures on a regular basis, and hold police managers accountable for their performance as measured by these data".[3] Compstat is a performance management tool based on the goal of continuous improvement, reflecting the paradigm of modern policing: accountability at all levels of a police agency.

1 E-mail: ilijazi@mup.gov.rs.
2 Police Foundation, The Growth of CompStat in American Policing, by D. Weisburd, S. D. Mastrofski, R. Greenspan, and J. Willis (Washington, D.C.: 2004).
3 Philadelphia Police Department, "The CompStat Process," 2003, (www.ppdonline.org/hq_compstat.php), May 6, 2003.

Implemented as innovative crime-reduction program in 1994 by then commissioner William Bratton of the New York City Police Department and his staff, Compstat has evolved over time and grown – from a basic and fairly rudimentary process involving the collection and analysis of crime data to ensure accountability and information sharing among police members into a more complex and more effective management mechanism. Since mid-nineties Compstat has been recognized as a major innovation in American policing and has since been widely embraced management model focused on crime reduction. In the few years since its appearance, the Compstat model has been adopted in numerous cities in the United States of America under various acronyms. The process has recently been described as an "emerging police managerial paradigm"[4] or "a new paradigm revolutionizing law enforcement management and practice"[5] while others have called it "perhaps the single most important organizational/administrative innovation in policing during the latter half of the 20th century".[6]

PRINCIPLES OF COMPSTAT

Compstat has a well-established and proven track record in reducing crimes and improving the overall operating systems of several major metropolitan police departments in the United States. Police Departments such as New York, Boston, Philadelphia, Miami, New Orleans, and Newark, New Jersey have all experienced significant reduction in violent crimes as a result of the implementation of the Compstat crime control model (Figure 1). Although many of these departments have custom tailored the COMPSTAT process to their own department and community needs, the core elements of COMPSTAT have remained the same. Compstat comprises information-sharing, responsibility and accountability, and improving effectiveness. It includes four generally recognized core principles.

An essential component of the Compstat philosophy is its emphasis on holding police managers directly accountable for combating the crime in their area of responsibility and providing them the authority to deploy their resources to achieve the targeted goals.

The elements of Compstat consist of four distinct principles:

1. Accurate and timely information or intelligence

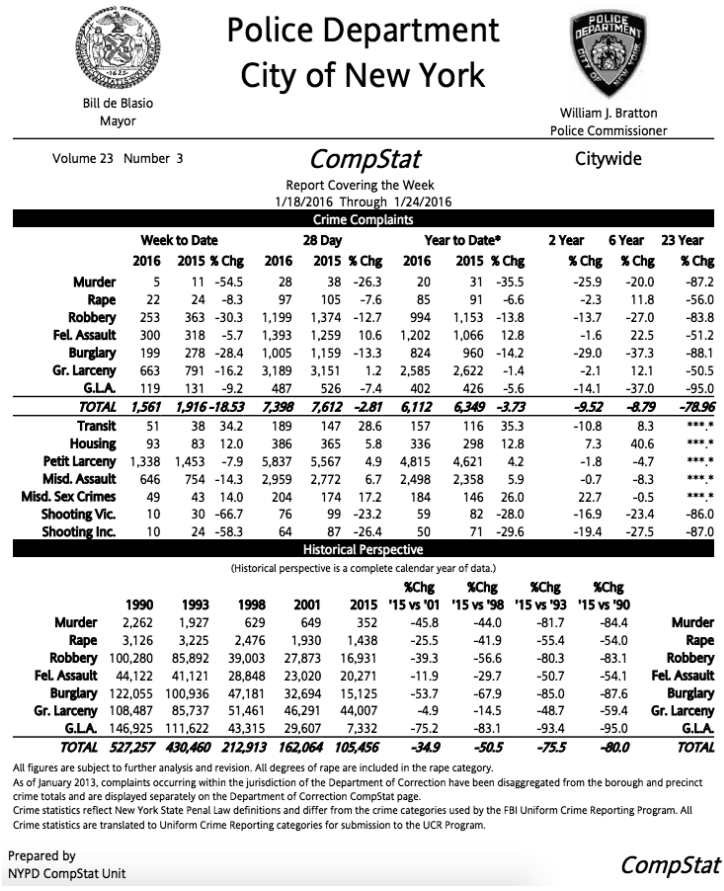
Gathering accurate and timely intelligence or information is essential to effectively responding to any problem or situation. Crime intelligence relies on data primarily from official sources, and it is required to provide a method in which essential information can easily and effectively be shared with all levels of the organization. These information should be accurate and available as close as possible to real-time. Collected crime and disorder data is then used to produce crime maps, emerging crime trends and patterns, and other products of analysis. Subsequently, decision makers use these information products to identify crime problems to be addressed. This principle suggests that the information or intelligence is used to apply the necessary resources to an identified problem area, enabling leaders to have more holistic view of the entire organization.[7]

4 Ibid.

5 Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies, Bureau of Justice Assistance, Police Executive Research Forum, 2013, (http://www.policeforum.org/Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies.pdf)

6 Manhattan Institute, Center for Civic Innovation, Do Police Matter? An Analysis of the Impact of New York City's Police Reforms, Civic Report no. 22, by G. L. Kelling and W. H. Sousa, (December 2001), (www.manhattan-institute.org), July 26, 2006.

7 Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies, Bureau of Justice Assistance, Police Executive Research Forum, 2013, pp. 5 (http://www.policeforum.org/Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies.pdf)



Police Department
City of New York

Bill de Blasio
Mayor

William J. Bratton
Police Commissioner

Volume 23 Number 3

CompStat

Citywide

Report Covering the Week
1/18/2016 Through 1/24/2016

Crime Complaints

	Week to Date			28 Day			Year to Date*			2 Year	6 Year	23 Year
	2016	2015	% Chg	2016	2015	% Chg	2016	2015	% Chg	% Chg	% Chg	% Chg
Murder	5	11	-54.5	28	38	-26.3	20	31	-35.5	-25.9	-20.0	-87.2
Rape	22	24	-8.3	97	105	-7.6	85	91	-6.6	-2.3	11.8	-56.0
Robbery	253	363	-30.3	1,199	1,374	-12.7	994	1,153	-13.8	-13.7	-27.0	-83.8
Fel. Assault	300	318	-5.7	1,393	1,259	10.6	1,202	1,066	12.8	-1.6	22.5	-51.2
Burglary	199	278	-28.4	1,005	1,159	-13.3	824	960	-14.2	-29.0	-37.3	-88.1
Gr. Larceny	663	791	-16.2	3,189	3,151	1.2	2,585	2,622	-1.4	-2.1	12.1	-50.5
G.L.A.	119	131	-9.2	487	526	-7.4	402	426	-5.6	-14.1	-37.0	-95.0
TOTAL	*1,561*	*1,916*	*-18.53*	*7,398*	*7,612*	*-2.81*	*6,112*	*6,349*	*-3.73*	*-9.52*	*-8.79*	*-78.96*
Transit	51	38	34.2	189	147	28.6	157	116	35.3	-10.8	8.3	***.*
Housing	93	83	12.0	386	365	5.8	336	298	12.8	7.3	40.6	***.*
Petit Larceny	1,338	1,453	-7.9	5,837	5,567	4.9	4,815	4,621	4.2	-1.8	-4.7	***.*
Misd. Assault	646	754	-14.3	2,959	2,772	6.7	2,498	2,358	5.9	-0.7	-8.3	***.*
Misd. Sex Crimes	49	43	14.0	204	174	17.2	184	146	26.0	22.7	-0.5	***.*
Shooting Vic.	10	30	-66.7	76	99	-23.2	59	82	-28.0	-16.9	-23.4	-86.0
Shooting Inc.	10	24	-58.3	64	87	-26.4	50	71	-29.6	-19.4	-27.5	-87.0

Historical Perspective

(Historical perspective is a complete calendar year of data.)

	1990	1993	1998	2001	2015	%Chg '15 vs '01	%Chg '15 vs '98	%Chg '15 vs '93	%Chg '15 vs '90	
Murder	2,262	1,927	629	649	352	-45.8	-44.0	-81.7	-84.4	Murder
Rape	3,126	3,225	2,476	1,930	1,438	-25.5	-41.9	-55.4	-54.0	Rape
Robbery	100,280	85,892	39,003	27,873	16,931	-39.3	-56.6	-80.3	-83.1	Robbery
Fel. Assault	44,122	41,121	28,848	23,020	20,271	-11.9	-29.7	-50.7	-54.1	Fel. Assault
Burglary	122,055	100,936	47,181	32,694	15,125	-53.7	-67.9	-85.0	-87.6	Burglary
Gr. Larceny	108,487	85,737	51,461	46,291	44,007	-4.9	-14.5	-48.7	-59.4	Gr. Larceny
G.L.A.	146,925	111,622	43,315	29,607	7,332	-75.2	-83.1	-93.4	-95.0	G.L.A.
TOTAL	*527,257*	*430,460*	*212,913*	*162,064*	*105,456*	*-34.9*	*-50.5*	*-75.5*	*-80.0*	*TOTAL*

All figures are subject to further analysis and revision. All degrees of rape are included in the rape category.
As of January 2013, complaints occurring within the jurisdiction of the Department of Correction have been disaggregated from the borough and precinct crime totals and are displayed separately on the Department of Correction CompStat page.
Crime statistics reflect New York State Penal Law definitions and differ from the crime categories used by the FBI Uniform Crime Reporting Program. All Crime statistics are translated to Uniform Crime Reporting categories for submission to the UCR Program.

Prepared by
NYPD CompStat Unit

CompStat

Figure 1: *CompStat Report*

2. Effective tactics

Relying on past experience and appropriate resources, decision makers and executives plan tactics that will respond adequately to the identified problem. These tactics may include members of law enforcement, as well as members of government and community. Compstat program involves crime control strategy meetings, which increase information sharing between the organization's executives and the commanders of operational units, thus creating conditions for collective process for developing tactics as well as accountability for developing these tactics.

Compstat tactics encourage "thinking outside the box" and make every resource, both internal and external, credible enough to be reconsidered as possible solution to a problem. Compstat tactics also provide for a sense of urgency in responding to problems.

3. Rapid deployment of resources

Traditional methods of policing are characterized by reactive policing model, organizational inflexibility and centralized authority. Opposed to the reactive policing model, the Compstat model aims to deploy resources to emerging crime trends or patterns to enable a

strategic police response, as a means of heading off the problem before it continues or escalates. As such, the tactics should be deployed in a timely manner.

Compstat strives to identify emerging problems using real-time information and a real-time capability to address the ongoing situation rapidly and directly. CompStat seeks to apply this approach to regular, recurring crime patterns, trends and hot spots (Figure 2). This concept also applies to recurring internal risk management incidents. Rapid deployment of resources increases the likelihood of affecting a problem before it continues and expands.

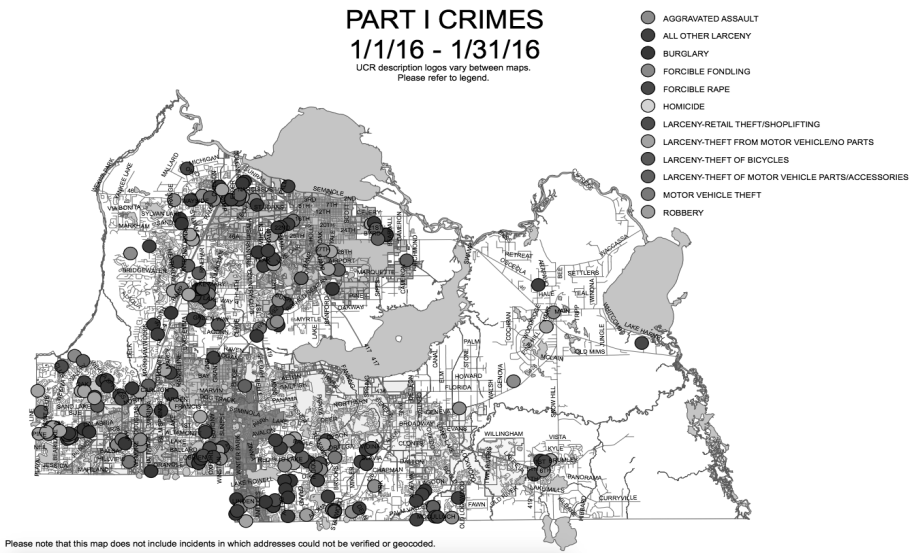


Figure 2: *CompStat - Prediction of Crime*

4. Relentless follow-up and assessment

A vital element in any operational plan is the need to critically assess past tactics and impact that the implementation of the plan executed on the targeted goals. The essence of the Compstat process is managing for results. Basic indicators of the results are identifying whether the plan succeeded or failed to affect the identified problem or issue and to what degree it can be shown through quantitative and/or qualitative measures. Any effort the police department invests - no matter whether administrative, operational or investigative - is evaluated by the results achieved in accomplishing the desired outcomes.

The Compstat meeting provides the opportunity to follow-up and assess on the success of current and past strategies in coping with identified problems. This success or lack thereof, provides insight of how to improve current and future planning and deployment of resources.

The primary method for measuring a successful outcome of a crime reduction strategy is by using crime statistics. Changes in numbers and continued monitoring of a target area can demonstrate the long-term effectiveness, or lack thereof, of any crime reduction strategy.

Two components that are integral to the Compstat process are also key features of community policing: solving problems in opposite to simply reacting to them, and recognizing quality-of-life issues as generators for criminal activity. The Broken Windows Theory model focuses on the importance of disorder (e.g. broken windows) in generating and sustaining

more serious crime.[8] The rapid deployment of resources that is one of core components of Compstat gets immediate results, as opposed to other forms of community policing that make vague references to the eventuality of change.

One of the main reasons for Compstat's success is seen in its ability to combine elements of both traditional- and community-based programs: "It melds both the reactive and proactive approaches of policing by first focusing on the problem, reacting to it, and ultimately utilizing resources to address it".[9]

Compstat fosters accountability by holding police leaders, top executives and other individuals responsible for knowing the details about the crime in their assigned areas and for devising plans to reduce crime levels. Compstat encourages information sharing within a police department as well as between police and other organizations that can help eliminate conditions that contribute to crime. Actually, key principle of Compstat—gathering and analyzing data to produce solutions—is so universal, it has been adopted by other organizations that have no connection to policing.

THE COMPSTAT PROCESS

The most widely recognized element of Compstat is its regularly occurring meetings where executives of police departments and officers discuss and analyze crime problems and the strategies used to address those problems.

At the core of the Compstat process is an examination and review of an organization's status as indicated by quantifiable statistical indicators. The process begins by collecting, analyzing and mapping crime data as it occurs. In a police environment, this means analyzing numbers and locations of crimes and arrests as well as suspects, victims, days and times of criminal activity, and so forth, to identify crime patterns, clusters, suspects, and hot spots. Using these data a report is compiled and forwarded to organizational unit's commander. After the statistical trends are reviewed and discussed, it is up to the commander to devise effective tactics to address the problem areas. Subordinates are encouraged to formulate problem-solving strategies that will result in increasing incidences of crime. The Compstat process encourages creativity in creating strategies, allocating resources, and deploying police personnel while holding managers and employees accountable for confronting the problems of crime proactively.[10]

Once a plan of action is formulated, commanders must then deploy personnel and resources in a timely manner, which is often the most challenging element of Compstat, due to conflicting work schedules and limited funds. Finally, the executives must determine if the intended goals were accomplished and, if not, must alter their strategies or come up with new ones to effectively address the problem.

Law enforcement leaders may see several benefits from a Compstat program. For example, Compstat can help focus attention and resources on crime and the causes of crime. In return, this focus can lead to better deployment plans. Compstat can also be a helpful tool to demonstrate that police resources are monitored and used effectively.

It is crucial that the strategy, purpose, and goals of Compstat program must be clearly articulated and understood not just by the decision makers and top executives, but by all

8 George L. Kelling and James Q. Wilson, Broken Windows: The Police and Neighborhood Safety, Atlantic Monthly, March 1982 Issue (http://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/)

9 Susan Geoghegan, Compstat Revolutionizes Contemporary Policing, Hendon Publishing (http://www.hendonpub.com)

10 Jeff Godown, The CompStat Process: Four Principles for Managing Crime Reduction, The Police Chief, February 2016 (http://www.policechiefmagazine.org)

personnel within the organization. To ensure that employees understand this information, it should be continuously communicated to all ranks of the department. Once employees understand the purpose and goals of Compstat, it can become a valuable tool for moving an organization in unison towards shared goals.[11]

Compstat systems are much more than a meeting, then rather dynamic performance management system. Two Compstat meetings are never the same, nor should they be, even in the same organization. But it is essential that Compstat meetings be consistent with an organization's mission, organizational strategies, and culture.

While Compstat was developed to meet the needs of the NYPD in 1994, the experiences of other agencies since then demonstrate that Compstat can be adapted for use in any law enforcement agency. According to Bill Bratton, who introduced Compstat to NYPD "An inherent strength of Compstat and performance management systems is that they can be modified to direct and control significantly different environments. Compstat may be affected by cultural and organizational differences, budget constraints, and agency bureaucracies."[12]

Just as Compstat can be modified to fit the needs of different agencies, it can continue to evolve after being implemented. It is also a flexible strategy, so it can be a key tool for leaders looking to implement organizational change, or direct organization towards newly established vision, mission and values. It provides leaders with a mechanism for holding commanders and other employees responsible for responding to the crime and quality-of-life problems within their area of responsibility. To strengthen the accountability process, it is necessary that the department's leadership team understands its responsibilities and has a clear view of crime, and that the attendees at the Compstat meetings leave the meeting with a clear understanding of what are their priorities, what is expected of them and how they will be held accountable. Many agencies organize accountability by geographic area.[13]

Follow-up, as an application of the fourth principle of Compstat, can take many forms, from formal procedures, such as written reports, to track and ensure follow-up, to short briefings and informal discussions. This step helps agencies to identify successful strategies by closely examining the impact of various approaches, implementing successful strategies in other areas, and improving or abandoning ineffective strategies.

FUTURE OF COMPSTAT

Restrictions in public sector budgets require more efficient policing, and Compstat can help to ensure that police resources are monitored and used effectively. Compstat can help agencies establish priorities and demonstrate their effectiveness in achieving goals.

Some authors believe that future of Compstat lies in its flexibility: program is easily tailored by each city and municipality to fit its particular needs.[14] Law enforcement agencies that have studied the NYPD's Compstat process have successfully incorporated some, but not all, of its components into their policing strategies.[15]

11 Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies, Bureau of Justice Assistance, Police Executive Research Forum, 2013, pp. 8 (http://www.policeforum.org/Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies.pdf)
12 Ibid. pp. 9
13 Ibid, pp.10-15.
14 Dr. Vincent E. Henry, Managing Crime And Quality Of Life Using Compstat: Specific Issues In Implementation And Practice, (http://www.unafei.or.jp/english/pdf/RS_No68/No68_12VE_Henry2.pdf)
15 Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies, Bureau of Justice Assistance, Police Executive Research Forum, 2013, (http://www.policeforum.org/Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies.pdf)

The strength of the Compstat process lies in the management and accountability factors. While computer mapping and rapid deployment of resources are key components, without a clear, purposeful strategy routinely communicated to all employees and effective leadership Compstat would not be expected to remain a critical part of policing in the future. (Figure 3)

Figure 3: *CompStat - Dashboard*

Compstat process is achieved by combining technology resources with the human factor, and it is likely to continue evolving with policing innovations and technological advances. Breakthroughs in information systems and computer technology will have an impact on the ability of police agencies to quickly and accurately identify crime problems and deploy resources. Managing the enormous quantities of available information will probably require that agencies place a higher priority on investing in crime analysis, including implementing principles of predictive analytics and ILP. This implies hiring professional crime analysts, providing them with training to stay abreast of the latest developments, and fully utilizing their skills to perform sophisticated analyses. Developing crime analysis dashboard systems, so that commanders can have more immediate access to crime numbers, may help relieve crime analysts of the administrative tasks associated with preparing reports. Agencies will continue to find innovative ways to apply the four Compstat principles, as well as examine how they can use Compstat to track important measures in addition to crime rates, such as use of force, public opinion about the police, complaints against officers, and metrics to assess the effectiveness of community policing efforts. Compstat might also become more decentralized.

Impact of social media offers police agencies new opportunities to communicate with the public via platforms like Facebook and Twitter, thus changing the way the Compstat is conducted, and to inform public and demonstrate to the community their work. Use of internet is natural opportunity for police to exchange information and opinions from the public, and social media can facilitate this process.

INTRODUCING COMPSTAT IN THE MINISTRY OF INTERIOR OF THE REPUBLIC OF SERBIA

Ministry of Interior of the Republic of Serbia is recently going through many organizational and infrastructural changes, seeking to keep pace with contemporary trends in effective policing. Introducing Compstat in MoI is recognized as importance of implementing effective strategies and principles in order to improve information sharing and accountability across the organization, aiming at crime reduction and overall improvement of crucial life issues at the society.

MoI recognizes that success of any Compstat program depends on effective crime analysis. Crime analysis provides the information and findings that guide the Compstat meetings and help decision makers to deploy resources more effectively. Analysts should provide insight on crime patterns and trends, not simply report raw crime numbers, so it was expected that the idea of introducing Compstat in the MoI would emerge in the Department for Statistical Analytics and Development.

A common component in effective police strategies is the use of systematic crime analysis to help guide and prioritize crime reduction efforts, as MoI is continually challenged with limited resources, deployment issues, and other pressures that test its capacity to provide quality public safety service and implement crime reduction strategies.[16]

One of the principal challenges of establishing a Compstat system is deciding which performance indicators should be measured: "outcomes", such as crime reduction and improved quality of life, or police activity, such as arrests and traffic stops. Using principles of community policing, as well as principles of predictive analytics and ILP which are also introduced to MoI, strategic approach to introducing Compstat to MoI was to on metrics related to crime reduction and quality of life improvement.

Study authors found that both Compstat and community policing value flexibility and promote a decentralized decision-making process. However, Compstat tends to push accountability down primarily to middle managers, while community policing places greater emphasis on the role of lower-level officers. And in contrast to community policing, Compstat focuses more on internal accountability and data-driven problem-solving. Community policing places a high value on partnerships with outside persons and entities, while Compstat looks to select the most effective method to solve a problem—even if that method may not involve community policing.[17]

Since the methods of Compstat are transferable, compatible, and replicable in any organization or environment, in Department for Statistical Analytics and Development Compstat functions as a crime control process manifested in recurring meetings, usually weekly, during which the organizations performance indicators are reviewed critically for opportunities for improvement. Formal reports are made weekly, monthly, quarterly and annually using contemporary computer tools (GIS, SPSS, IBM-COGNOS) and submitted to senior executives and decision makers in MoI. (Figure 4)

16 The Integration Of Crime Analysis Into Patrol Work: A Guidebook, Bruce Taylor, Ph.D. NORC at the University of Chicago Rachel Boba, Ph.D. Florida Atlantic University with Sergeant Jeff Egge Minneapolis Police Department,

17 Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies, Bureau of Justice Assistance, Police Executive Research Forum, 2013, pp. 24 (http://www.policeforum.org/Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies.pdf

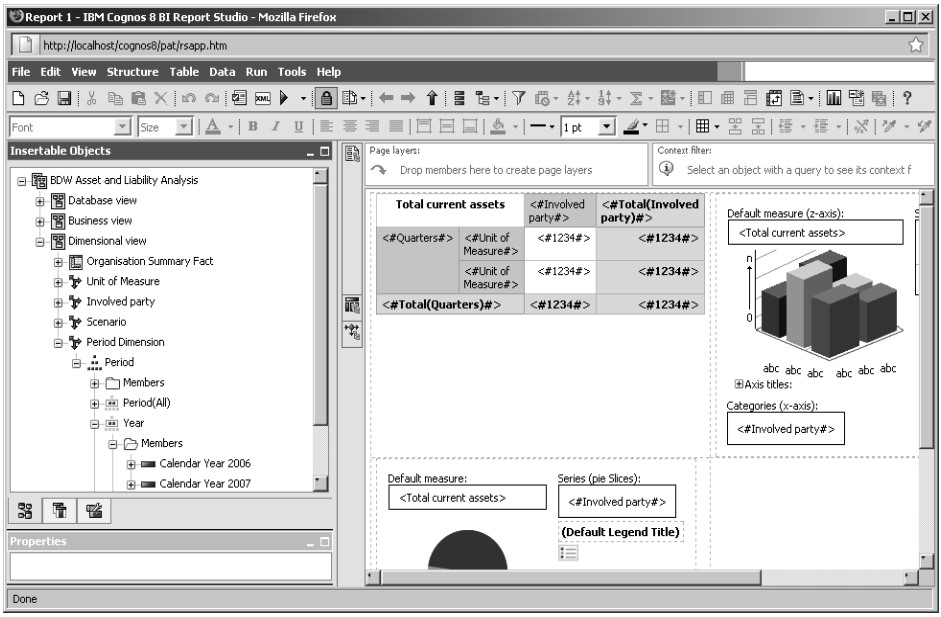


Figure 4: *CompStat to MoI – IBM-COGNOS Dashboard*

At the core of the process is an examination and review of an organization's status as revealed by quantifiable statistical indicators. In a police environment, this means analyzing numbers and locations of crimes and arrests as well as suspects, victims, days and times of criminal activity, and so forth, to identify crime patterns, clusters, suspects, and hot spots. Strategies are then formulated to counter increasing incidences of crime. The Compstat process encourages creativity in creating strategies, allocating resources, and deploying police personnel.

The CompStat process is seen as a two-pronged examination of police operations, relying to best practice of contemporary policing.[18] The first prong looks outwardly at crime and its effects in the community, while the second examines the organization internally to identify best practices in managing such police personnel and risk management issues as sick time, use of force, pursuits, complaints, and accompanying municipal liability. The examination of crime and internal police department processes allows for the reengineering of those processes in response to crime, an action that can produce significant public safety gains not only in terms of reducing crime but also in increasing effectiveness in various other essential police performance measures.

18 Jeff Godown, The CompStat Process: Four Principles for Managing Crime Reduction, The Police Chief, February 2016 (http://www.policechiefmagazine.org)

REFERENCES

1. Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies, Bureau of Justice Assistance, Police Executive Research Forum, 2013 (http://www.policeforum.org/Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies.pdf)
2. George L. Kelling and James Q. Wilson, Broken Windows: The Police and Neighborhood Safety, Atlantic Monthly, March 1982 Issue (http://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/)
3. Jeff Godown, The CompStat Process: Four Principles for Managing Crime Reduction, The Police Chief, February 2016 (http://www.policechiefmagazine.org)
4. Manhattan Institute, Center for Civic Innovation, Do Police Matter? An Analysis of the Impact of New York City's Police Reforms, Civic Report no. 22, by G. L. Kelling and W. H. Sousa, (December 2001), (www.manhattan-institute.org), July 26, 2006.
5. Philadelphia Police Department, "The CompStat Process," 2003, (www.ppdonline.org/hq_compstat.php), May 6, 2003.
6. Police Foundation, The Growth of CompStat in American Policing, by D. Weisburd, S. D. Mastrofski, R. Greenspan, and J. Willis (Washington, D.C.: 2004).
7. Susan Geoghegan, Compstat Revolutionizes Contemporary Policing, Hendon Publishing (http://www.hendonpub.com)
8. The Integration Of Crime Analysis Into Patrol Work: A Guidebook, Bruce Taylor, Ph.D. NORC at the University of Chicago Rachel Boba, Ph.D. Florida Atlantic University with Sergeant Jeff Egge Minneapolis Police Department.

UDC: 343.533.9::004

CRIMINAL OFFENSES AGAINST INTELLECTUAL PROPERTY RIGHTS IN THE CYBERCRIME

Milica Stojković[1]

Abstract: The sum of crimes were computers, computer networks, computer data, as well as their products, both in the material as well as in electronic form, appearing as its object the execution of this kind of crime and funds for the execution of the same, its called cybercrime (high-tech crime). It is important to point out the characteristics of these various offenses, which connects the unity of group object protection. The appearance of this type of crime is characterized by the abuse of information and broadcasting technologies. In addition to the damage of computer data and programs, computer sabotage, making the introduction of computer viruses, computer fraud, unauthorized access to a protected computer, computer network and electronic data processing, prevent and limit access to public computer network and unauthorized use of a computer or computer network, in this area indirectly includes offenses against intellectual property, assets and legal transactions in which recognize the characteristics of this group of offenses. Intellectual property is the product of human creativity, creativity and innovation in science, technology and art, and consists of the rights of authors, inventors and other holders of intellectual property rights. This term for certain creations of the human mind and commercial symbols representing intangible property which can enjoy different levels of protection of exclusive rights similar to ownership, enabling their commercial activities and the exploitation of the market, which leads to frequent abuses and violations of intellectual property rights, and often and in the field of cybercrime, which thus causes large-scale economic damage, which will be discussed in this paper.

Key words: criminal offense, intellectual property, information technology, computer data

INTRODUCTION

Nowadays, the impact of computers is so great that it reflects on the entire world around us. In the modern world there is one big perfected front which is present worldwide. However, full confidence in modern computing technology can be very dangerous and the consequences that economic, social and personal way. Sure, they represent the most revolutionary technical and technological discovery. In addition to all of their benefits and advantages, can easily become a tool of abuse of individuals, groups and organizations illegal, unlawful and socially dangerous activities. The real boom and mass phenomenon experienced by viruses spreading RS in offices and households, followed by development of the Internet, creating a huge base of users-both potential victims and those malicious.[2]

Cybercrime is a form of criminal conduct, in which the use of computer and broadcasting technologies, as well as information systems manifests as a way to commit the offenses, where the computer and computer network used as a means or purpose of enforcement. High tech-

1 E-mail:mstojkovic1@yahoo.com

2 Веиновић М., Милосављевић М., Грубер Г., Информатика, Универзитет Сингидунум, Београд 2009.

nology can be abused in various ways, and the crime can have any kind of conventional forms of crime, such as theft, tax evasion, fraud, and data obtained in this way are used to obtain illegal profit in each critical situation.

Organizations criminals increasingly orient the action of robberies in which the object is abusing computer electronics. Do not record a fall classic robbery, but from year to year a new type of crime in which the electronics used as a means to win the multi-million criminals sum of money.[3] New forms of value, concentration data, new ambience operation with new methods and techniques, narrowing the time scale of operation to expand the geographical area of mobility and stability risks are changes that favor the spread of cybercrime.

GENERAL CHARACTERISTICS OF CRIMINAL OFFENSES IN THE CYBERCRIME

The new offenses is not fully covered area where action is being taken against the security of computer data and various forms of abuse of information technology. As with the development of computers and expanding the number of its users is increasingly damaging the security of computer data of legal and natural persons, opens up new technical possibilities to carry out existing and the emergence of new crimes by abusing the Internet. One of the existing definition of this type of crime is that it is "the commission of offenses for which its subject and object have the Internet as a global computer network and computer that make the trained persons in order to cause harmful effects or obtaining illegal material benefit".[4] The Criminal Code of the Republic of Serbia determines the terms movable, computer data, computer networks, computer software, computer virus, computer and computer system. Due to factors of technical equipment and training of police officers, legal regulations which do not comply with contemporary forms of crime, lack of operational training for public officials, as well as the difficulty in discovering the identity and location of offenders, difficult is the way to combat high-tech crime.

Criminal offenses against the security of computer data enters the so-called high technology or computers crime, or, cybercrime.[5] This term represents exercise of criminal offenses by which such facility chili as a means to commit the offenses occurring computers, computer networks, computer data, computer systems, as well as their products in material and electronic form. The concept, features, bodies of criminal prosecution and the procedure for this type of crime, are governed by the provisions of the Law on organization and jurisdiction of state authorities to combat cybercrime.[6]

Computer and information system is one of the modern system that is played on the stage of the international community. This system has entered the homes, institutions and a large number of citizens because of their necessity for the modern trends of business and communication. Some individuals, groups and organization to breach his weight, because of capacity, character and quality it represents. Modern threats are multiple, usually by viruses, respectively, of viral system, which destroy the data, system and computer network.

The information system is an integrated set of components for collecting, recording, storing, processing and transmitting information. Business enterprises, organizations and individuals rely on information management systems in their operations, maintain competitive-

3 Алексић, Ж., Милосављевић З., Лексикон криминалистике, Београд, 1993.

4 Стаменковић, Б., Високотехнолошки криминал- практични водич кроз савремено кривично право и примјере из праксе, Подгорица, 2014.

5 Martin, D., Martin F.P., Cybercrime, menaces vulnérabilités et rispostes, Paris, 2001.

6 „Сл.гласник РС", бр.61/2005 и 104/2009, The Office of the High Tech Crime exists as a separate department Higher Public Prosecutor's Office with headquarters in Belgrade.

ness in the market, offer a variety of services and improvement of personal skills. Business organizations depend on computer information systems to process the its financial accounts and business transactions, manage human resources, municipal governments depend on information systems to offer basic services to its citizens, individuals use information systems to advancing their knowledge, for the conclusion of various legal transactions.

The Criminal Code[7] of the Republic of Serbia prescribes criminal responsibility and punishment for criminal offenses against security of computer data. The perpetrators of these acts carried out computer abuse, which caused material or non-pecuniary damage to natural or legal persons. The object of protection of these crimes is the security of computer data and systems, or, computer networks.[8]

INDIVIDUAL COMPUTER CRIMINAL OFFENSES

The criminal legislation of the Republic of Serbia, the system of offenses against the security of computer data consists of the following crimes: damage to computer data or programs, computer sabotage, creation and introduction of computer viruses, computer fraud, unauthorized access to a protected computer, computer network and electronic data processing, prevention and restricting access to a public computer network, unauthorized use of a computer or computer network, making, procuring or providing other means to commit offenses against the security of computer data.

The offense of damaging computer data about the program consists in the unauthorized deletion, alter, damage, conceal or otherwise committing useless computer data or programs. Computer sabotage makes the person who enters, destroys, deletes, alter, damage, conceals or otherwise renders useless computer data or programs, or destroy or damage a computer or other device for electronic processing and transmission of data in order to prevent, or significantly disturbing the process of electronic processing and transmission of data from which are of importance to the state organ, public service institution, company or other entity. Creating and introducing computer viruses consists in the intention of its introduction, or its introduction into someone else's computer or computer network. Computer fraud represents the input of incorrect data, leakage entering correct data, or otherwise conceal or disguise the information which influence the result of electronic processing and transmission of data in order to obtain for himself or another unlawful material gain, thereby causing damage to another person. Unauthorized access to a protected computer, computer network or electronic data processing consists in the unauthorized inclusion in a computer or computer network, or unauthorized access to electronic data processing by violating measures. Preventing and limiting access to the public computer network is a criminal offense which consists in preventing unauthorized or om, sert access to the public computer network. Unauthorized use of a computer or computer network is use of computer services or computer network with the intent to yourself or another person obtaining illegal material benefit. Making, procuring or providing other means to commit offenses against the security of computer data is a punishable offense which involves preparatory work for the execution of any other computer part, and consists in possessing, making, procuring, selling, or giving each other the use of a computer, computer system , computer data or programs for the execution of any of the offenses against the security of computer data.

7 „Сл.гласник РС", бр.85/2005, 88/2005-испр.107/2005-испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014
8 Водинелић, В., Методика откривања, разјашњења и доказивања рачунарског криминалитета, Загреб, 1990.

THE COMMON CHARACTERISTICS OF CRIMINAL OFFENSES AGAINST INTELLECTUAL PROPERTY

Intellectual property is a set of rights relating to: literary, artistic and scientific works, artist interpretations of performers, phonograms, videograms, broadcasts, inventions in all fields of human endeavor, scientific discoveries, industrial designs, factory, trade and service marks, and trade names and trade names, protection from unfair competition, and all other rights relating to intellectual activity in the industrial, scientific, literary and artistic field. With all its forms, it is very similar to real property law. The essential difference between intellectual property and real property law is tenure as a de facto relationship appropriation things she real right exists and there is intellectual property, because they are intelectual creations that can not hold. A common feature of industrial property rights and property rights are subject as a result of intellectual creativity, or spiritual, non-material creation and economic functions, which is reflected in the exclusive authority of the commercial exploitation of intellectual property through guarantees of subjective rights. Intellectual property rights of employers and their employees are protected by national law and by international treaties.

The basic principle of the market economy, freedom of competition, from which it follows that it is used for free public domain rule, and intellectual property exception. Intellectual property as a private right is available only under certain conditions, for new, original, distinctive work of intellectual creation, which go beyond the public domain and intellectual property rights of others. The second principle is the limit to protect creations of the mind, and commercial symbols. Intellectual property does not protect ideas as such, in absolute terms, but only a specific expression of those ideas and the practical application of ideas.

Intellectual property constitutes a preventive law relating to certain marketing activities of others in order to prevent unauthorized commercialization of creations of the mind, without the consent of the copyright holder. Protection of intellectual property is by its nature temporary and is aimed at channeling the intellectual creations in the public domain once the exclusive rights cease.

Rules to prevent unfair competition are aimed at ensuring the efficient functioning of the market economy by preserving the liberty and fair business competition and protect the interests of consumers. Certain rules to prevent unfair competition complement the protection of intellectual property. Industrial property rights are recognized on the basis of an application filed Bureau of Industrial Property and give exclusive rights related to the subject matter of protection, while limits to the protection against unfair competition are not based on the recognition of the rights, but also of the view that acts contrary to good business practice should be banned. Protection against unfair competition relating to intellectual creations and commercial symbols, especially in the case of confusion, discrediting, misconceptions, while taking undue advantage and the use of undisclosed information. In this way, a competitive company or its activities, in particular, products or services that it offers, are being threatened.

INDIVIDUAL CRIMINAL OFFENSES AGAINST INTELLECTUAL PROPERTY RIGHTS

The offenses against intellectual property include: violation of moral rights of authors and performers, unauthorized use of copyright works or objects of related rights, unauthorized removal or alteration of electronic information on copyright and related rights, violation of patent rights and unauthorized utilization of design.

Violation of moral rights of authors and performers includes the full or partial disclosure, distribution of copies of someone else's work or interpretations of, or otherwise publicly disclosing someone else's copyright work or a performance by the perpetrator under his name or the name of another person. These persons without permission modify or process a copyright work or a recorded performance, or put into circulation copies of another's work or performance in a way which offends the honor or reputation of the author or artist. When unauthorized use of copyright works or objects of related rights, we recognize unauthorized disclosure, recording, copying, or otherwise publicly disclosing fully or partially copyright works, interpretations, phonograms, videograms, broadcasts, computer programs or databases, or marketing, or in order to put into circulation keeping the same object.

When we talk about the unauthorized removal or alteration of electronic information on copyright and related rights, we recognize the unauthorized removal or alteration of electronic information on copyright or related right, or marketing, importing, exporting, broadcast or otherwise publicly communicating copyright works or objects of related rights from which the electronic information on rights has illegally been removed or altered. In violation of patent rights offender unlawfully produces, imports, exports, offers for distribution, sells, stores or used in the course of trade a product or process is protected by patent. Unauthorized use of someone else's design, those who in their product in the market of unauthorized use, in whole or in part, another's registered or the protected product design.

Legal protection of intellectual property has become an important task, and compliance is an essential condition for the legitimate and proper business. It is obvious that we are talking about crimes with blanket norm, which is to say that it must have regard to the relevant legislation normally regulates some forms of intellectual property.[9] Protection of new ideas or maintain existing trade secrets is a very important part in modern business competitiveness. Innovation can be protected by being registered with the relevant institutions to guarantee the protection of intellectual property rights. Patents, trademarks, designs, geographical origin and new plant varieties with copyrights are examples of important rights that may prevent competition simply copied some new product or service. Trade secrets and know-how can also be protected through confidentiality agreements and contracts with employees. Effective protection of intellectual property rights contributes to economic growth, attracting investors and rounded framework necessary in the process of international integration.

INTELLECTUAL PROPERTY RIGHTS AND CYBER CRIME

In economic decision-making, we are often witnesses of counterfeit and pirated goods, which harms the holders of intellectual property rights, leading economic entities that operate legally in an unequal position, decrease of foreign investments, and in some cases, pose a serious threat to the health and safety of consumers . This type of goods in recent years is a global problem, but authorities to implement measures to protect intellectual property rights have a responsibility to prevent the unauthorized use of intellectual property rights and trade in goods that are subject to abuse these rights. In practice, the range of goods that counterfeits is very wide, so it falsifies everything from branded apparel and footwear, parts for technical equipment, toys for children, cosmetic products, medicines and food. Computer crime directed to intellectual property rights is widespread in a large scale in Serbia (especially the developed-piracy movie, music and software). In the area of intellectual property protection authorities should focus activity on the permanent control of the goods suspected of infringing

9 Чејовић, Б., Кулић М., Кривично право, Универзитет Привредна академија, Правни факултет за привреду и правосуђе, Нови Сад, 2014.

intellectual property rights, which are carried out at the request of copyright owner, as well as ex officio. Today, in the age of high technology, often is the way and manner of placement of goods and services that are incurred as a result of violations of intellectual property rights, accompanied by the abuse of computers which caused material or non-pecuniary damage to natural or legal persons. Disturbing the security of computer data and systems, or computer networks, for the purpose of abuse of intellectual property rights, in practice there are many obstacles in the timely detection and prosecution of perpetrators of this type of crime.

Data security is a specific segment. Today, the introduction of intellectual property rights in working life, a passage through the door of the world of computers. This is a good way to spread the business module, commercial profit, product placement and others. The largest number of criminal cases do employees within businesses, whose reporting is avoided. In the role of perpetrators of criminal offenses can be found clerks, cashiers, computer operators and managers. These are specific individuals, non-delinquent, socially adaptive and non-violent. It should also be noted that organized criminal groups particularly significant area becomes a digital economy and e-commerce.[10] Form cyber groups whose task is engaging in electronic legal and illegal markets, and the digital economy, in order to commit various types of fraud.

Intellectual property as the intellectual capital of its holder receives an absolutely new dimension with the development of the Internet. Cyber crime today has different forms in intellectual property. The perpetrators of these crimes intentional act with the intent to obtain an unlawful material benefit. The value of intellectual property is large, the Internet's potential is unlimited, and the power of computer technology is huge. Profit from cyber crime is big, a little risk. The highest price paid cybercrime companies and the national economy. Cyber crime has a negative impact on trade, competitiveness, innovation and global economic growth.

The preconditions for successful fight against computer crime directed towards the quality of intellectual property legislation, mobility IT personnel, associations, relevant government institutions, the study of comparative jurisprudence, and continuing education.

CONCLUSION

Intellectual property and business data are the most sensitive and most valuable company resources. They are exposed to various risks, are subject to a permanent loss and industrial espionage. Therefore, access to the segment of security and protection of computer systems has to be the most serious business. Systems are faced with contradictory demands, you need a quick and easy flow of information and security that is not compromised.

The criminal justice system of Republic of Serbia has introduced a number of criminal offenses and sanctions that are prescribed for certain forms and aspects of comitting computer crimes, modeled upon the Convention on Cybercrime[11] and other relevant EU documents. With the formation of special bodies for combating cyber crime within the police, public prosecutors and judges, conditions have been created to deal with it. Also certain criminal offenses against intellectual property are prescribed with appropriate sanctions for the perpetrators. However, the current situation is still unfavorable regarding the implementation of legislation in practice, because of the discrepancy between the legal and factual situation.

Criminal individuals, groups and organizations adapt to new social conditions using new crime techniques and methods, especially Internet, which is particularly evident in the abuse

10 Костић, М., Констатиновић-Вилић, С., Николић-Ристановић, Криминологија, Прометеј-Земун, 2011.
11 Incorporated into the law of the Republic of Serbia Law on Ratification of the Convention on Cybercrime, Службени гласник РС, бр.19/09

of intellectual property rights. Cybercrime in the field of intellectual property is characterized by unlimited distribution within the area of computer connections, detection of heavy and large material consequences.

The real volume of this type of crime remains unknown, since many abuses remain undetected, and they discovered unreported because of the potential negative labeling entity within which it was created. This type of crime is characterized by high dynamics and different forms of expression. Hazard its existence causes great economic damage scale, followed by a loss of business reputation, trust in the security of the computer business, comuter information, the risk of violations of fundamental rights and freedoms of natural persons, over breaches of rules of business practice for companies, compromising state.

The struggle in order to eliminate the crimes of intellectual property rights in the cyber crime represents joint force of IT personnel, specialized experts in intellectual property rights and legal experts for computer crime, with all relevant institutions at the local, national and international level.

REFERENCES

1. Алексић, Ж., Милосављевић З., Лексикон криминалистике, Београд, 1993.
2. Bowker, A., The Cybercrime Handbook for Community Corrections: Managing Risk in the 21th Century, Springfield Thomas, 2012.
3. Чејовић, Б., Кулић М., Кривично право, Универзитет Привредна академија, Правни факултет за привреду и правосуђе, Нови Сад, 2014.
4. Димитријевић, П., Право информационе технологије, Ниш, 2011.
5. Костић, М., Констатиновић-Вилић, С., Николић-Ристановић, Криминологија, Прометеј-Земун, 2011.
6. Martin, D., Martin F.P., Cybercrime, menaces vulnérabilités et rispostes, Paris, 2001.
7. Moore, R., Cyber crime: Investigating High- Tehnology Computer Crime, Cleveland, Mississippi, Anderson Publishing, 2005.
8. Матијашевић, Ј., Кривичноправна регулатива рачунарског криминалитета, Привредна академија, Нови Сад, 2013.
9. Петровић, С., Компјутерски криминалитет, Београд, 2000.
10. Стаменковић, Б., Високотехнолошки криминал- практични водич кроз савремено кривично право и примјере из праксе, Подгорица, 2014.
11. Субошић Д., Организација и послови полиције, Криминалистичко-полицијска академија, Београд, 2010.
12. Веиновић М., Милосављевић М., Грубер Г., Информатика, Универзитет Сингидунум, Београд 2009.
13. Водинелић, В., Методика откривања, разјашњења и доказивања рачунарског криминалитета, Загреб, 1990.
14. Warr., M., Companions in Crime, Cambridge, 2002.
15. Закон о потврђивању Конвенције о високотехнолошком криминалу, „Сл.гласник РС“, бр.19/09
16. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, „Сл.гласник РС“, бр.61/2005 и 104/2009
17. Кривични законик РС „Сл.гласник РС“, бр.85/2005, 88/2005-испр.107/2005-испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014

Topic VIII

INNOVATIVE TECHNIQUES AND EQUIPMENT IN FORENSIC ENGINEERING

UDC: 343.983:[502.175:543.95
502.175:502.51(497.11)

MICROBIAL ENVIRONMENTAL FORENSICS: MOLECULAR MICROBIOLOGY APPROACHES TO WATER SAFETY ISSUES IN THE REPUBLIC OF SERBIA

Smilja Teodorović, PhD[1]
Academy of Criminalistic and Police Studies, Belgrade
Bojana Vujović
Jaroslav Černi Institute for the Development of Water Resources, Belgrade
Vera Raičević, PhD
University of Belgrade, Faculty of Agriculture, Department of Microbial Ecology

Abstract: Environmental forensics is a field in which scientific methods are employed in order to identify potentially hazardous environmental contaminants and provide defensible evidence regarding the events surrounding the contaminant release in a regulatory and/or legal context. Microbial environmental forensics involves the application of microbiology to environmental forensics scenarios, with a goal of understanding release histories and sources of microbial contaminants in the environment, identifying responsibility of parties who released the contaminant, as well as responsibility for remediation, determining whether the contaminant caused harm, etc. According to the World Health Organization (WHO), unsafe drinking and recreational waters are a leading cause of preventable morbidity and mortality in humans. Therefore, the presence of pathogenic microbial contaminants in water inflicts immense risks for human health. Healthcare institutions represent specific indoor environments, in which drinking water is used daily for various purposes and where water-associated human pathogens have been implicated in healthcare-associated infections. Therefore, waterborne pathogen detection, molecular identification and genetic characterization represent an initial step in microbial environmental forensics. This work is, then, followed by microbial source tracking, that is, the discrimination between many possible sources of microbial contamination.

In efforts to learn about pathogen population distribution, structure, diversity, pathogenicity and source, we have analysed environmental samples throughout the Republic of Serbia. We have used molecular biology and bioinformatics tools to describe populations of an opportunistic human bacterial pathogen, *Pseudomonas aeruginosa,* and their relationship to clinical bacterial populations. Our future work will expand in the direction of a more specific assessment of interplay between environmental and clinical *P. aeruginosa* isolates in individual healthcare institutions in Serbia.

Keywords: forensics, microbial DNA analyses, waterborne pathogens, HAI.

INTRODUCTION

Water is essential for life. It is indispensable for drinking, swimming, recreation, domestic use, industrial use and irrigation. Quality of water has a major impact on human, but also animal and plant, health. However, estimates indicate that approximately 780 000 000 people worldwide lack access to safe water sources and about 2 500 000 000 to proper sanitation. As

1 smilja.teodorovic@kpa.edu.rs.

a consequence of inadequate protection of drinking water sources, unsafe water storage or inadequate hygiene, disease outbreaks occur. In addition, increased background morbidity rates for a prolonged period of time have also been attributed to water of poor quality. It has been proposed that access to safe water and improved hygiene and sanitation have the potential to prevent at least 9.1% of the global disease burden and 6.3% of all deaths[2]. However, despite the fact that majority of countries, including the Republic of Serbia, have adopted National Standards to regulate quality of various water types, over 800 000 deaths per year are still reported worldwide as a consequence of unsafe water supply, poor sanitation and hygiene.

The underlying causative agents of water-related human infections are pathogenic microorganisms. Most frequently, these pathogens spread through water contaminated with human or animal faces and cause diarrhoea. However, as indicated by the Center for Disease Control (CDC) in the United States (US), diarrheal disease is not the only risk to human health stemming from unsafe water, inadequate sanitation and insufficient hygiene practices. Specifically, environmental bacteria such as members of the *Pseudomonas* and *Aeromonas* genus, may cause skin infections in individuals with skin cuts or abrasions in recreational waters[3]. These infections can sometimes even be fatal.

An interesting and important aspect of drinking water exploitation is its daily use in healthcare facilities for hand washing, bathing, oral care, medical devices, etc., particularly in lieu of water microorganisms which may inflict disease in humans. In other words, healthcare institutions represent a unique ecosystem, comprising of the hospital environment, microorganisms, patient and hospital staff. Waterborne pathogens originating from water of inadequate quality have been implicated in healthcare-associated infections (HAIs)[4]. HAIs or nosocomial infections are infections of patients and hospital personnel acquired during the hospital stay, as a reaction to the presence of an infective agent or its toxins, which were not present prior to hospital admission. Numerous records indicate that HAIs have been recognized as early as 3000 B.C. by ancient Egyptians, later by Greeks and Romans, and through mid-19th century, when they conquered hospital surgical wards[5]. Today they occur in 5–10% of all patients, but are most commonly encountered in ones with weakened immune systems, such as patients in intensive care units (ICU). The most common causative agents of HAIs are *Staphylococcus aureus*, *Clostridium perfringes*, *Salmonella spp.*, *Escherichia coli*, *Candida*, *Enterococcus fecalis*, *Pseudomonas aeruginosa*, *Legionella sp.*, non-tuberculous *Mycobacteria* and others. In addition to increasing morbidity and mortality rates, these infections also increase the average length and cost of hospitalization. For instance, annual cost related to HAIs in the US is above 30 000 000 000 US dollars[6]. Between 1997 and 2007, 137 nosocomial epidemics have been reported in the Republic of Serbia, affecting a total of 2 308 patients[7]. One study investigated microbiological factors associated with blood nosocomial infections identified over a period of one year in a Serbian hospital. HAIs occurred at a 17.4 per 1000 admissions rate at an intensive care unit and were caused by coagulase negative *Staphylococci* (21.4%), *Staphylococcus aureus* (14.3%), *Klebsiella spp.* (13.3%), *Pseudomonas aeruginosa* (8.2%) and *Acinetobacter spp.* (7.1%)[8].

As stated above, many studies have linked HAIs with water quality. Though several Gram-negative pathogens have been found to persist in water systems, the association be-

2 Prüss-Üstün et al., 2008.
3 Pond, 2005.
4 Myers et al., 2014.
5 Prakash, 2011.
6 Scott, 2009.
7 http://www.blic.rs/vesti/drustvo/lece-jednu-a-zakace-drugu-bolest/5mrkg82.
8 Šuljagić and Mirović, 2006.

tween *P. aeruginosa* infections and water sources is best understood[9]. Here, we focus on this human pathogen in the context of environmental forensics.

DEFINING A PROBLEM: ROLE OF PSEUDOMONAS AERUGINOSA IN NOSOCOMIAL INFECTIONS

P. aeruginosa is an aerobic, rod-shaped, Gram-negative bacterium, commonly present in the environment (Figure 1). It infects animals, both invertebrates and vertebrates (including humans), primarily affecting immunocompromised individuals, hence the designation opportunistic pathogen. It does so by producing a large variety of extracellular toxins, including exotoxin A and enterotoxins, which are determining factors in bacteria's high virulence in a variety of different hosts[10]. In humans, *P. aeruginosa* infection is most often characterized by red, bumpy, itchy rash, which resembles measles[11], as well as swimmer's ear. However, more serious conditions in patients with weakened immune systems include pneumonia, breast inflammation, conjunctivitis, blood, bone and urinary tract infections, nausea, fever and chills[1213]. *P. aeruginosa* is a recognized cause of HAIs with potentially serious complications, such as colonization the lungs, urinary tract or kidneys[14]

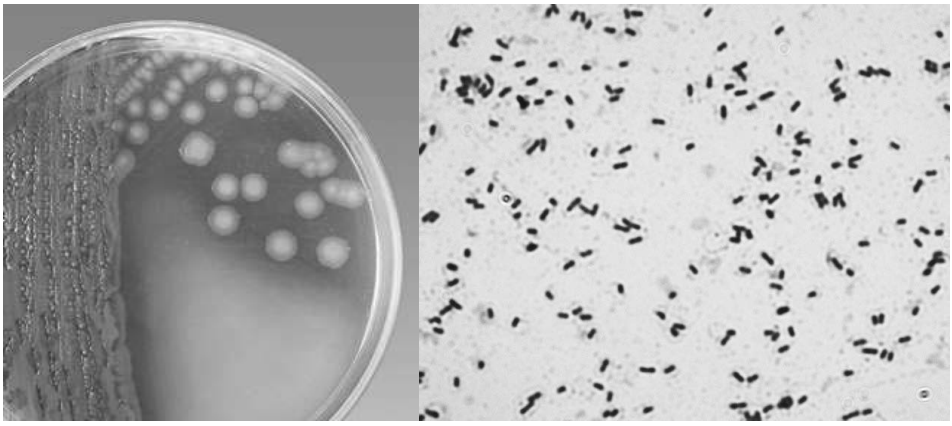


Figure 1: *P. aeruginosa colonies on Cetrimide agar (left) and Gram-negative rod cells under 1000x (right)*

P. aerugionsa is distributed worldwide and characterized by a remarkable ability to adapt to a variety of habitats. It thrives in soil, aquatic environments (streams, lakes, rivers, oceans), sewage, faeces, as well as in human skin and gastrointestinal tracts. It can multiply in water environments and also on the surface of suitable organic materials in contact with water. It has been isolated from a range of moist environments such as sinks, water baths, swimming pools, hot water systems, showers and spa pools. Besides the skin, nose, throat and faeces of infected individuals, *P. aeruginosa* can pass into water through broken pool-circulation pipes or from dirt tracked onto the deck, during certain irregular start-up procedures in water installations, etc. Also, it can survive in filter lines, garden hoses and lane lines coiled on

9 Cervia, 2012.
10 http://www.phac-aspc.gc.ca.
11 http://www.aquaticcouncil.com.
12 http://www.webmd.com/a-to-z-guides/pseudomonas-infection-topic-overview.
13 Djordjevic et al., 2013.
14 Bartram et al., 2003.

the deck[15]. *P. aeruginosa*'s persistence and durability in the environment, including drinking water supply systems and other water installations, are attributable to its ability to form so called biofilms, complex, slimy bacterial communities that adhere to a variety of surfaces. Once formed, these attached structures are very difficult to destroy, since bacterial cells in them are protected against chlorine and other disinfection agents. *P. aeruginosa's* presence in water reservoirs and other environmental habitats, including hospital systems, poses a significant threat to public health. There exists abundant evidence demonstrating the presence of *P. aeruginosa* in tap water used in the ICU and patient rooms. For example, a 2001 study found that 74% of taps without temperature selection were contaminated with *P. aeruginosa*[16]. A 2005 study demonstrated that 39% of water samples from electronic faucets in haematology units and ICUs yielded *P. aeruginosa*[17].

In HAIs, *P. aeruginosa* is predominantly encountered in ICUs, neonatal ICUs and burns units, where patients have immature or weakened immune systems and delicate skin. For instance, one study conducted in a University Clinical Center in Kragujevac, Serbia reported that *Pseudomonas* species were responsible for as high as 40% of nosocomial infections in surgery and intensive care wards[18]. Water point sources responsible for disease outbreaks may be taps that have not been used regularly, sink drains, water baths, devices (mechanical respiratory ventilators, catheters, incubators), equipment (needles, catheters, endoscopes), surgical instruments, hands of healthcare workers, feeding and mineral water bottles[1920]. The main route of infection is by exposure of susceptible tissue, notably wounds and mucous membranes, to contaminated water or surfaces. Cleaning of contact lenses with contaminated water can cause a form of keratitis. Ingestion of drinking-water is not an important source of infection.[21] *P. aeruginosa* has been found to survive within droplet nuclei and can remain in aerosols for long periods of time, thus there is evidence of potential airborne transmission.[22] Inhalation can occur through dispersed water from fountains, showers, cooling towers, air-conditioning units.

POSSIBLE SOLUTIONS: ENVIRONMENTAL FORENSICS APPROACH

Environmental forensics is a discipline in which scientific methods are employed in order to identify potentially hazardous environmental contaminants and provide defensible evidence regarding the events surrounding the contaminant release in a regulatory and/or legal context. More specifically, microbial environmental forensics involves the application of microbiology to environmental forensics scenarios, with a goal of understanding release histories and sources of microbial contaminants in the environment, identifying responsibility of parties who released the contaminant, as well as responsibility for remediation, determining whether the microorganism caused harm, etc. However, given that only a limited number of environmental microorganisms can successfully be cultured in the laboratory, microbial fo-

15 http://www.aquaticcouncil.com.
16 Halabi, M., Wiesholzer-Pitt, M., Schöberl, J., Mittermayer, H. (2001): Non-touch fittings in hospitals: a possible source of Pseudomonas aeruginosa and Legionella spp. J. Hosp Infect. 49(2):117-21.
17 Merrer et al., 2005.
18 Ilić and Marković-Denić, 2009.
19 Banerjee and Stableforth, 2010.
20 Subudhi, 2012.
21 de Victorica, J., Galván, M. (2001) Pseudomonas aeruginosa as an indicator of health risk in water for human consumption. Water Science and Technology, 43:49–52.
22 Clifton, I. J., Peckham, D. G. (2010): Defining routes of airborne transmission of *Pseudomonas aeruginosa* in people with cystic fibrosis. Expert Review of Respiratory Medicine, 4(4), 519-529.

rensics has not sufficiently been exploited in environmental forensics in the past. Nowadays, thanks to the development of an array of molecular biology techniques, analysis of microbial DNA is an indispensable tool in environmental forensics[23].

In the context of HAIs, the role of microbial environmental forensics is to identify microbial pollutants in the hospital environment, determine their origin(s), relationships, designate them as causative agent(s) of an infection of an individual or a group of individuals and infer about their transmission route. Contemporary approaches to solving this task involve DNA comparisons of related microbial strains and assessment of molecular variation between them. This can be achieved by methods such as DNA fingerprinting, molecular phylogeny, whole genome sequencing, etc.[2425] Specifically, there exists abundant evidence which links *P. aeruginosa* infections to tap water used in ICUs and patient rooms. A 2002 study used genetic techniques to demonstrate the epidemiological relationship between water isolates and patient infection with *P. aeruginosa*, concluding that faucets were the source of infection in 15 out of 45 patients[26]. A 2005 study investigated 132 cases of *P. aeruginosa* infections using genetic techniques to match strains causing illness to potential sources. Faucets in an ICU were linked to 42% of these cases[27]. A 2007 study used genetic-based epidemiological evidence linking *P. aeruginosa* with waterborne HAIs. Over a six-month period, 19 out of 38 patient infections were acquired via tap water or cross-transmission[28]. Another study reported *P. aeruginosa* responsible for the death of newborn baby due to respiratory and multiple organ failure caused by pneumonia and sepsis following a water birth[29]. Genetic and environmental evidence associated long or artificial fingernails in hospital nurses with *P. aeruginosa* colonization and suggested their role in a prolonged disease outbreak in a neonatal ICU[30].

It is clear that *P. aeruginosa*'s distribution, abundance, perseverance and pathogenicity demand the need to conduct its tight environmental control, including indoor environments such as healthcare facilities. Effective control is dependent on specific epidemiological knowledge, which can be gained through molecular typing methods, allowing for unique molecular signatures of individual bacterial isolates[31]. Multilocus Sequence Typing (MLST) is one of the techniques employed for molecular characterization of bacterial isolates. It is based on DNA sequence analysis of fragments of several housekeeping genes. MLST scheme for *P.aeruginosa* was developed in 2004[32], based on seven genes: *acsA*, *aroE*, *guaA*, *mutL*, *nuoD*, *ppsA* and *trpE*[33]. Its applications include epidemiological research and detection of *P. aeruginosa* transmission routes, as well as phylogenetic relationships between isolates[3435]. Within the MLST scheme, any level of nucleotide differences between isolates at each locus is designated as distinct allelic variant represented by a unique number. Each bacterial isolate is, thus, characterized by seven numbers which represent a sequence type (ST).

As a first step in microbial environmental forensics work, we have used molecular biology, bioinformatics and population genetics approaches to identify and characterize populations of *P. aeruginosa* from various habitats in the Republic of Serbia. Using a subset of five

23 Morrison and Marphy, 2010.
24 Grundmann et al., 1995.
25 Pattnaik and Jana, 2005.
26 Reuter et al., 2002.
27 Blanc et al., 2004.
28 Roques et al., 2007.
29 Byard and Zuccollo, 2010.
30 Moolenaar, 2000.
31 Xing, 2012.
32 Curran, 2004.
33 http://pubmlst.org/paeruginosa.
34 Curran, 2004.
35 Khan, 2008.

genes within the MLST scheme (*acsA*, *guaA*, *mutL*, *ppsA* and *trpE*), we have compared genetic make-up of thirty *P. aeruginosa* environmental isolates amongst each other, as well as to the *P. aeruginosa* isolated from diverse geographic backgrounds and habitats. Table 1 depicts results for three *P. aeruginosa* isolates from water samples in the Republic of Serbia, including affiliation to a specific ST. Additionally, results include other *P. aeruginosa* isolates from the MLST database which belong to the identical STs as each of the Serbian isolates. For instance, *P. aeruginosa* isolated from drinking water in Serbia is, per MLST, identical to isolates from sputum and blood, suggesting high genetic similarity between environmental (water) and clinical isolates.

Table 1: *Molecular characterization of P. aeruginosa from Serbian water samples and their relationship to clinical isolates*

Name	Locality	Water type	Allelic variants					ST	Isolates from MLST database with the same ST	Isolate origin
			acsA	guaA	mutL	ppsA	trpE			
BV1	Palic-Ludas channel	Surface water	11	6	18	15	19	487	PA0220	Sputum
									AUS672	Other
BV2	Belgrade	Surface water	16	30	11	20	7	555	HA_B2	Sputum
									AUS515	Other
									AUS695	Bronchial lavage
BV3	Belgrade	Drinking water	11	11	11	27	7	198	F1SIB1	Sputum
									PAamb243	Blood
									FQSE39-0910	Sputum

CONCLUSION

Bacterial detection, molecular identification and genetic characterization represent an initial step in microbial environmental forensics. Our investigations on environmental populations *of P. aeruginosa* in Serbia, assessing pathogen population distribution, structure, diversity and pathogenicity, allow us to make a connection between environmental and clinical *P. aerugionosa* populations. Following this work and using the established methodology, our efforts will focus on specifically accessing environmental and clinical isolates from hospital environments, in attempts to answer questions related to their interplay, sources of infection, cross-contamination, etc. Work on microbial source tracking in healthcare institutions will help us to advance our understanding in *P. aeruginosa*'s potential to cause HAIs in every-day hospital practice in the investigated region. This research is designed with an intention to play a role in the future development of improved control strategies and regulations governing the control of the bacterium that negatively impacts the environment and public health.

REFERENCES

1. Banerjee, D., Stableforth, D. (2000). The treatment of respiratory *Pseudomonas* infection in cystic fibrosis. *Drugs*, *60*(5), 1053–1064.
2. Banerjee, D., Stableforth, D. (2000): The treatment of respiratory pseudomonas infection in cystic fibrosis: what drug and which way? Drugs, 60(5), 1053–1064.
3. Bartram, J. et al., eds. (2003): Heterotrophic plate counts and drinking-water safety: the significance of HPCs for water quality and human health. WHO Emerging Issues in Water and Infectious Disease Series. London, IWA Publishing.
4. Blanc, D., Nahimana, C., Petignat, C., Wenger, A., Bille, J., Francioli, P. (2004): Faucets as a reservoir of endemic *Pseudomonas aeruginosa* colonization/infections in intensive care units. Intensive Care Medicine. 30:pp. 1964–1968.
5. Byard, R. W., Zuccollo, J. M. (2010). Forensic issues in cases of water birth fatalities. *The American journal of forensic medicine and pathology*, *31*(3), 258–260.
6. Cervia, J. (2012): Keeping afloat in a rising tide of waterborne HAIs: 8 Facts healthcare leaders must know. Infection Control Today (http://www.infectioncontroltoday.com/articles/2012).
7. Clifton, I. J., Peckham, D. G. (2010): Defining routes of airborne transmission of *Pseudomonas aeruginosa* in people with cystic fibrosis. Expert Review of Respiratory Medicine, 4(4), 519–529.
8. Curran, B., Jonas, D., Grundmann, H., Pitt, T., Dowson, C.G. (2004): Development of a Multilocus Sequence Typing Scheme for the Opportunistic Pathogen *Pseudomonas aeruginosa*. *Journal of Clinical Microbiology*. pp. 5644–5649.
9. de Victorica, J., Galván, M. (2001) *Pseudomonas aeruginosa* as an indicator of health risk in water for human consumption. Water Science and Technology, 43:49–52.
10. Djordjevic, Z., Folic, M. M., Zivic, Z., Markovic, V., Jankovic, S. M. (2013). Nosocomial urinary tract infections caused by *Pseudomonas aeruginosa* and *Acinetobacter* species: Sensitivity to antibiotics and risk factors. *American journal of infection control*, *41*(12), 1182–1187.
11. Douglas Scott II, CDC report, 2009, The DirecT MeDical cosTs of Healthcare-Associated Infections in U.S. Hospitals and the Benefits of Prevention.
12. Grundmann, H., Kropec, A., Hartung, d., Daschner, F.D., Pitt, T.L. (1995): Discriminatory power of three DNA-based typing tehniques for *Pseudomonas aeruginosa*. *J.Clin.Microbiol.* 33:528–534.
13. Halabi, M., Wiesholzer-Pitt, M., Schöberl, J., Mittermayer, H. (2001): Non-touch fittings in hospitals: a possible source of *Pseudomonas aeruginosa* and *Legionella* spp. J. Hosp Infect. 49(2):117–21.
14. Ilić, M., Marković-Denić, L. (2009). Nosocomial infections prevalence study in a Serbian university hospital. *Vojnosanitetski pregled*, *66*(11), 868–875.
15. Khan, N.H., Ashan, M., Yoshizawa, S., Hosoya, S., Yokota, A., Kogure, K. (2008): Multilocus Sequence Typing and Phylogenetic Analyses of Pseudomonas aeruginosa Isolates from the Ocean. *Applied and Environmental Microbiology*. 74, 20: 6194–6205.
16. Merrer, J. E., Girou, E., Ducellier, D., Clavreul, N., Cizeau, F., Legrand, P., Leneveu, M. (2005): Should electronic faucets be used in intensive care and hematology units? Intensive Care Med 31:1715–8.

17. Moolenaar, R. L., Crutcher, J. M., San Joaquin, V. H., Sewell, L. V., Hutwagner, L. C., Carson, L. A., Jarvis, W. R. (2000). A Prolonged Outbreak of *Pseudomonas Aeruginosa* in a Neonatal Intensive Care Unit Did Staff Fingernails Play a Role in Disease Transmission? *Infection Control & Hospital Epidemiology*, *21*(02), 80–85.
18. Morrison, R. D., Murphy, B. L. (2010). *Environmental forensics: contaminant specific guide*. Academic Press.
19. Myers, E. R., Carbone, H. L., Thompson, K. M., Hanlin, J. H. (2014): Managing the Risk of Waterborne HAIs. Infection Control Today (http://www.infectioncontroltoday.com).
20. Pattnaik, P., Jana, A. M. (2005). Microbial forensics: applications in bioterrorism. *Environmental Forensics*, *6*(2), 197–204.
21. Pond, K. (2005). *Water recreation and disease: plausibility of associated infections: acute effects, sequelae, and mortality*. World Health Organization.
22. Prakash, S. K. Nosocomial infection an overview. *Maulana Azad Medical College, New Delhi*.
23. Prüss-Üstün, A., Bos, R., Gore, F., Bartram, J. (2008): Safer water, better health: costs, benefits and sustainability of interventions to protect and promote health. World Health Organization, Geneva.
24. Public Health Agency of Canada (http://www.phac-aspc.gc.ca, www.publichealth.gc.ca)
25. Reuter, S., Sigge, A., Wiedeck, H., Trautmann, M. (2002): Analysis of transmission pathways of *Pseudomonas aeruginosa* between patients and tap water outlets. Crit Care Med. 30:2222-8.
26. Roques, A. M., Boulestreau, H., Lasheras, A., Boyer, A., Gruson, D., Merle, C., Castaing, Y., Bebear, C. M., Gachie, J. P. (2007): Contribution of tap water to patient colonization with *Pseudomonas aeruginosa* in a medical intensive care unit. J. Hosp. Infect. 67: 72–8.
27. Subudhi, C.P.K. (2012). *Pseudomonas aeruginosa* and hospital water systems [ppt]. Retrieved from www.healthprotectionsociety.org.uk.
28. Šuljagić, V., Mirović, V. (2006). Epidemiological characteristics of nosocomial bloodstream infections and their causes. *Vojnosanitetski pregled*, *63*(2), 124–131.
29. Xing, J., Yue, B. F., He, Z. M. (2012). Overview of Molecular Typing Methods for *Pseudomonas aeruginosa*. *Chinese Journal of Comparative Medicine*, *8*, 016.

UDC: 343.532
343.9.018

ANTI-COUNTERFEITING FOOD AND DRUG PACKAGING TECHNOLOGIES AND FORENSIC TOOLS: PRESENT STATE AND FUTURE TRENDS

Jelena Đuriš, PhD
University of Belgrade, Faculty of Pharmacy,
Department of Pharmaceutical Technology and Cosmetology
Bojana Vidović, PhD
University of Belgrade, Faculty of Pharmacy, Department of Bromatology
Bojan Čalija, PhD
University of Belgrade, Faculty of Pharmacy,
Department of Pharmaceutical Technology and Cosmetology
Nikola Milašinović, PhD[1]
Academy of Criminalistic and Police Studies, Belgrade

Abstract: Counterfeiting of food and drugs is an emerging issue, affecting worldwide public health and safety. State-of-the-art packaging technologies are one of the key factors in combating illicit food and drugs distribution. Many packaging options are available for safe authentication of the original products, including overt or visible features, covert or hidden markers, forensic markers and track and trace technologies. The most frequently used visible features are holograms, optically variable devices, protective inks and colour-changing films, watermarks, and high resolution printing markers such as guilloches. Apart from the protective features applied at the product package, it is also possible to mark individual product units (e.g. tablets) with the company logo or other symbols. Invisible features include various prints and images that can only be seen through special filters or under UV/IR light. Invisible digital watermarks and laser coding are also available. Some of invisible features may be added to the visible printing ink (e.g. microencapsulated scents). Forensic markers require specific laboratory techniques for authentication, ranging from chemical and biological analysis to specific DNA markers, isotopes and various types of micro-markers. Container serialization, bar codes (linear or data matrix) and specific markings on the container surface are used in order to be able to track and trace each individual product. Radio frequency identity tagging is a packaging feature used by some food and drugs manufacturers for secure tracking throughout the whole distribution chain. Suspect counterfeit food or drug products can be visually inspected by forensic microscopic techniques, or through qualitative and quantitative analysis of product such as FT-IR, MS, and Raman Spectroscopy, LC, UPLC, GC, and NMR. Rheological and thermal analysis of product may also be helpful to identify counterfeit products.

Keywords: food and drug authentication, packaging technologies, forensic techniques, anti-counterfeiting markers.

1 Corresponding author: nikola.milasinovic@kpa.edu.rs.

INTRODUCTION

The counterfeit products market is an increasingly serious global problem.[2] The evidence shows that ever-increasing products are being counterfeited, ranging from batteries, cosmetic and household products, to electronics goods, food and beverages, and medicines.[3] In addition to the economic losses to food and pharmaceutical industry, counterfeit food and medicines present serious public health problems.

According to the WHO definition, a medical product is counterfeit "*when there is a false representation in relation to its identity (e.g. any misleading statement with respect to name, composition, strength, or other elements), its history or source (e.g. any misleading statement with respect to manufacturer, country of manufacturing, country of origin, marketing authorization holder*)". Therefore, counterfeit drugs may include products with the correct ingredients or with the wrong ingredients, without active ingredients, with insufficient active ingredients or with fake packaging.[4] It is estimated that 10% of medicines around the world and 25% in less developed countries may be counterfeit. Consequently, the use of these products is associated with possible therapeutic failure or even potentially toxic effects and death.[5],[6] Recent evidence suggests that the most counterfeit drugs include anticancer, lipid lowering drugs, antihypertensive and anti-infective drugs, whereas previously counterfeit products had more to do with lifestyle drugs such as antiallergic and endocrine agents (such as hormones and steroids) as well as drugs for the treatment of erectile dysfunction. [7],[8]

Other types of products associated with counterfeit and resulting in a public health risk events include food, alcoholic beverages, coffee, spices and dietary products.[9] Lipton, Coca-Cola, and Nestlé products have been reported as some of the most counterfeited products found within the European Union. Also, products like condensed milk and mineral water are targeted by counterfeiters.[10] Organic food and food/herbal supplements are linked to possible counterfeiting concerns.[2]

2 Pollinger, Z.A., Counterfeit goods and their potential financing of international terrorism. The Michigan Journal of Business, 1(1):85-102, 2008.
3 2015 Situation Report on Counterfeiting in the European Union, Europol and the Office for Harmonization in the Internal Market, April 2015, p. 36.
4 Definitions of SSFFC Medical Products, available at: http://www.who.int/medicines/regulation/ssffc/definitions/en/.
5 Chika, A., Bello, S.O., Jimoh, A.O., Umar, M.T., The Menace of Fake Drugs: Consequences, Causes and Possible Solutions. Research Journal of Medical Sciences, 5(5):257-261, 2011.
6 Blackstone, E.A., Fuhr, J.P., Pociask, S., The Health and Economic Effects of Counterfeit Drugs. American Health & Drug Benefits, 7(4):216-224, 2014.
7 Sanofi-Aventis (2008), Press Pack: Drug Counterfeiting, available at: http://ec.europa.eu/internal_market/indprop/docs/conf2008/wilfried_roge_en.pdf.
8 Newton, P.N., M.D. Green, F.M. Fernandez, N.P.J. Day and N.J. White, Counterfeit anti- infective drugs. Lancet Infectious Diseases, 6:602-613, 2006.
9 Alocilja, E.C., NanoBio Sensors and Integrated Microsystems for Intelligent Food Packaging. 2009 Symposium on Nanomaterials for Flexible Packaging. Columbus, Ohio, USA.
10 Kerry, J., New Packaging Technologies, Materials and Formats for Fast-Moving Consumer Products. In: Innovations in Food Packaging. Han, J. (Ed.), Academic Press, Elsevier Ltd., London, United Kingdom, 2014.

Table 1: *The most commonly used anti-counterfeiting technologies*

OVER FEATURES	COVERT FEATURES	FORENSIC MARKERS	TRACK AND TRACE TECHNOLOGIES
Holograms	Invisible printing	DNA tagging	Serialization
Optically variable devices	Digital watermarks	Isotopic tags	Bar codes
Colour-shifting inks and films	Anti-copy or anti-scan features	Micro-markers	RFID tagging
Security graphics	Embedded images		Topography
Sequential product numbering			
On-product marking			

Rapid growth of cheap and low-quality counterfeit products has accelerated the rate of implementation of anti-counterfeiting technologies. State-of-the-art packaging technologies are one of the key factors in combating illicit food and drugs distribution. Some major technologies associated with anti-counterfeiting include overt/visible features, covert features, forensic and track and trace technologies (Table 1).[11]

OVERT (VISIBLE) FEATURES

As the name implies, overt technologies are visible by the naked eye, providing quick and easy visual authentication of products. However, their applying can increase the cost of production, consequently restrict supply availability and require the consumer training for effective authentication. Additionally, it should be mentioned that visible features only provide minimum security, since these can be faked by counterfeiters to result in confusion the customers. This demonstrates a need for their use in combination with other security features. Some popular overt technologies used in supply chains include holograms, optically variable devices, colour-shifting inks and films, security graphics, watermarks, and sequential product numbering.[12]

Holograms

Hologram presents a three-dimensional drawing that is the most widely used example of overt security technologies. Its visible effects can be seen easily by tilting or rotating the image, or by moving its position or the light source.[13] These security features are available in a variety formats such as: holographic shrink sleeves to protect branded bottled products against counterfeiting and refilling, blister packaging aluminium foil, pharmaceutical PVC, where the hologram is applied as a thin stripe to PVC sheets used to make blister packs, holographic induction cap seals, polyester-based tamper evident labels used to seal packages as well as holographic hot stamping foil where the hologram is fused to the host surface by heat and pressure.[14]

11 IMPACT Principles and Elements for National Legislation against Counterfeit Medical products: Text Endorsed by IMPACT General Meeting; International Medical Products Anti-Counterfeiting Taskforce, Lisbon, 2007, available at: http://www.who.int/impact/events/FinalPrinciplesforLegislation.pdf.
12 Power, G. Anticounterfeit technologies for the protection of medicines 2008, World Health Organization: Geneva, p. 13.
13 Davison, M., Pharmaceutical anti-counterfeiting: combating the real danger from fake drugs. Hoboken, New Jersey, John Wiley & Sons, Inc., 2011.
14 Deisingh, A.K., Pharmaceutical counterfeiting. Analyst, 130(3):271-279, 2005.

Optically variable devices

These security features are very similar to holograms, but without 3D illusion. They exhibit optical effects such as moving images or colour changes. Typically, they are composed of a transparent film as the image carrier on a reflective backing layer, usually a very thin layer of aluminium. For added security, it is possible to make the process of partial de-metallization, where some reflective layers are chemically removed to give an intricate outline to the image.[15]

Color-shifting inks and films

The colour-shifting optical effect is the result of a use of different colour combinations where the specific colours can be detected when viewed at different angles.[12] Due to limited and tightly controlled supply of the colour-shift inks, these overt technologies can be difficult to replicate. Pfizer was one of the first pharmaceutical companies to introduce a unique company logo on to the packaging of drugs using colour-shift ink (Figure 1).

Figure 1: *Anti-counterfeit measures for protection of one of Pfizer's most known brands, Viagra®*[16]

Security graphics

To increase security packaging features, guilloches (highly complex design pattern generated by mathematic formulas), line modulation and line emboss, may be used as a background in a discrete zone such as an overprint area, or as complete pack graphics.[12,17]

15 Patel, R. P., Patel, Y. B., Prajapati, B. G., Borkhataria, C.H., Outline of Pharmaceutical Packaging Technology. International Research Journal of Pharmacy, 1:105-112, 2010.
16 Available at: http://www.zdnet.com/pictures/photo-viagra-rfid-weeds-out-fakes/.
17 Zadbuke, N., Shahi, S., Gulecha, B., Padalkar, A., Thube, M., Recent trends and future of pharmaceutical packaging technology. Journal of Pharmacy & Bioallied Sciences, 5(2):98-110, 2013.

Sequential product numbering

This technology includes the use of unique sequential numbering of each label in a batch, which can make counterfeits easier to detect in the supply chain. The main disadvantages of this feature are that the sequence is predictable and easily replicated, and end users need some means of access to the database. The more secure option is serialization with a pseudo-random non-repeating sequence.[16]

On-product marking

For separate products from the original package, such as solid dosage forms, the effective security can be achieved by on-product marking with special images or codes.

COVERT SECURITY FEATURES

Unlike visible security features that are intended to help customers and non-specialists to easily recognize counterfeit food and drug products, cover (invisible) features are designed to assist the brand owners to identify counterfeited product and track legitimate medicines without discovery by counterfeiters.[18],[19] As the name indicates, these features are secret and can be discovered only through close observation or by using special filters and detectors.[20] Covert features which can be identified by simple, low-cost devices such as filters or lamps are sometimes referred as "semi-covert".[12] In that case, the term "covert" is used only for the features readable only by sophisticated laboratory instruments.[12] The main advantage of covert features is that they are hard to identify, and therefore, it is less expected that counterfeiters will fake them in comparison to the visible features. Besides, these features allow brand owners to identify counterfeit product and conduct an investigation without notifying supply chain stakeholders of the invisible anti-counterfeit feature.[12] Finally, these features can be easily added or modified in a way that does not affect design of packaging, which is important from the regulatory perspective.

A number of covert technologies are used nowadays in food and drug industry, each with its own advantages and drawbacks. Among the most commonly used covert technologies are: invisible printing, digital watermarks, anti-copy and anti-scan features, embedded images and laser coding.[21]

Invisible printing

This technology includes use of invisible inks that can be visualized under ultraviolet or infrared light. These special inks can be printed on primary or secondary packaging consisted

18 Perry, G., Wang, P.G., Wertheimer, A.I. Counterfeit Medicines Volume II Detection, Identification and Analysis - ILM Publication, 2013.
19 Siew, A., Anticounterfeiting Technologies: Tools to Combat Counterfeiters. Pharmaceutical Technology, 37, 2013.
20 Werblow, S., Anti-Counterfeiting Packaging. In: The Wiley Encyclopedia of Packaging Technology. Yam, K. (Ed.), Hoboken, New Jersey, John Wiley & Sons, Inc., 2009.
21 Kumar, A.K., Gupta, N.V., Lalasa, P., Sandhil, S. A. Review on Packaging Materials with Anti-Counterfeit, Tamper-Evident Features For Pharmaceuticals. International Journal of Drug Development and Research, 5(3):0975-9344, 2013.

of various materials and formulated to show different colours depending on the wavelength of light used for visualization.[16,20] Determination of spectral signature sometimes necessitates the use of specialized readers or instruments such as spectrophotometers.[19]

Digital watermarks

Invisible information can be digitally encrypted within graphics and placed on the packaging.[18,20] These information can be taken using cameras or scanners and decoded using special software programs.[18]

Anti-copy or anti-scan features

These features are intended to prevent unauthorized copying or scanning. They usually appear as uniform tones that reveal hidden images upon copying or scanning of packaging.[18]

Embedded images

Embedded images are images invisible to the naked eye, embedded within the graphic elements of the packaging.[20] These images can be revealed only by using special filters.

Laser coding

This technology is used to print recognizable and difficult to copy artefacts that may contain specific batch details.[18,20] The main advantages of this technology are: no ink consumption, coding process is fast, and the technology is clear and precise. Additionally, this technology is applicable to wide variety of packaging materials including paper, rubber, plastic, metal and glass. Nevertheless, the wide use of this technique is limited by the need for expensive equipment.

FORENSIC MARKERS

Forensic markers rely on chemical and biological parameters. They are neither visible to the naked eye nor by common analytical procedures. Chemical taggants are added to inks and result in characteristic peaks or chemical reactions. Biological markers can be incorporated into product formulation, coating or packaging.[22]

DNA tagging

Sophisticated anti-counterfeit labels can be produced using bioengineered DNA. DNA tagging is invisible and product specific and requires forensic level authentication.[9] It is therefore an extremely high counterfeit barrier, because the unique DNA sequence can never be

22 Sternberger-Rutzel, E., Combating the Counterfeiters. Contract Pharma, 2012, available at: http://www.contractpharma.com/issues/2012-04/view_features/combatting-the-counterfeiters.

replicated by a counterfeiter. DNA taggants are successfully used in the pharmaceutical, food and cosmetics industry.[23] Short synthetic DNA fragments, with a specific sequence of nucleotide bases, are included within the matrix of a label or security ink. Typically, the target DNA strand is detected by adding the opposite strand, which has a complementary sequence to the original and which has a fluorescent tag molecule that is activated when bound to another DNA strand.[12] A colour change in the DNA infused ink used for label printing can be induced by a simple wipe of the activation solution. This biochemical reaction only occurs in the presence of the DNA tag and cannot be replicated in a fake label product. Complete deciphering of DNA sequence requires laboratory analysis.[24] Biotechnology can be further coupled with the digital technology, by printing the barcodes using DNA-marked ink.[25] Similarly to DNA marking, antibody-based systems also rely on the recognition of specific chemical markers in the product sample.[12]

Isotopic tags

Isotopic tags are altered variants of common molecules already occurring in the product. The altered isotope composition gives the molecule a slightly different mass without altering the chemistry.[12] For example, stable isotope-labelled glucose was prepared, allowing differentiation between specific batches of granules and tablets. Products were analysed using mass spectrometry.[26]

Micro-markers

TruTag® microparticles are forensic markers that can be used for pharmaceuticals and food products authentication (Figure 2). They are manufactured starting from an inert excipient, silicon dioxide, which undergoes a specific process of association with an optical signature. TruTag® microparticles can be added to coatings and cores or be applied to the exterior of edible goods.[27]

Figure 2: *TruTag® spectral microtags for authentication and anti-counterfeiting*[28]

23 Applied DNA Sciences Launches DNA Taggant and On-Site Authentication for Pharmaceutics, 2014, available at: http://www.marketwired.com/press-release/applied-dna-sciences-launches-dna-taggant-on-site-authentication-pharmaceutics-nasdaq-apdn-2001421.htm.
24 Biowell unveils world's first DNA anti-counterfeit label, 2015, available at: http://biotecheast.com/modules.php?op=modload&name=News&file=article&sid=189.
25 DigitalDNA®, available at: http://www.adnas.com/products/digital-dna.
26 Felton, L.A., Shah, P.P., Sharp, Z., Atudorei, V., Timmins, G.S., Stable isotope-labeled excipients for drug product identification and counterfeit detection. Drug Development and Industrial Pharmacy, 37(1):88-92, 2011.
27 TruTag® Technologies Market Applications, available at: http://www.trutags.com/market-applications/.
28 TruTag® Video and Image Galery, available at: http://www.trutags.com/news/images/.

Microtrace Microtaggant® is a unique numeric code sequence represented by a multiple coloured layer particle format, ranging in size from 20 to 1200 microns. These markers can be used as dry powder to be incorporated into bulk materials, or they are incorporated into security inks, adhesives or labels. The information they contain is read using microscope, UV light or laser pen.[29] Furthermore, electrically active magnetic nanoparticles can be embedded in packaging materials. They are versatile and relatively simple to prepare and detect.[8]

There are several approaches to the concept of intelligent packaging, especially in the food industry, that contribute to assurance of the product safety and authenticity. These include time-temperature indicators, freshness indicators, gas indicators and various sensors.[8]

TRACK AND TRACE TECHNOLOGIES AND SERIALIZATION

Track and trace is the process of assigning a unique identity to each stock unit during manufacture which then remains with it throughout the supply chain until its consumption. Information is attached in the form of a unique pack coding, enabling access to the same information on a secure database.[30] Examples of track and trace systems are Pedigree used in United States[31] and mPedigree used in developing countries of Africa. Serialization includes the process of generating, encoding and verifying the unique identity of individual physical items/products[32], and is usually combined with track and trace technologies. Tracking of food and pharmaceutical products is achieved through incorporation of GS1 (Global Standards one) elements, such as serialized global trade item number (sGTIN) on the components of the packaging materials.[29] The main challenges of serialization implementation are the complexity of data that is to be tracked, and the need for potentially huge, multi-access databases.[33] For such purposes, graphical systems are used as common data carriers, including two-dimensional barcodes or quick response (QR) codes (Figure 3). Radio frequency identifier (RFID) uses radio wave technology to read, and in some cases write, information on printed chips that are placed on the product to be tracked.[12]

Figure 3: *RFID tag, barcodes and QR code*[34]

RFID tags can be passive or active, depending on the power supply and the level or response to electronic queries and signal transmittance. They can serve as tamper evident features or track and trace technologies.[19] QR codes can be printed over holograms or embedded into the hologram as an integral part of the overall holographic image (Figure 4).

29 Microtaggant® Identification Particles, available at: http://www.microtracesolutions.com/taggant-technologies/microtaggant-identification-particles.
30 Bansal, D., Malla, S., Gudala, K., Tiwari, P., Anti-Counterfeit Technologies: A Pharmaceutical Industry Perspective. Scientia Pharmaceutica, 81(1):1-13, 2013.
31 US Food and Drug Administration Prescription Drug Marketing Act – Pedigree Requirements under 21 CFR Part 203, available at: http://www.fda.gov/ohrms/dockets/98fr/06d-0226-gdl0001.pdf.
32 National Council for Prescription Drug Programs Drug pedigree in healthcare background, available at: http://www.ncpdp.org/members/wg17/201001227%20NCPDP%20%20Drug%20Pedigree-Background_v1.pdf.
33 Pharmaceutical Technology Europe Improving packaging security, available at: http://pharmtech.findpharma.com/pharmtech/article/articleDetail.jsp?id=718108.
34 Asset Management, available at: http://www.inspectall.com/features/asset-management.

Figure 4: *QR code embedded into the hologram (adapted from HoloQR™ technology)*[35]

Specific markings on the surface of the packaging materials (intervening lines or dots schemes) can also be used to track and trace batches of products. There are also examples of the packaging materials (plastics) having different roughness on the surface that can also be tailored to match specific batches.

Some companies use several approaches on the same product to prevent its counterfeiting. One of the most frequently adulterated Pfizer drugs, Viagra®, is protected by a visible feature (colour shift), 2D barcode and RFID tag (Figure 1).

The authentication companies, such as Authentix®, Food Marketing Institute, Grocery Manufacturers Association or Inmar provide brand protections in various fields of everyday life, from industrial, agricultural, food and pharmaceutical products, to healthcare and other adulteration issues. Figure 5 illustrates the legitimate supply chain and the parallel counterfeit supply chain, showing that leakage and counterfeit entry can happen at nearly any point.

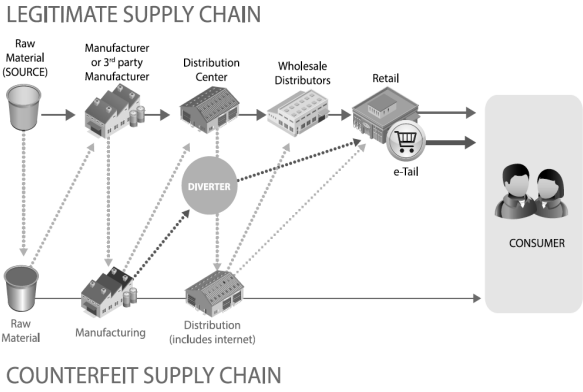


Figure 5: *Legitimate and counterfeit supply chain*[36]

Possible scenarios include a) direct online sales (as the fastest route from the counterfeiter to the consumer), b) suppliers counterfeiter that provide materials to manufacturers who create their branded products and sell them directly to retailers, c) counterfeit product may also find its way to the retailer by entering the supply chain through distributors, and/or d) counterfeit product may also move directly through the counterfeit supply chain to a diverter who sells directly to a retailer. However, there are many techniques that could be used to help to identify counterfeit products, and these will be discussed hereinafter.

35 Holoptica Pharmaceuticals, available at: http://holopticauk.com/pharmaceuticals/.
36 GMA/FMI Brand Protection Best Practices, available at: http://www.gmaonline.org/file-manager/Collaborating_with_Retailers/GMA_Inmar_Brand_Protection.pdf.

FORENSIC TECHNIQUES IN DISCOVERY OF COUNTERFEIT PRODUCTS

Counterfeit pharmaceutical and food products, usually of a poor quality, are a global health problem, particularly in low- and middle-income countries that have weak drug and food regulatory systems, having important health consequences. Moreover, the expanding international trade of agricultural and food products, enhanced production capabilities, but at the same time increased the production of counterfeit products. Food adulteration pose public health risks from ingestion and social risks from illness while diminishes confidence in the food supply. Atomic Force Microscopy[37], Colorimetry[38], High Pressure Liquid Chromatography[39], Thin Layer Chromatography[40], Fourier Transform Infrared Spectroscopy[41], Mass Spectrometry[13] and Raman Spectroscopy[42], Gas Chromatography[43], Nuclear Magnetic Resonance[44],[45], and Fluorescence[46], are among many techniques that could be used in identification of counterfeit products. Some of them, such are Colorimetry, HPLC, TLC or Raman Spectroscopy, are being rapid techniques while at the same time show high performances while keeping the cost as low as possible.[47] In addition to Raman Spectroscopy, DSC coupled with Raman facilitates the visualization and understanding of molecular manifestations underlying transient thermal transitions, such as polymorphic transformation of crystalline pharmaceuticals (Figure 6).

37 Lal, R., Ramachandran, S., Arnsdorf, M.F., Multidimensional atomic force microscopy: a versatile novel technology for nanopharmacology research. AAPS Journal, 12:716–728, 2010.
38 Green, M.D., Mount, D.L., Wirtz, R.A., Short communication: Authentication of artemether, artesunate and dihydroartemisinin antimalarial tablets using a simple colorimetric method. Tropical Medicine & International Health, 6:980–982, 2001.
39 Deconinck, E., Sacré, P.Y., Courselle, P., De Beer, J.O., Chromatography in the Detection and Characterization of Illegal Pharmaceutical Preparations. Journal of Chromatographic Science, 51(8):791-806, 2013.
40 Sherma, J., Analysis of counterfiet drugs by thin layer chromatography. Acta Chromatographica, 19:5-20, 2007.
41 Martino, R., Malet-Martino, M., Gilard, V., Balayssac, S., Counterfeit drugs: analytical techniques for their identification. Analytical and Bioanalytical Chemistry, 398:77-92, 2010.
42 Bate, R., Tren, R., Hess, K., Mooney, L., Porter, K., Pilot study comparing technologies to test for substandard drugs in field settings. African Journal of Pharmacy and Pharmacology, 3:165-170, 2009.
43 Ornelas-Soto, N., Barbosa-García, O., Lopez-de-Alba, P., Procedures of Food Quality Control: Analysis Methods, Sampling and Sample Pretreatment, In: Quality Control of Herbal Medicines and Related Areas, Shoyama, Y. (Ed.), ISBN: 978-953-307-682-9, InTech, DOI: 10.5772/23206, 2011.
44 Holzgrabe, U., Malet-Martino, M., Analytical challenges in drug counterfeiting and falsification-The NMR approach. Journal of Pharmaceutical and Biomedical Analysis, 55:679–687, 2011.
45 Savorani, F., Capozzi, F., Engelsen, S.B., Dell' Abate, M.T., Sequi, P.Pomodoro di Pachino: an authentication study using 1H NMR and chemometrics – protecting its P.G.I. European certification. In: Magnetic resonance in food science: challenges in a changing world. Guðjónsdóttir, M., Belton, P., Webb, G. (Ed.), Royal Society of Chemistry, 2009, pp. 158–166.
46 Da Silva Fernandes, R., da Costa, F.S.L., Valderrama, P., Marco, P.H., de Lima, K.M.G., Non-destructive detection of adulterated tablets of glibenclamide using NIR and solid-phase fluorescence spectroscopy and chemometric methods. Journal of Pharmaceutical and Biomedical Analysis, 66:85–90, 2012.
47 Kovacs, S., Hawes, S.E., Maley, S.N., Mosites, E., Wong, L., Stergachis, A., Technologies for Detecting Falsified and Substandard Drugs in Low and Middle-Income Countries. PLoS ONE, 9(3):e90601, 2014.

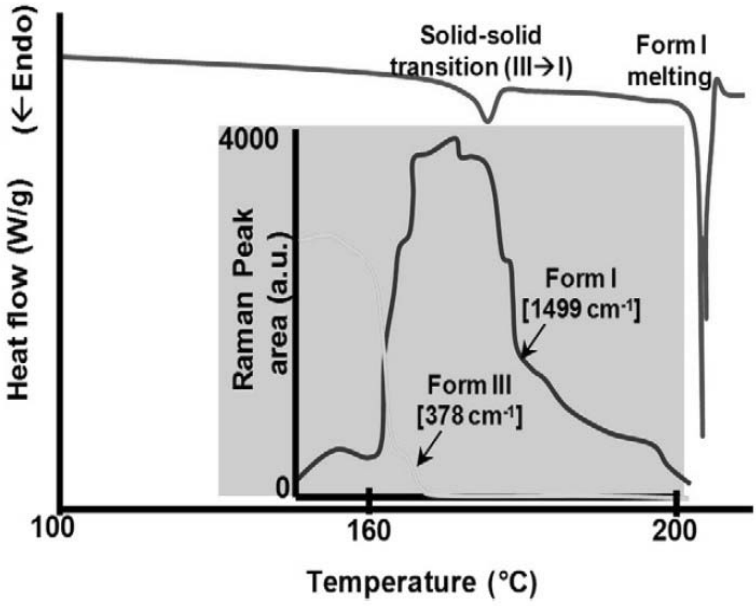


Figure 6: *DSC thermogram of sulfathiazole form III showing transition to form I and the subsequent melting event of form I. Inset shows the simultaneously measured Raman peak areas of corresponding polymorphs*[48]

Nevertheless, the triple quadrupole, ion trap and hybrid mass spectrometry (LC/MS/MS) offers tiered portfolios for both qualitative and quantitative product analysis across a broad range of markets including pharmaceutical, food safety, environmental and other markets. LC is a separation technique that analyses complex sample matrices in liquids. HPLC offers high throughput and sensitivity in the analysis of liquid samples. They could be used either in stand-alone configurations or as systems-integrated with mass spectrometers (LC-MS and LC-MS/MS). Nowadays there are nanoHPLC systems, typically used to separate components of very small biological samples for further analysis with ion trap or hybrid mass spectrometers in order to supports authenticity, safety and meat quality[49],[50] or various drugs and potential doping agents of black market products.[51] HPLC technique can be coupled with UV Spectrophotometry, hence becoming a strong tool for detecting pharmaceutical counterfeit products (Figure 7).

48 Paudel, A., Raijada, D., Rantanen, J., Raman spectroscopy in pharmaceutical product design. Advanced Drug Delivery Reviews, 89:3-20, 2015.
49 Method Development for Fake Lamb Meat Detection using LC-MSMS system, available at: http://sciex.com/Documents/posters/asms2015_73food_Guo.pdf.
50 Whitworth, J., LC-MS/MS method supports authenticity, safety and meat quality. Food Quality, 2015, available at: http://www.foodqualitynews.com/Lab-Technology/Method-using-SCIEX-QTRAP-6500-for-meat-contamination.
51 Krug, O., Thomas, A., Walpurgis, K., Piper, T., Sigmund, G., Schänzer, W., Laussmann, T., Thevis, M., Identification of black market products and potential doping agents in Germany 2010-2013. European Journal of Clinical Pharmacology, 70(11):1303-1311, 2014.

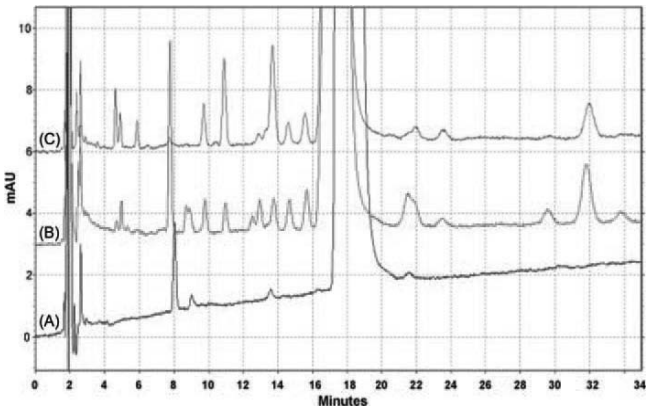


Figure 7: *HPLC–UV chromatograms of samples of tetrahydrolipstatin drugs*[38]

GC is a separation technique that analyses complex sample matrices in gases, comprising both separation and detection technology. Separation technology is common to all gas chromatography analysers, and is paired with either a conventional detector (GC) or with different types of mass spectrometers (GC-MS).[13,38]

Spectroscopic techniques are often preferred to chromatography for the identification of counterfeit products since they are fast, require less (or no) sample preparation and (some) are non-destructive. Among various techniques, FT-IR has demonstrated its usefulness to detect counterfeit or adulterated drugs. FT-IR and NMR are often used in the structure elucidation of active compounds or novel analogues found in illegal pharmaceutical preparations[38]. Figure 8 shows IR spectra of suspect tablet B-1 (a), suspect tablet B-2 (b), and authentic table B (c)

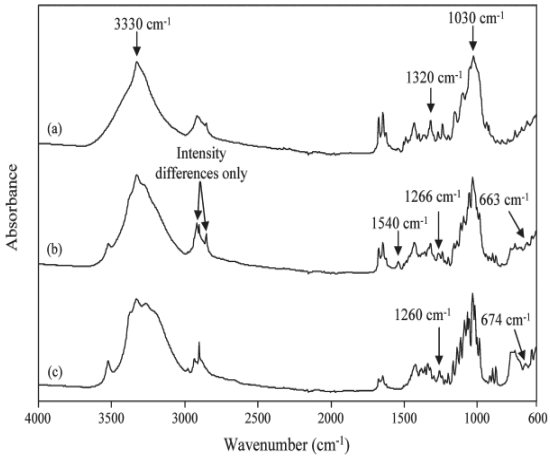


Figure 8: *Representative macro IR spectra of suspect tablet B-1 (a), suspect tablet B-2 (b), and authentic table B (c). The arrows indicate inconsistencies between the suspect tablets and authentic tablet B.*[52]

52 Lanzarotta, A., Lakes, K., Marcott, C.A., Witkowski, M.R., Sommer, A.J., Analysis of Counterfeit Pharmaceutical Tablet Cores Utilizing Macroscopic Infrared Spectroscopy and Infrared Spectroscopic Imaging. Analytical Chemistry, 83(15):5972–5978, 2011.

The elemental analysis, handheld elemental analysis, flat sheet thickness measurement, rheological and thermal analysis, contaminant detection in packaged materials and density measurement may be performed by various thermal techniques in order to detect counterfeit products as well.[53],[54]

Over the past several years European Union Customs reported a 200% increase in food-related counterfeit seizures. Anti-counterfeit Food Packaging Market is expected to reach $62.5 billion, globally, by 2020, as reported by Allied Market Research,[55] while MarketsandMarkets reported Anti-counterfeit Packaging Market by Technology (RFID, Coding & Printing, Holograms, Security Labels), usage Feature (Track & Trace, Tamper Evidence, Overt & Covert Features), End-Use (Food & Beverages, Pharmaceuticals, Automotive) is estimated to worth $153.95 billion.[56]

CONCLUSION

Counterfeiting of food or medicines represents a global issue affecting public health and safety worldwide. There are several approaches to protection of products authenticity, with the most of them being related to the products packaging. The prominent techniques include application of overt or visible features, covert or hidden markers, forensic markers and track and trace technologies. Multiple measures are sometimes taken to protect the integrity of a specified product supply chain. It is expected that more affordable packaging feature, but with the same level of safeness, will be developed in the future. Furthermore, it is expected that additional physicochemical techniques are used as forensic tools to detect counterfeit products.

REFERENCES

1. Alocilja, E.C., NanoBio Sensors and Integrated Microsystems for Intelligent Food Packaging. 2009 Symposium on Nanomaterials for Flexible Packaging. Columbus, Ohio, USA.
2. Applied DNA Sciences Launches DNA Taggant and On-Site Authentication for Pharmaceutics, available at: http://www.marketwired.com/press-release/applied-dna-sciences-launches-dna-taggant-on-site-authentication-pharmaceutics-nasdaq-apdn-2001421.htm.
3. Bansal, D., Malla, S., Gudala, K., Tiwari, P., Anti-Counterfeit Technologies: A Pharmaceutical Industry Perspective. Scientia Pharmaceutica, 81(1):1-13, 2013.
4. Bate, R., Tren, R., Hess, K., Mooney, L., Porter, K., Pilot study comparing technologies to test for substandard drugs in field settings. African Journal of Pharmacy and Pharmacology, 3:165-170, 2009.
5. Biowell unveils world's first DNA anti-counterfeit label, available at: http://biotecheast.com/modules.php?op=modload&name=News&file=article&sid=189.
6. Blackstone, E.A., Fuhr, J.P., Pociask, S., The Health and Economic Effects of Counterfeit Drugs. American Health & Drug Benefits, 7(4):216-224, 2014.
7. Chika, A., Bello, S.O., Jimoh, A.O., Umar, M.T., The Menace of Fake Drugs: Consequences, Causes and Possible Solutions. Research Journal of Medical Sciences, 5(5):257-261, 2011.

53 Thermal Analysis of Foods, available at: http://people.umass.edu/~mcclemen/581Thermal.html.
54 Padmanabhan, M., The application of rheological thermal analysis to foods. Proceedings of the 3rd International Symposium on Food Rheology and Structure. Laboratory of Food Process Engineering: ETH Zürich, Switzerland, 2003.
55 World Anti-counterfeit Packaging (Food and Beverages) Market - Opportunities and Forecasts, 2014 – 2020, available at: https://www.alliedmarketresearch.com/anti-counterfeit-packaging-food-beverages-market.
56 Markets And Markets Press Releases, available at: http://www.marketsandmarkets.com/PressReleases/anti-counterfeit-market.asp.

8. Da Silva Fernandes, R., da Costa, F.S.L., Valderrama, P., Marco, P.H., de Lima, K.M.G., Non-destructive detection of adulterated tablets of glibenclamide using NIR and solid-phase fluorescence spectroscopy and chemometric methods. Journal of Pharmaceutical and Biomedical Analysis, 66:85–90, 2012.
9. Davison, M., Pharmaceutical anti-counterfeiting: combating the real danger from fake drugs. Hoboken, New Jersey, John Wiley & Sons, Inc., 2011.
10. Deconinck, E., Sacré, P.Y., Courselle, P., De Beer, J.O., Chromatography in the Detection and Characterization of Illegal Pharmaceutical Preparations. Journal of Chromatographic Science, 51(8):791-806, 2013.
11. Deisingh, A.K., Pharmaceutical counterfeiting. Analyst, 130(3):271-279, 2005.
12. DigitalDNA®, available at: http://www.adnas.com/products/digital-dna.
13. Felton, L.A., Shah, P.P., Sharp, Z., Atudorei, V., Timmins, G.S., Stable isotope-labeled excipients for drug product identification and counterfeit detection. Drug Development and Industrial Pharmacy, 37(1):88–92, 2011.
14. Green, M.D., Mount, D.L., Wirtz, R.A., Short communication: Authentication of artemether, artesunate and dihydroartemisinin antimalarial tablets using a simple colorimetric method. Tropical Medicine & International Health, 6:980–982, 2001.
15. Holzgrabe, U., Malet-Martino, M., Analytical challenges in drug counterfeiting and falsification-The NMR approach. Journal of Pharmaceutical and Biomedical Analysis, 55:679–687, 2011.
16. IMPACT Principles and Elements for National Legislation against Counterfeit Medical products: Text Endorsed by IMPACT General Meeting; International Medical Products Anti-Counterfeiting Taskforce, Lisbon, 2007, available at: http://www.who.int/impact/events/FinalPrinciplesforLegislation.pdf.
17. Kerry, J., New Packaging Technologies, Materials and Formats for Fast-Moving Consumer Products. In: Innovations in Food Packaging. Han, J. (Ed.), Academic Press, Elsevier Ltd., London, United Kingdom, 2014.
18. Kovacs, S., Hawes, S.E., Maley, S.N., Mosites, E., Wong, L., Stergachis, A., Technologies for Detecting Falsified and Substandard Drugs in Low and Middle-Income Countries. PLoS ONE, 9(3):e90601, 2014.
19. Krug, O., Thomas, A., Walpurgis, K., Piper, T., Sigmund, G., Schänzer, W., Laussmann, T., Thevis, M., Identification of black market products and potential doping agents in Germany 2010-2013. European Journal of Clinical Pharmacology, 70(11):1303-1311, 2014.
20. Kumar, A.K., Gupta, N.V., Lalasa, P., Sandhil, S. A. Review on Packaging Materials with Anti-Counterfeit, Tamper-Evident Features For Pharmaceuticals. International Journal of Drug Development and Research, 5(3):0975-9344, 2013.
21. Lal, R., Ramachandran, S., Arnsdorf, M.F., Multidimensional atomic force microscopy: a versatile novel technology for nanopharmacology research. AAPS Journal, 12:716–728, 2010.
22. Lanzarotta, A., Lakes, K., Marcott, C.A., Witkowski, M.R., Sommer, A.J., Analysis of Counterfeit Pharmaceutical Tablet Cores Utilizing Macroscopic Infrared Spectroscopy and Infrared Spectroscopic Imaging. Analytical Chemistry, 83(15):5972–5978, 2011.
23. Markets And Markets Press Releases, available at: http://www.marketsandmarkets.com/PressReleases/anti-counterfeit-market.asp.
24. Martino, R., Malet-Martino, M., Gilard, V., Balayssac, S., Counterfeit drugs: analytical techniques for their identification. Analytical and Bioanalytical Chemistry, 398:77-92, 2010.
25. Method Development for Fake Lamb Meat Detection using LC-MSMS system, available at: http://sciex.com/Documents/posters/asms2015_73food_Guo.pdf.
26. Microtaggant® Identification Particles, available at: http://www.microtracesolutions.com/taggant-technologies/microtaggant-identification-particles.
27. National Council for Prescription Drug Programs Drug pedigree in healthcare background, available at: http://www.ncpdp.org/members/wg17/201001227%20NCPDP%20%20Drug%20Pedigree-Background_v1.pdf
28. Newton, P.N., M.D. Green, F.M. Fernandez, N.P.J. Day and N.J. White, Counterfeit anti-infective drugs. Lancet Infectious Diseases, 6:602-613, 2006.

29. Ornelas-Soto, N., Barbosa-García, O., Lopez-de-Alba, P., Procedures of Food Quality Control: Analysis Methods, Sampling and Sample Pretreatment, In: Quality Control of Herbal Medicines and Related Areas, Shoyama, Y. (Ed.), ISBN: 978-953-307-682-9, InTech, DOI: 10.5772/23206, 2011.
30. Padmanabhan, M., The application of rheological thermal analysis to foods. Proceedings of the 3rd International Symposium on Food Rheology and Structure. Laboratory of Food Process Engineering: ETH Zürich, Switzerland, 2003.
31. Patel, R. P., Patel, Y. B., Prajapati, B. G., Borkhataria, C.H., Outline of Pharmaceutical Packaging Technology. International Research Journal of Pharmacy, 1:105-112, 2010.
32. Paudel, A., Raijada, D., Rantanen, J., Raman spectroscopy in pharmaceutical product design. Advanced Drug Delivery Reviews, 89:3-20, 2015.
33. Perry, G., Wang, P.G., Wertheimer, A.I. Counterfeit Medicines Volume II Detection, Identification and Analysis - ILM Publication, 2013.
34. Pharmaceutical Technology Europe Improving packaging security, available at: http://pharmtech.findpharma.com/pharmtech/article/articleDetail.jsp?id=718108
35. Pollinger, Z.A., Counterfeit goods and their potential financing of international terrorism. The Michigan Journal of Business, 1(1):85-102, 2008.
36. Power, G. Anticounterfeit technologies for the protection of medicines 2008, World Health Organization: Geneva, p. 13.
37. Sanofi-Aventis (2008), Press Pack: Drug Counterfeiting. Available at: http://ec.europa.eu/internal_market/indprop/docs/conf2008/wilfried_roge_en.pdf.
38. Savorani, F., Capozzi, F., Engelsen, S.B., Dell' Abate, M.T., Sequi, P.Pomodoro di Pachino: an authentication study using 1H NMR and chemometrics – protecting its P.G.I. European certification. In: Magnetic resonance in food science: challenges in a changing world. Guðjónsdóttir, M., Belton, P., Webb, G. (Ed.), Royal Society of Chemistry, 2009. pp. 158–166.
39. Sherma, J., Analysis of counterfiet drugs by thin layer chromatography. Acta Chromatographica, 19:5-20, 2007.
40. Siew, A., Anticounterfeiting Technologies: Tools to Combat Counterfeiters. Pharmaceutical Technology, 37, 2013.
41. Situation Report on Counterfeiting in the European Union, Europol and the Office for Harmonization in the Internal Market, April 2015, p. 36.
42. Sternberger-Rutzel, E., Combating the Counterfeiters. Contract Pharma, 2012, available at: http://www.contractpharma.com/issues/2012-04/view_features/combatting-the-counterfeiters.
43. Thermal Analysis of Foods, available at: http://people.umass.edu/~mcclemen/581Thermal.html.
44. TruTag® Technologies Market Applications, available at: http://www.trutags.com/market-applications/.
45. US Food and Drug Administration Prescription Drug Marketing Act – Pedigree Requirements under 21 CFR Part 203, available at: http://www.fda.gov/ohrms/dockets/98fr/06d-0226-gdl0001.pdf.
46. Werblow, S., Anti-Counterfeiting Packaging. In: The Wiley Encyclopedia of Packaging Technology. Yam, K. (Ed.), Hoboken, New Jersey, John Wiley & Sons, Inc., 2009.
47. Whitworth, J., LC-MS/MS method supports authenticity, safety and meat quality. Food Quality, 2015, available at:http://www.foodqualitynews.com/Lab-Technology/Method-using-SCIEX-QTRAP-6500-for-meat-contamination.
48. World Anti-counterfeit Packaging (Food and Beverages) Market - Opportunities and Forecasts, 2014–2020, available at: https://www.alliedmarketresearch.com/anti-counterfeit-packaging-food-beverages-market.
49. Zadbuke, N., Shahi, S., Gulecha, B., Padalkar, A., Thube, M., Recent trends and future of pharmaceutical packaging technology. Journal of Pharmacy & Bioallied Sciences, 5(2):98–110, 2013.

UDC: 623.445:66.017

ANTI–BALLISTIC PROTECTION AS AN ASPECT OF CONTEMPORARY COMBATING TERRORISM

Marko Z. Ristić[1]
Radovan V. Radovanović, PhD[2]
Academy of Criminalistic and Police Studies, Belgrade
Bojan Ž. Janković, PhD[3]
University of Belgrade, Faculty of Physical Chemistry

Abstract: The problem of protection of humans by projectile firearms and explosive devices is old just as much as the man's knowledge about the possible harmful effects of firearms on living organisms. Awareness of the need to wear protective ballistic equipments has been evolving along with this knowledge. Personal protection against firearms is still a fundamental question of security. One of important aspects of anti–ballistic protection represents its technical and technological development. Nanotechnology can play a vital role in defence and space systems by minimising size, weight and power consumption that are important for long–range coverage. Within security system, levels incorporating the protection against lethal weapons, nanotechnology has an irreplaceable role in the development of anti–ballistic and shatterproof armour and advanced sensors. Therefore, these applications of nanotechnology are indispensable sub–units within defence forces of a country, including here equipment for the special police forces in order to suppress terrorist activities against civilians and objects. New nanocomposite should have higher impact resistance than present fibre composite systems and should have significantly reduced weight. The aim of this work is to summarize the results of the previous research in this field and through their critical analysis indicate the possible direction for further research in order to find optimal solutions that are required for people's safety.

Keywords: nanotechnology, anti–ballistic protection, technology developments, security

INTRODUCTION

With violent crimes on the rise, criminals have been steadily arming themselves with better and better ammunition and weaponry. Organised crime and terrorist networks are known to evolve rapidly, and to make the most of technological innovation. After the attack of September 11, 2001 in the USA it is clear that terrorists seek all available resources that can wreak enormous mess, confusion and chaos. The recent terrorist attack on November, 2015 in Paris, France is the logical consequence of such assaults. It is the job of police units and special police forces to stay ahead of this trend and therefore be better trained to protect civilians.

1 Corresponding author; Criminalist Specialist in Forensic Identifications, M.Sc. in Physical Chemistry, E–mail: markoffh@yahoo.com
2 Full Professor, Ph.D. in Mechanical Engineering, E–mail: radovan.radovanovic@kpa.edu.rs
3 Research Associate and Teaching Assistant, Ph.D. in Physical Chemistry, E–mail(s): bojanjan@ffh.bg.ac.rs; bojanjankovi78@gmail.com

The officials have been forced to provide the police officers and soldiers fighting terrorists with better equipment. Police officers that are assigned to the counter terrorism have special body armour needs. One of the most important pieces of the anti–ballistic protection equipment that can be issued to a police officer is his *personal body armour*.

During the past decades, police officers have complained that bullet–proof vests are uncomfortable, top heavy and hot. Some of the larger global bullet–proof vest companies (such as *Mehler Law Enforcement GmbH*[4]) have actually corrected these shortcomings through research and development, ensuring police officers feel more comfortable and therefore more willing to use the body armour every day.

LITERATURE SURVEY AND SOME IMPORTANT RESEARCH RESULTS

It is recommended that the SWAT (Special Weapons and Tactics) teams should wear overt vests of at least Protection Level III, which still protects against a large array of weaponry but it does not hinder movement. These vests have to be silent and manageable so the officer can move quickly and quietly to ensure hostage safety. There are various Protection Level III carriers that can be upgraded to level IV by adding hard protection plates.

The table below shows the qualitative evaluation of penetration three handgun grain models into the protective anti–ballistic equipment at different distances (Table 1).

Table 1: *Qualitative evaluation of penetration of protective ballistic equipment by some pistol grains*[5]

Protection Level	**7.62 mm M57**		**7.65 mm M70**		**9 mm CZ 99**	
	25 m	50 m	25 m	50 m	25 m	50 m
I	yes	yes	yes	yes	yes	yes
II	yes	yes	no	no	no	no
III	no	no	no	no	no	no

As it can be noticed from the presented table, bulletproof vests of Protection Level III (such as protective plates made from aluminum oxide or carbide) at a distances of 25 m and 50 m cannot break any of the considered pistol grains models.

The National Institute of Justice has modified the older ballistic standards 01.01.03 and 01.01.04 for testing of body armour. The new standard 01.01.06 is somewhat stricter. To meet the new standards, protective vests must have one of the four additional layers of Kevlar in comparison to those made under the old standard, when a vest had significant increase in weight. It should also be mentioned that the US security institutions allow the purchase of vests appropriate level of protection no matter by which standard they are made. However, despite all of this, it should be noted that the levels of protection on any of these standards are very high.

When the threat to rifle rounds increases, including armour–piercing projectiles (see Table 2, Types III and IV), ballistic fabric alone is insufficient. Stopping these threats requires

4 *http://www.m–l–e.de*
5 The table is formed by an image taken from Ref. [15]

adding a ceramic plate to the outside of the vest. The hard ceramic blunts and/or erodes the projectile nose, which increases the projected area of the projectile and spreads the load across more of the fabric.

Law enforcement officers that are assigned to counter terrorism have special body armour needs. For this type of task, an overt vest level III or IV with special emphasis on a carrier that includes tactical SAPI plates[6] is recommended. The new models are not only made of clay, but also of composite materials such as polyethylene. These plates will stop a high velocity M80 and 30 calibre bullets with a minimum velocity of 2850 feet per second (Table 2).

Table 2: *National Institute of Justice (NIJ) Ballistic Threat Standards*[7]

Protection Level	Projectile	Weight (g)	Velocity ($m \cdot s^{-1}$)	Kinetic Energy (Relative to Type IIA)
Type IIA	9 mm FMJ RN	8.0	373 ± 9.1	1.0
	40 S&W FMJ	11.7	352 ± 9.1	1.3
Type II	9 mm FMJ RN	8.0	398 ± 9.1	1.1
	357 magnum JSP	10.2	436 ± 9.1	1.7
Type IIIA	357 SIG FMJ FN	8.1	448 ± 9.1	1.5
	44 magnum SJHP	15.6	436 ± 9.1	2.7
Type III (Rifles)	7.62 mm FMJ*	9.6	847 ± 9.1	6.2
Type IV (AP Rifle)	30 cal.**	10.8	878 ± 9.1	7.5

Acronyms/Abbreviations:

FMJ RN = Full Metal Jacketed; JSP = Jacketed Soft Point; FN = Flat Nose;

RN = Round Nose; SJHP = Semi–Jacketed Hollow Point; AP = Armour–Piercing

* Steel–Jacketed Bullets, U.S. military designation M80

** AP Bullets, U.S. military designation M2 AP

The research in nanotechnology belongs to the one of the top five of the most expensive scientific programs in the world. In this regard, over 60 countries, including the Republic of Serbia, have launched their national nanotechnology programs. The discovery of new materials, processes and events at the nanoscale as well as permanent development of new experimental instrumental techniques for the study provides new opportunities for the development of innovative nanostructured materials. The constant development of new materials opens up completely new perspectives in many areas of technology and engineering (Figure 1). By using such powerful and lightweight materials with each other, even stronger and lighter composite material will be created, which will be able to completely replace traditional materials. The use of nanotechnology in the development and design of protective equipment will considerably enhance the performance of current materials, making them stronger and more resistant to deformation [17]. Thus, nanotechnology inventions have become a part of contemporary combating against crime and terrorism.

6 *http://www.bulletproofme.com/RP-Level-4-Stand-Alone.html*
7 The table were taken from Ref. [13]

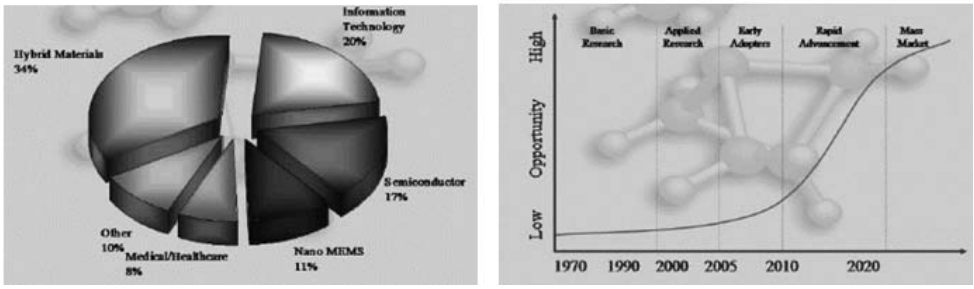


Figure 1: *Histogram of the current state (left) and evolution of nanotechnology with the tendency of development until 20208*

The potential applications of nanotechnology in the development of protective equipment are in the technology of artificial muscles and biocompatible tissues, light–weight bulletproof vests in the form of T–shirts, shields and blankets for protection against explosions. Thinner, lighter and more flexible materials with superior dynamic and mechanical properties are desirable for these applications. In particular, in making bulletproof vests, shields and blankets for protection against explosion, the best material with a high level of elasticity to cause rejection or diversion of projectiles from target specifically aimed at reducing injuries caused by use of firearms should be selected.

Since recently police and anti–terrorist units have found that fire resistant police clothing is of great importance, therefore the blue fire, cut and bullet–proof T–shirt carrier Nomex–Kevlar is developed by VBR–Belgium.[9] The new blue cut, fire and bullet–proof T–shirt carrier Nomex–Kevlar of VBR Belgium consists of a T–shirt which is providing front and rear stab protection and two bullet–proof packages NIJ–3A (04) of 250x300 mm have been processed. Therefore, it is ideal alternative to wearing a bullet–proof protection during the summer seasons.

The design of armour for personnel anti–ballistic protection depends on the specific threat. For fragments and lower velocity penetrators, vests are typically made from polymer fibres [16]. Advances in fibres for personnel armour began with the use of fibreglass and nylon. These were followed in the late 1960s by poly–aramid fibres (DuPont PRD 29 and PRD 49), now called *Kevlar*. Later, high molecular weight polyethylene fibres, made of *Spectra Shield* and *Dyneema*, were also used as backing in vests. *Zylon*, made of polybenzobisoxazole (PBO), has also been considered.

Figure 2 depicts how the evolution of fibres has steadily improved the performance of polymer vests. Thus, the primary factor in the design of armour for vests is the selection of the fibre.

8 The image was taken from: *http://www.directionsmag.com/entry/nanotechnology-and-the-fight-against-terrorism/123894*
9 *http://www.vbrbelgium.be/*

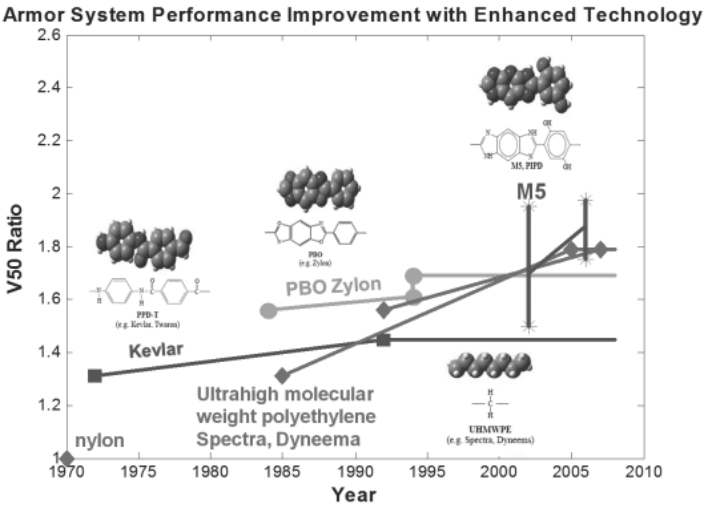


Figure 2: *Increase in ballistic performance as a function of improved fibres*[10],[11]

The central tasks of anti–ballistic protection are the absorption and the dissipation of energy caused by a ballistic impact. For this reason, bulletproof vests generally consist of a number of layers. Their fabrics or composite lay ups are made of yarns of high–performance fibres. The impact of a bullet makes the material absorb the kinetic energy–a handgun projectile travels at speed of 400 meter per second–thus stretching fibres and other stiff fibres which disperse the load over a large area throughout the material. This slows the bullet down and finally hinders it from penetrating the body.

Body armour designed specifically to defeat rifle fire has to be more rigid, because those projectiles travel at speeds of around 800 m a second. Therefore, besides the layers with fibres, hard materials such as ceramics or metal plates have to be inserted. The protective plates absorb and dissipate this greater kinetic energy upon impact and also the bullet itself gets blunted.

The two most critical factors for high performance fibres are therefore their strength and the level to which they can extend before fraction. During the last few decades, different chemical materials have been invented and constantly upgraded to achieve better effects. Today`s main high–performance fibres, Kevlar, Twaron, Dyneema and Spectra are based on the chemical bonds of para–aramid and high performance polyethylene.

Kevlar® is the trademark for aramid fibres, produced by US Company *DuPont*. Its *Kevlar*® KM2 technology is used in different armour applications, including the Interceptor body armour used by the US military. Kevlar has an equal weight basis to steel but is five times stronger, while being more flexible. The latest–development *Kevlar*® XP reduces potentially serious ballistic and trauma injuries due to its new structure. At the moment the company is researching a completely new high–performance fibre named M5, which is supposed to incorporate ultra–high strength as well as ultra–high thermal and flame resistance.

Aramid fibres include *Kevlar*® from *DuPont*, the tried and true material. *Twaron*® is the European version of aramid fabric. Both have the advantage of being more flexible for greater comfort. The polyethylene fibres include *Spectra*® by *Honeywell* or *Dyneema*® (by *DSM* in

10 This figure depicts how the V50 of fiber–based vests has increased as new fibres have been introduced over the years.

11 The image was taken from Ref. [14]

Europe) offer both advantages and disadvantages: ~25% lighter, better multiple hit and blunt trauma performance, but also ~20% more expensive and stiffer with a corresponding reduction in comfort.

Gold Flex® by *Honeywell* is a high–tech fibre made from aramid. It is ultra–light and ultra–thin, but also the most expensive. Most *Gold Flex*® bullet–proof vests are actually a blend of fibres to keep the cost down.[12]

M5 fibre is a high performance fibre originally developed by *Akzo Nobel* and currently produced by *Magellan Systems International*, but it is not yet commercially available. This PIPD[13] fibre is much anticipated and apparent likely contender in the anti–ballistic protection market. Tests by the US Army at the Natick Soldier Centre labs have indicated a very promising likelihood of success with this new high–strength polymer [20]. The M5 fibre polymer repeat unit is illustrated in Figure 3.

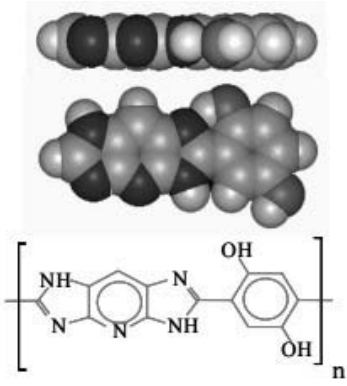


Figure 3: *Chemical structure of M5 fibre*[14]

The paper [3] was describes the potential of M5 fibre as an armour material and illustrates that potential by examining the ballistic impact response of composite materials which contain less than optimal M5 fibre from the early stages of the fibre development.

MODERN BODY ARMOURS

Modern body armour solutions are typically manufactured from ceramic, polycarbonate or aramid fibres, with each solution optimised to provide anti–ballistic protection against specific threats [10]. Traditionally, there has been a trade–off between the level of protection and the degree of mobility offered by body armour; a trade–off that is still apparent [6]. Advancements in body armour have led to the development of highly engineered, light–weight and *easy–to–put–on* solutions which offer anti–ballistic protection to vital organs situated within the torso [18] – an example also demonstrated within Figure 4. Such fibre–based solutions not only attempt to address the issue of comfort and freedom of movement, but also allow engineers to develop body armour capable of providing anti–ballistic protection against a myriad of threats.

12 *http://www.bulletproofme.com/How_to_Select_Body_Armor.shtml*
13 *poly{2,6–diimidazo[4,5–b4`,5`–e]pyridinylene–1,4(2,5–dihydroxy)–phenylene}*
14 The image was taken from: *http://www.m5fiber.com/magellan/m5_fiber.htm*

Figure 4: *Bullet/stab–proof vest*[15]

Not all aramid–fibre armours are capable of providing protection in sharp force events. The low–speed nature of stab incidents allows cutting weapons to push aside the aramid fibres which typically provide anti–ballistic protection. In order to provide protection against low–speed stab events, aramid fibres can be enhanced via methods such as:

- Carbon nanotube reinforcements;
- Incorporating discrete plates, and
- Thermoplastic impregnation.

The stab testing of a series of aramid fibre specimens featuring thermoplastic coatings to enhance stab resistance are shown in Figure 5:

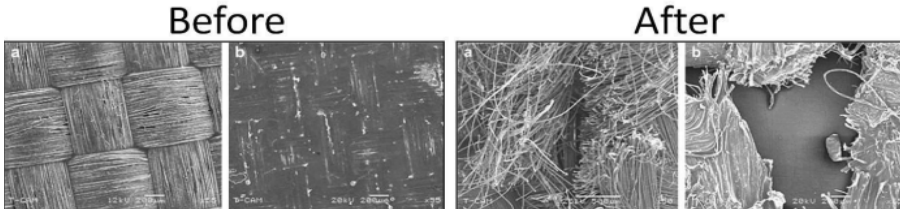


Figure 5: *SEM images of pre– and post–stab testing at an impact energy of 24,3 J; Kevlar™ (a) and Polyethylene (b) coated fabrics*[16]

A diagrammatic explanation of how the fibres, shown in Figure 5, behaved when under ballistic impact is shown in Figure 6.

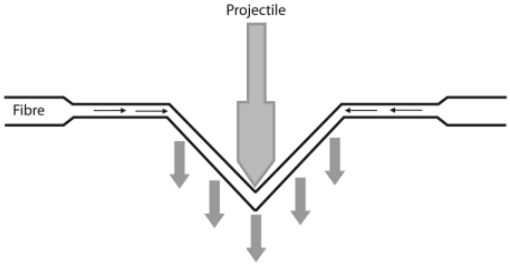


Figure 6: *Behaviour of an individual fibre when impacted by a projectile*[17]

High performance textiles allow individual yarns to stretch and break to efficiently and quickly absorb the impact energy from knife and ballistic missiles [18].

15 The image was taken from: *http://www.mensjournal.com/explosive-miler*
16 The image was taken from Ref. [11]
17 The image was taken from Ref. [18]

The purchasers and end–users of body armour require a balance between the level of protection and factors such as:

- *Mass* – Minimising and appropriately distributing across wearer.
- *Comfort* – Conforming to the wearers body and sufficiently breathable.
- *Mobility* – Flexible and must not impede movement.
- *Added Value* – Such as back support, quick release and add–on protection systems.
- *Durability* – Capable of withstanding typical environmental exposure and have an appropriate service life.

Through a series of interviews with serving British police officers, a range of issues have been highlighted which related to the use of body armour and the carriage of mandatory appointments, i.e. handcuffs and the radio. Such issues included:

1. Too much bulk, weight and a lack of flexibility.
2. Poor fitting – specifically female armour within the breast region, less muscle mass and smaller waists.
3. Restricted movement while detaining suspects and turning in vehicle.
4. Body armour riding up when seated – restricting breathing.
5. High thermal stress and poor ventilation – reducing the chase capacity of officers, and causing undergarments to be soaked with sweat.

The issues noted have the potential to impede the operational capabilities of police officers, as highlighted by a recent study investigating the impact of police body armour and associated equipment on officer mobility [5]. Police officers within the UK have also reported a number of significant physiological changes when wearing body armour ranging in mass from 2.9 to 6.2 kg, these include [9]:

- An increase in minute ventilation – the volume of air inhaled and exhaled.
- Reduced pulmonary function – how well gases circulate around the body.
- A reduction in forced vital capacity – the amount of air forcibly exhaled.
- Abnormal sensations, pain and decreased extremity movement likely caused by damaged nerves due to ill–fitting armour.
- An increase in skin temperature and heart rate.

The trade–off between protection and mobility continues to be present with modern body armour. The use of highly technical fibres has facilitated the development of flexible armour capable of providing protection against a range of ballistic threats. To provide protection, fibre–based body armour requires reinforcing which has shown to increase armour mass.

There is therefore a need for the development of a modern body armour solution capable of providing a level of protection found with the armour, which incorporates the flexibility demonstrated by fibre–based solutions.

BODY ARMOURS BASED ON CARBON NANOTUBES

Carbon nanotubes are “honeycomb” tube–shaped structures which are categorized as containing single, double or multiple walls. At a typical width of one ten thousandths the width of a single human hair, carbon nanotubes have demonstrated a number of benefits to their use over conventional materials, including:

- Greater electrical conductivity than copper;

- Improved thermal conductivity over diamond, and
- Better mechanical strength than high tensile steel.

Body armour incorporating carbon nanotubes have demonstrated greater energy absorbing characteristics over conventional technical fibre solutions. A diagram depicting the behaviour of a carbon nanotube under ballistic impact is shown in Figure 7.

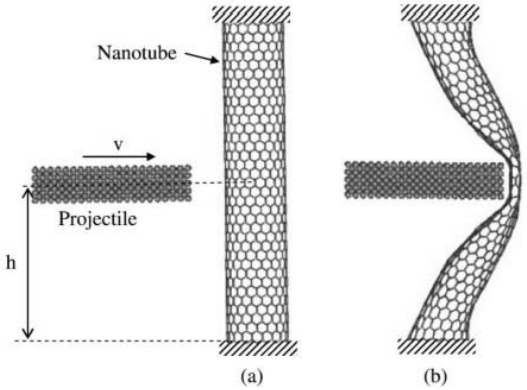


Figure 7: *Carbon nanotube behaviour (a) pre– and (b) post projectile impact*[18]

To facilitate the manufacture of textiles using carbon nanotubes, a number of developments have been made, including reducing the substrate temperature used to grow high–quality nanotubes[19]. By reducing the growth temperature from approximately 700°C to below 400°C, the process of generating nanocomposite materials for use within protective solutions was shown to be more feasible and financially viable [2]. It has been suggested that there is the potential to manufacture a 600μm thick carbon nanotube yarn based body armour that could provide sufficient protection anti–ballistic protection against a bullet with impact energy of 320 J [12].

In accordance with the above statements, the solution lies in the application of carbon nanotubes, a substance light as air, *stronger* than *Kevlar*, and capable of protecting one better in nearly every aspect. Unfortunately, carbon nanotubes are currently expensive to synthesize; the price per pound is often $1000 or more. It is often difficult to create long strands of nanotubes, as each nanotube is at most several hundred micrometers long.

To synthesize longer nanotubes, one must create smaller nanotubes and link them together to form the strands. To create these nanotubes, scientists have developed three main methods: *electric arc*, *laser ablation* and *chemical vapour deposition* (CVD). With a Young's modulus of nearly one TPa, strength of 13–53GPa, and a tensile strain failure of about 16%, carbon nanotubes are ideally suited for defence of the body from bullets and other things such a shrapnel from explosions. The nanotube specific energy absorption is *far higher* than any of currently used materials for bullet–proof armour, including *Kevlar* and PBO. Another quality of nanotubes is that they are *very hard*. If compressed correctly at a pressure of 24 GPa, one can synthesize a super–hard material with hardness of up to 152 GPa, which is harder than diamond at 140 GPa. Therefore, nanotubes would likely deflect, deform, or severely damage incoming projectiles.

18 The image was taken from Ref. [17]
19 *http://www.surrey.ac.uk/mediacentre/press/2011/45450_breakthrough_in_low_temperature_growth_of_carbon_nanotubes.htm*

BODY ARMOURS BASED ON SPECIFIC PHYSICAL PROPERTIES OF LIQUIDS

A number of government research laboratories, academic institutions and an array of defence technology companies have been investigating the generation of *liquid armour*[20]. The aim of such is to be fluid in its natural state and provide suitable anti–ballistic protection when a threat such as a ballistic projectile or knife blade is detected [16]. Liquid armour can typically be split into two groups:

- Magneto Rheological (MR) based, and
- Shear Thickening Fluid (STF) based.

Magneto Rheological based body armour comprises of a mix of iron particles and a non–magnetic viscous solution. Magneto Rheological Fluids (MRF) belongs to the class of the so–called fluids with controllable behaviour (or controlled fluids). A MR fluid is composed of dense micronic (range of 0.1–10μm) magnetic particles, held in suspension by a liquid medium (dispersion medium) of the lower density, typically an oil. When subjected to a magnetic field, the apparent viscosity of the fluid increases so much that it reaches a point where it behaves like a viscoelastic solid. Important to this behaviour is that the yield stress of the fluid in the active state can be precisely controlled by varying the intensity of applied magnetic field. Once they are magnetised, the iron particles attract one another to create dipole columns within 20 thousandths of a second [19]. This is depicted in the Figure 8 below.

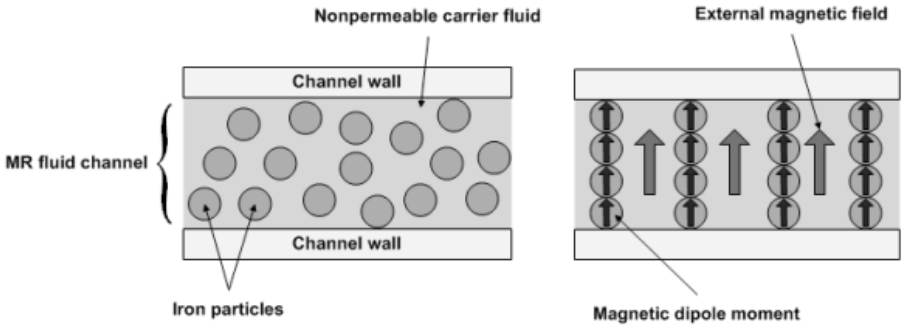


Figure 8: *Microstructures of MR fluids: (a) magnetic iron particles dispersed in nonmagnetic suspension (b) evolution of columnar structure under the application of an external magnetic field*[21]

The energy dissipation effects of MR impregnated Kevlar™ samples have been investigated for the incorporation into future body armour solutions. MR fluid was shown to occupy the space between the high strength Kevlar™ fibres, therefore once magnetised the fluid solidifies and increases the shear resistance of the armour–therefore enhancing energy absorption.

The practicality of Shear Thickening Fluid–based liquid armour has been heavily investigated by researchers at the US Army Research Laboratory [7]. Upon ballistic impact, the molecules within STF–based liquid armour lock together and harden to cause the impact force to be absorbed over a greater area than that compared to armour manufactured from traditional Kevlar™, as demonstrated in Figure 9.

20 *http://www.ccm.udel.edu/STF/contacts.html*
21 The image was taken from Ref. [19]

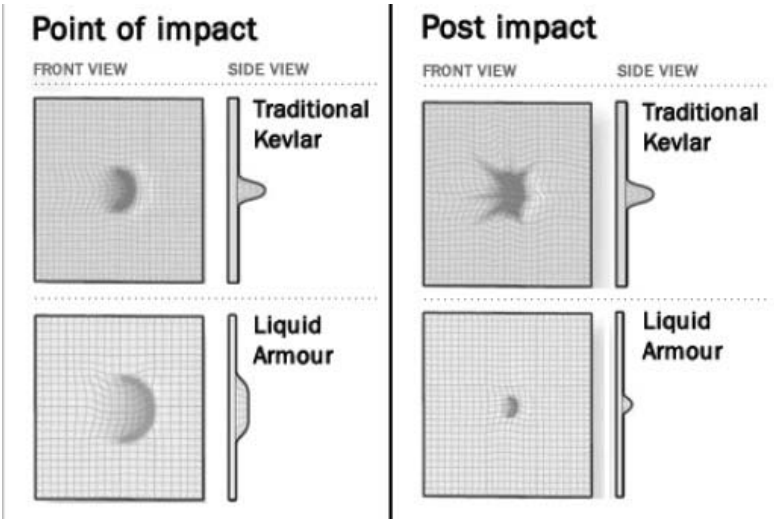


Figure 9: *The ballistic impact behaviour of traditional and STF based liquid armour*[22]

The enhanced behaviour of STF liquid armour may have the potential to reduce the risk of sustaining life threatening internal injuries.[23] Findings published by BAE Systems demonstrated that by impregnating Kevlar™ layers with STF, the number of layers to achieve a suitable level of protection against a ballistics round from a 9 mm, handgun was reduced from 31 traditional Kevlar™ layers to 10 STF impregnated layers. Such reduction in the number of Kevlar™ layers may potentially facilitate the development of armour that could have a significantly reduced mass and increased flexibility over traditional Kevlar™ based body armour.

The protective effectiveness of STF–based textiles against both stab and puncture threats has also been investigated [4.8]. As with ballistic testing, STF–based Kevlar™ fabric demonstrated significantly improved resistance – reducing the number of Kevlar™ layers down from 15 neat layers to 12 STF impregnated layers. It is understood that this enhancement was attributed to a reduction in the mobility of the Kevlar™ yarns – therefore preventing the stab or puncture threat from creating a window to penetrate the fabric [4]. The testing of STF impregnated nylon–fabric samples demonstrated, improved performance over neat alternatives and allows the low cost and more readily available STF–based fabrics [7].

CONCLUSION

The paper presents the most important issues in the field of new materials for personnel anti–ballistic protection for police and law enforcement purposes. The main items have been focused to torso armour, and body armour weight. The authors have come to a conclusion that the today's body armours appear to be more effective, especially on the direction of combating terrorism. Because of all that, this review paper provides a summary of current research in the field of technology development of bullet–proof vests with the primary aim of their innovative implementation in the police and security structures of the Republic of Serbia.

22 The image taken from: *https://www.baesystemseducationprogramme.com/what-is-engineering/liquid-armour.php*
23 *http://www.bbc.co.uk/news/10569761*

REFERENCES

1. Abrate, S. (ed.), *Impact Engineering of Composite Structure*, Springer Science & Business Media, 2011
2. Chen, G. *et al.*, Growth of carbon nanotubes at temperatures compatible with integrated circuit technologies, *Carbon*, Vol. 49, No. 1, 2011, pp. 280–285
3. Cunniff, P. M., Auerbach, M. A., High Performance M5 Fiber for Ballistics/Structural composites, *Course Mechanical Behavior of Polymers*, MIT, D. Roylance, 2005
4. Decker, M. *et al.*, Stab resistance of shear thickening fluid (STF)–treated fabrics, *Composites Science and Technology*, Vol. 67, No. 3–4, 2007, pp. 565–578
5. Dempsey, P., Handcock, P., Rehrer, N., Impact of police body armour and equipment on mobility, *Applied ergonomics*, 2013, pp. 1–5
6. Drain, J. *et al.*, Physical Mobility Implications of Torso Body Armour, *2nd International Congress on Soldiers' Physical Performance*, 2011, p. 179
7. Egres, R. G. Jr. *et al.*, Stab Resistance of Shear Thickening Fluid (STF)–Kevlar Composites for Body Armor Applications. *Proceedings of the 24th Army Science Conference*, Orlando, FL, 2004
8. Houghton, J. *et al.*, Hypodermic Needle Puncture of Shear Thickening Fluid (STF)–Treated Fabrics, *Society for the Advancement of Material and Process Engineering*, 2007.
9. Konitzer, L. *et al.*, Association between back, neck and upper extremity musculoskeletal pain and the individual body armor, *Journal of hand therapy: Official Journal of the American Society of Hand Therapists*, Vol. 21, No. 2, 2008, pp. 143–8; quiz 149
10. Levinsky, A., Sapozhnikov, S., Grass, T., Development of knife– and bullet–impact–resistant composite structures, *Mechanics of Composite Materials*, Vol. 48, No. 4, 2012, pp. 405–414
11. Mayo, J. Jr., *et al.*, Stab and puncture characterization of thermoplastic–impregnated aramid fabrics, *International Journal of Impact Engineering*, Vol. 36, No. 9, 2009, pp. 1095–1105
12. Mylvaganam, K., Zhang, L., Ballistic resistance capacity of carbon nanotubes, *Nanotechnology*, Vol. 18, No. 47, 2007
13. National Institute of Justice, *Selection and Application Guide 0101.06 to Ballistic–Resistant Body Armor For Law Enforcement, Corrections and Public Safety*, NCJ 247281, December 2014.
14. *Opportunities in Protection Materials Science and Technology for Future Army Applications*, Committee on Opportunities in Protection Materials Science and Technology for Future Army Applications, National Research Council of The National Academies Press, Washington DC, 2011, p. 16
15. Radovanovic, R., Ristic, M., Milic, J., Forensic significance in determining the parameters of action of pistols projectiles. In Lj. Maskovic (ed.), *Criminalistics and forensic processing of crime scenes events*: *Thematic Proceedings II*, Academy of Criminalistic and Police Studies, Belgrade, 2014, pp. 149–162, (published in Serbian language)
16. Radovanović, R., Ristić, M., Milić, J., Protective Ballistic Equipment–Forensic Engineering Aspects. In D. Kolarić *et al.* (eds.), *5th International Scientific Conference "Archibald Reiss Days": Thematic Proceedings of International Significance, Vol. 3*, Academy of Criminalistic and Police Studies, Belgrade, 2015, pp. 341–52
17. Ristic, M., Milic, J., The use of nanotechnology in the development of protective equipment. In D. Kolaric (ed.), *6th Scientific and Professional Conference with International Participation "Countering Contemporary Forms of Crime Analysis of the Current Situation, European Standards and Measures for Improvement", Tara, May 26–29, 2015: Proceedings, Vol. 3*, Academy of Criminalistic and Police Studies and the Hanns Seidel Foundation, Belgrade, 2015, pp. 447–460 (published in Serbian language)
18. Scott, R., *Textiles for protection*, Woodhead Publishing Limited, Cambridge, 2005
19. Son, K. J., *Impact Dynamics of Magnetorheological Fluid Saturated Kevlar and Magnetostrictive Composite Coated Kevlar*, University of Texas, Austin, 2009
20. Wilusz, E. (Ed.), *Military textiles*, Woodhead Publishing in Textiles, 2008

UDC: 351.75:004.932.2

SHADOW REMOVAL OF MOVING OBJECT FOR VIDEO MONITORING SYSTEMS

Feng Xu, PhD[1]
National Police University of China,
Department of Forensic Science and Technology, Shenyang

Abstract: In recent years, video surveillance has become more and more important for enhanced security and it is indispensable technology for fighting against all types of crime with the construction of sky-net in China. Shadow elimination is the research focus of moving target tracking and detection in the current research of intelligent monitoring. However, shadows extracted along with the objects can result in large errors in object localization and recognition. In this paper, the author proposes an improved method of moving shadow detection and elimination based on HSV colour space according to the actual situation of public security work. First, noise interference is eliminated by the pre-treatment for the sequence image. Then the shadow can be detect and eliminated in HSV colour space according to the characteristics of hue and luminance. Finally, the missing edge contour can be filled using morphological corrosion and expansion algorithm. Experimental results show that the proposed method can effectively eliminate the shadow and provide a more complete outline; it has better real-time performance and robustness.

Keywords: intelligent monitoring, shadow, HSV colour space, morphology.

INTRODUCTION

With the rapid development of video monitoring system in China in recent years, the video investigation has become an important tool to combat crime and it plays an increasingly important role in criminal detection and law enforcement. With the development of sky-net project, the surveillance system has been spread all over the roads, key departments, case prone areas, public areas and densely populated areas. The improvement of the efficiency and scope of video data is an important task at present. Intelligent monitoring technology can maximize the use of key information in video surveillance, automatically recognize object, detect and alarm emergency situations and record the related information. It is the forefront research in the field of video surveillance because it can help investigators in dealing with variety of unexpected situation without increasing the manpower and material resources.

The research contents of intelligent monitoring technology mainly includes the following three aspects: moving object detection, object tracking and behaviour analysis. The moving target detection is the basis of the analysis of target tracking and behaviour. It will produce obvious shadow region when the target motion is illuminated by light in practical application process. If one does not consider the effect of shadow, it usually causes multiple targets in one, false target, target shape distortion, even missing the target in the serious situation and can directly affect the results of subsequent processing. Therefore, the detection and elimination of shadow in moving object detection is of crucial importance and must not be ignored.

1 E-mail: xufeng_ccpc@hotmail.com.

OVERVIEW OF SHADOW ELIMINATION ALGORITHM

Detection of moving objects in dynamic sequence is at the core of many computer vision applications, including video surveillance, people tracking, traffic monitoring, video coding, etc. In these applications, an effective and efficient background subtraction is critical. A commonly used approach is to detect moving object pixels by using Gaussian mixture model[2]. However, the current techniques typically ignore the misclassification of shadows as moving objects due to some important visual features, which can cause serious problems while segmenting and extracting moving objects. Since shadow points are usually adjacent to object points, shadows and moving objects may be merged into a single blob with the commonly used segmentation techniques. Moreover, shadows can cause object distortion and affect all the measured geometrical properties, such as the assessment of moving object position, analysis of the behaviours of objects, and recognition of objects. For these reasons, shadow identification and removal is vital for dynamic sequence and has become an active research area[3].

Shadows are the result of the partial or whole occlusion of light ray on its way to background from the light source to an object in the scene. In particular, the dark regions on the background are called cast shadows, which consist of a centre part without light from light source, called umbra, and a soft transition from dark to bright, called penumbra, where some light from the light source reaches the background[4]. Based on the definition, many solutions have been proposed to identify shadow pixels from moving object pixels.

According to spectral features, shadow detection techniques can be roughly divided into two classes: intensity based and Chroma city-based techniques. Intensity-based techniques rely on grey levels of monochromatic images which aim at exploiting edge/texture information[5] or building shadow models based on statistical learning process[6] for shadow detection.

Since shadow regions in the current image contain the same textural information as corresponding regions in the background image, shadow identification can be performed according to texture/edge detection. Usually, edges in the background image are static, which can be used to improve the reliability of results. Stauder et al. detected shadows based on an algorithm for segmentation of moving objects under the assumption that moving shadows were cast on the background of the scene. The changed regions from frame to frame caused by moving cast shadows were based on four assumptions, which led to four criteria. Especially, the edge information was employed for detecting likely shadow boundaries while the frame ratio was evaluated inside the change detection mask. Results showed that it was applicable for restricted indoor environments and only for one moving person. Moreover, the computation was quite expensive. Xu et al.[7] proposed an effective approach for the detection and removal of insignificance shadows, which was especially appropriate for the applications of indoor video surveillance and conferencing. In particular, edge information, i.e., canny edge detection, edge extraction and edge matching, was employed to detect the boundaries of moving objects and shadows. Some complex filling algorithms were applied to connect edge

2 Stauffer C, Grimson W e l. Adaptive background mixture models for real-time tracking. IEEE Computer Society Conference on Computer Vision and Pattern Recognition.
3 Prati A., Mikic I., Trivedi M. M., Cucchiara R. Detecting moving shadows: algorithms and evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence.
4 Stauder J., Mech R., Ostermann J. Detection of moving cast shadows for object segmentation. IEEE Transactions on Multimedia.
5 Fung G. S. K., Yung N. H. N., Pang G. K. H., Lai A. H. S. Effective moving cast shadow detection for monocular color traffic image sequences. Optical Engineering.
6 Hsieh Jun-Wei, Yu Shih-Hao, Chen Yung-Sheng, Hu Wen-Fong. Automatic traffic surveillance system for vehicle tracking and classification. IEEE Transactions on Intelligent Transportation Systems.
7 XU Dong, LI Xue-Long, LIU Zheng-Kai, YUAN Yuan. Cast shadow detection in video segmentation. Pattern Recognition Letters.

information to generate final object masks. As an extension of the previous literature, the same authors successfully separated moving foreground objects from its cast shadow regions by a region growing scheme. Li et al.[8] modelled each pixel as a kernel density estimation based on gradient features under grey levels, instead of colour space, which can suppress shadows as well as reflections. Although fake moving objects suppression was remarkable, a weakness of the method was to cause the increase of the false negative rate.

On the other hand, probability models provide a natural tool for dealing with uncertainty and complexity through spatial, temporal information or the combination of them. Due to the difference between moving shadow pixels and foreground object pixels, shadows can be characterized by some inherent statistical properties. Wang[9] proposed a probabilistic approach for foreground and shadow segmentation based on Markov random field and Bayesian network, which combined background, intensity and edge information. Later, a dynamic conditional random field model[10], which differed from the above-mentioned model, was proposed based on spatial and temporal dependencies by the same author. The results showed that the two methods greatly improved the accuracy of segmentation for foreground objects and moving cast shadows. Analogously, a single Gaussian model for shadow pixels as employed together with geometrical features, which performed well. However, due to the only use of luminance information, these methods tended to be less accurate while thresholds should be pre-prepared for the classification of moving shadow pixels and foreground object pixels. Furthermore, since the computational load was increased, it was complex to be integrated into the real-time system.

Besides, the orientation, size and even shape of shadows may be exploited according to proper prior knowledge of illumination source, object shape and ground plane. However, these techniques were strongly restricted to particular object type, such as pedestrians and vehicles. Shadows from various pedestrians were considered as a Gaussian model[11]. Based on conditional random field, a probabilistic discriminative framework was formulated by using spatial and temporal dependencies in traffic scenes. Spectral and geometrical properties of shadows were also exploited.

Another class of techniques is to employ colour information in different colour spaces for shadow identification and removal. Cucchiara et al.[12] exploited shadow properties in the hue, saturation and value (HSV) colour space to discriminate shadow pixels from moving object pixels. These properties showed that cast shadows darken the background in the luminance component, while the hue and saturation components changed within certain limits. Similarly, photometric invariant colour features defined by Salvador et al.[13] were expected to be constants for corresponding pixels in current image and background image. For practical applications, these features were permitted to change with certain range. The spectral properties can be used to extract shadows along with inherent geometrical constrains. For the selection of appropriate colour spaces, Benedek and Sziranyi compared several well-known colour spaces with six-parameter shadow model embedded into a globally optimal MRF framework. The limitation of these methods was that thresholds must be explicitly tuned for each scene.

8 LI Zheng, JIANG Po-Huang, Mab Hong, YANG Jian, TANG Dong-Ming. A model for dynamic object segmentation with kernel density estimation based on gradient features. Image and Vision Computing.
9 Wang Yang, Tan T, Loe Kia-Fock, Jian Kang-Wu. A probabilistic approach for foreground and shadow segmentation in monocular image sequences. Pattern Recognition.
10 WANG Yang, LOE K F, WU Jiang-kang. A dynamic conditional random field model for foreground and shadow segmentation. IEEE Transactions on Pattern Analysis and Machine Intelligence.
11 Hsieh Jun-Wei, Hu Wen-Fong, Chang Chia-Jung, CHEN Yung-sheng. Shadow elimination for effective moving object detection by Gaussian shadow modeling. Image and Vision Computing.
12 Cucchiara R., Piccardi M., Prati A., Sirotti S. Improving shadow suppression in moving object detection with HSV color information // 2001 IEEE Intelligent Transportation Systems Proceedings.
13 Salvador E., Cavallaro A., Ebrahimi T. Cast shadow segmentation using invariant color features. Computer Vision and Image Understanding.

Except for spectral information, statistical model is another useful tool for shadow detection in colour videos. Nadimi and Bhanu set up a physical model for moving shadows and foreground object detection based on a new spatial-temporal albedo test and dichromatic reflection model. Nicolas and Zaccarin presented a novel pixel-based statistical approach to model moving cast shadows of non-uniform and varying intensity, where shadow pixels were modelled as a mixture of Gaussian model for describing moving cast shadows on object surfaces. Zhang et al.[14] proved that the ratio edge was invariant to illumination changes. Based on the property, the literature focused on the analysis of local ratios for shadow detection. Similarly, local colour constancy properties were exploited due to reflectance suppression over shadow regions. The difference of two luminance ratios between two neighbouring pixels was constant for shadow regions while local constancy did not hold for moving objects. Choi et al.[15] decomposed three components in the RGB colour space to calculate chromaticity difference and brightness difference, where they proved that the chromaticity difference was zero while brightness difference was constant for shadow pixels. Due to the existence of noise, it was assumed that they followed a single Gaussian distribution. Finally, local intensity ratio was used to improve the performance of the algorithm. All of these algorithms assumed that the distribution of pixel points or edge points obeyed a determinate statistical model, where the accuracy strongly depended on parameter estimations. However, the data may be determined for parameter estimations by using empirical strategies in the process of estimation, which affected the effectiveness of these algorithms.

IMPROVED ALGORITHM BASED ON HSV COLOUR CHARACTERISTICS

In view of the deficiency of the shadow elimination method, the improved method is proposed in this paper according to the actual situation of public security work. The specific process is shown in Figure 1.

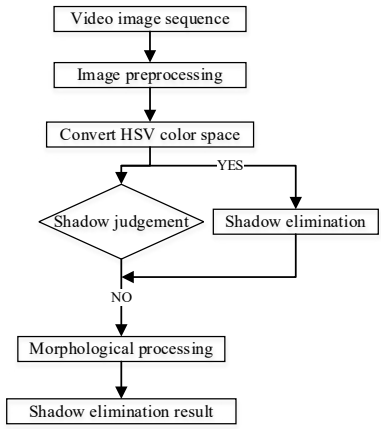


Figure 1: *Flow chart of shadow elimination*

14 Zhang Wei, Fang Xiang-Zhong, Yang X K K, Wu Q M J. Moving cast shadows detection using ratio edge. IEEE Transactions on Multimedia.

15 Yoneyama A.Yeh C. H.Kuo C. C. J. Moving cast shadow elimination for robust vehicle extraction based on 2D joint vehicle/shadow models. Proceedings of the IEEE Conference on Advanced Video and Signal Based Surveillance.

1. Image pre-processing

The video image contains noise components due to limited conditions and environmental impact, such as salt and pepper noise, Gaussian noise and impulse noise. The noise will affect the image quality and fuzzy image features. This paper carries on the median filter and Gauss filter to the video image, uses the bidirectional histogram equalization processing to highlight the edge of the image and enhances the ability to resist interference in order to improve the effect of shadow elimination.

2. Convert HSV colour space

RGB colour space is usually used in surveillance video capture process, RGB is converted to HSV colour mode in order to get a better treatment effect. HSV colour mode (H for hue, S for saturation and V for brightness) is closer to the human visual model and highlight the difference between shadows and moving objects because the colour mode can directly express the colour brightness information. The transformation formula is as follows:

$$\begin{cases} V = \max(R, G, B) \\ S = \frac{\max(R,G,B) - \min(R,G,B)}{\max(R,G,B)} \\ H = \begin{cases} 60 \times (R - B)/(S \times V), & \text{if } S \times V \geq 0.01 \text{ and } \max(R, G, B) = R \\ 60 \times (2 + (B - R)/(S \times V)), & \text{if } S \times V \geq 0.01 \text{ and } \max(R, G, B) = G \\ 60 \times (4 + (R - G)/(S \times V)), & \text{if } S \times V \geq 0.01 \text{ and } \max(R, G, B) = B \end{cases} \\ H = H - 300 \\ \text{if } H < 0, \text{ Then } H = H + 360 \end{cases}$$

The value range of R, G, B is [0,255], H is [0,360], S is [0,1], V is [0,255], H, S, V value range is normalized to [0,1] in the actual image processing, then the distribution of the H component is readjusted according to the following formula:

$$\begin{cases} H = H \times 80\% + 10\% \\ H = \begin{cases} V \times 10\%/50\%, & \text{if } S \times V < 0.01 \text{ and } V < 50\% \\ (V - 50\%) \times 10\%/50\%, & \text{if } S \times V < 0.01 \text{ and } V \geq 50\% \end{cases} \end{cases}$$

It can add light and dark grey areas, rich the image colour and grey detail and meet the perceptual characteristics of the human eye under the premise of preserving the original colour space by above method.

3. Shadow detection and elimination

Our eye is very easy to distinguish a moving target and its shadow. However, to automatically recognize the shadow of moving objects is the difficult problem of the intelligent monitoring system research. The information of position, shape characteristics, monitor screen surface properties and illumination can be obtained from the continuous monitoring of image. The colour attributes of the moving target shadow is significant different with background scene. So this paper uses HSV colour mode to judge the shadow, the specific formula is as follows:

$$\mathrm{sp}(x,y)=\begin{cases}1, & \alpha_S \le \frac{I_V(x,y)}{B_V(x,y)} \le \beta_S \\ & \cap\left(I_S(x,y)-B_S(x,y)\right) \le \tau_S \\ & \cap\left|I_H(x,y)-B_H(x,y)\right| \le \tau_H \\ 0, & \text{onther}\end{cases}$$

$l_H(x,y)$, $l_S(x,y)$, $l_V(x,y)$ respectively represents the component of the new input pixel $I(x,y)$ on the HSV, $B_H(x,y)$, $B_S(x,y)$, $B_V(x,y)$respectively represents the component of background pixel value on the HSV. If $I(x,y)$ is identified as the shadow, the $sp(x,y)$ is 0. $0<\alpha_S<\beta_S<1$, the value of α_S is based on the shadow intensity, the intensity of the shadow projection is stronger, α_S is smaller, and β_S is used to improve the robustness of the adaptive noise, so that the brightness of the current frame cannot be too close to the background.

The brightness V decreases and the shadow vector sum of is smaller than the background vector sum of , so one can distinguish the shadow through comparing two vectors, the calculation formula is as follows:

$$\mathrm{sp}(x,y)=\begin{cases}1, & ((H^2+S^2+V^2)<(H_b^2+S_b^2+V_b^2)) \\ & \cap\,(V<V_b<4V) \\ 0, & \text{other}\end{cases}$$

4. Morphological processing

There are discrete noises after shadow elimination in the image and edge breakpoint phenomenon under normal circumstances. The noise is not conducive to the further analysis of the interest target, so the noise must be reduced after shadow elimination. The general method is using morphological operations, including the expansion and corrosion operation to remove isolated noise and filling the missing edge contour. Finally, the satisfactory treatment effect can be obtained.

EXPERIMENTAL RESULT ANALYSIS

In order to verify the effectiveness of the proposed algorithm, Matlab in Inter Core i5 3.2GHz dual core CPU, 4GB memory hardware platform was used. The elimination and detection experiments of indoor and outdoor were carried out by using the international standard video sequence Highway I and Intelligent room. The result is as follows: (a) represents the original image, (b) represents difference calculation of the two values, (c) represents the image of literature [4], (d) represents the image of literature [5], (e) represents the image of this paper's algorithm.

(a) (b) (c) (d) (e)

Figure 2: *Processing results of 90th frame in Highway I video*

(a) (b) (c) (d) (e)

Figure 3: *Processing results of 104th frame in Highway I video*

(a) (b) (c) (d) (e)

Figure. 4: *processing results of 183th frame in Highway I video*

(a) (b) (c) (d) (e)

Figure 5: *Processing results of 280th frame in intelligent room video*

(a) (b) (c) (d) (e)

Figure 6: *Processing results of 510th frame in intelligent room video*

(a) (b) (c) (d) (e)

Figure 7: *Processing results of 840th frame in intelligent room video*

The light will have a clear shadow, and if these shadows don't get removed, it will seriously affect the precision of the detection and tracking of the moving target. The 90th, 104th and 183rd frame in Highway I video were intercepted. It can be found that the algorithms of c and d images, although can eliminate part of the shadow, will miss the main outline of target from the result of detection and elimination. The algorithm of this paper can better eliminate the shadow and ensure the integrity of the main target contour. The 280th, 510th, and 840th frame were intercept in intelligent room video. It can be found that the algorithm of c and d images can better eliminate the shadow but the noise interference is obvious, the algorithm of this paper can get a more complete external contour. Overall, the effect of noise elimination and

detection and elimination of shadow is better, and is also closer to the actual needs of public security work and has a high practical value.

CONCLUSION

Shadow is prevalent in moving object detection and tracking; it seriously affects the detection accuracy and missing of the target. The current algorithm of shadow elimination was analysed, and the shadow was removed by using HSV colour model according to the actual demand of public security work. Experimental results show that the proposed method can effectively eliminate the shadow and get a more complete outline; it has better real-time performance and robustness.

REFERENCES

1. Benedek C., Sziranyi T. Study on color space selection for detecting cast shadows in video surveillance. International Journal of Imaging Systems and Technology.
2. Choi Jin-Min, Yoo Yung-Jun, Choi Jin-Young. Adaptive shadow estimator for removing shadow of moving object. Computer Vision and Image Understanding.
3. LI Zheng, JIANG Po-Huang, Mab Hong, YANG Jian, TANG Dong-Ming. A model for dynamic object segmentation with kernel density estimation based on gradient features. Image and Vision Computing.
4. Nadimi S., Bhanu B. Physical models for moving shadow and object detection in video. IEEE Transactions on Pattern Analysis and Machine Intelligence.
5. Nicolas M. B., Zaccarin A. Learning and removing cast shadows through a multidistribution approach. IEEE Transactions on Pattern Analysis and Machine Intelligence.
6. Prati A., Mikic I., Trivedi M. M., Cucchiara R. Detecting moving shadows: algorithms and evaluation [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(7): 918–923.
7. Sanin A, Sanderson C, Lovell B C. Improved Shadow Removal for Robust Person Tracking in Surveillance Scenarios [A]. 2010, 20th International Conference on Pattern Recognition [C]. Conference Publications.
8. Stauffer C, Grimson W. E. L. Adaptive background mixture models for real-time tracking. [C]// IEEE Computer Society Conference on Computer Vision and Pattern Recognition. Fort Collins, USA, 1999: 246–252.
9. Stauffer C, Grimson W. E. L. Learning patterns of activity using real-time tracking [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2000, 22(8): 747–757.
10. Wang Yang, Tan T., Loe Kia-Fock, Jian Kang-Wu. A probabilistic approach for foreground and shadow segmentation in monocular image sequences. Pattern Recognition.
11. XU Dong, LI Xue-Long, LIU Zheng-Kai, YUAN Yuan. Cast shadow detection in video segmentation. Pattern Recognition Letters.
12. Yoneyama A. Yeh C. H. Kuo C. C. J. Moving cast shadow elimination for robust vehicle extraction based on 2D joint vehicle/shadow models[C]. Proceedings of the IEEE Conference on Advanced Video and Signal Based Surveillance (AVSS'03). Miami, FL, USA. IEEE Computer Society. 2003. 229–236.
13. Zhang Wei, Fang Xiang-Zhong, Yang X. K. K., Wu Q M J. Moving cast shadows detection using ratio edge. IEEE Transactions on Multimedia.

UDC: 43.983:615.074
615.074:543

STUDIES OF THE METABOLISMAND DISTRIBUTION OF METHYLONE IN RATS BY LIQUID CHROMATOGRAPHY-MASS SPECTROMETRY

Xueguo Chen, PhD[1]
National Police University of China,
Department of Forensic Chemistry, Shenyang

Abstract: A specific and sensitive liquid chromatography-electrospray ionization-ion trap mass spectrometry (LC-ESI-ITMS) method was developed and employed for the studies of metabolism and distribution of methylone in rats. The determination and quantitative analysis of methylone in urine, plasma and liver were accomplished individually, the precursor and major product ion of methylone was monitored in positive ion detection mode as m/z 190.1 with LC-ESI-ITMS. The method validation of the analysis of methylone in urine, plasma and liver was performed and the results showed that the method had good precision and repeatability. The urinary metabolites of methylone in rats were investigated by analysing urine specimens after administrating to rats with LC-ESI-ITMS, totally four metabolites of methylone were obtained. The distribution of methylone in rats was examined after oral administration, and the result showed that the concentration in urine was higher than other parts.

Keywords: designer drug, LC-MS, distribution, metabolism, methylone.

INTRODUCTION

Designer drugs are synthesized to circumvent existing laws on controlled substances in order to enhance the pharmacological activities of already known drugs[2]. As a relatively new cathinone-type designer drug, methylone [2-methylamino-1-(3, 4-methylenedioxyphenyl) propan-1-one] has gained popularity among drug users and is available illicitly in tablet or powder form in many countries, and is also named as 3,4-methylenedioxymethcathinone or bk-MDMA or M_1, and it is sold as "legal highs" or "bath salts" in all regions[3]. The abuse of it in recent years has increased the need for the study of detection, metabolism and distribution of methylone[4]. Several analytical approaches have been used for determining the composition of synthetic drugs, especially for the determination of methylone in pharmaceutical samples and biomaterials, including thin layer chromatography[5], gas chromatography-mass spectrometry[6] and liquid chromatography-mass spectrometry (LC-MS)[7]. However, relatively little information about the metabolism, distribution and addiction potential of methylone is available[8].

1 E-mail: dicpchenxg@hotmail.com.
2 D. P. Katz, D. Bhattacharya, S. Bhattacharya, J. Deruiter, C. R. Clark, V. Suppiramaniam and M. Dhanasekaran, Toxicol. Lett., 2014, 229, 349–356.
3 L. J. De Felice, R. A. Glennon and S. S. Negus, Life Sci., 2014, 97, 20–26.
4 K. Kovács, A. R. Tóth and E. M. Kereszty, Orv Hetil., 2012, 153, 271–276.
5 N. N. Daeid, K. A. Savage, D. Ramsay, C. Holland and O. B. Sutcliffe, Sci. Justice, 2013, 54, 22–31.
6 A. M. Leffler, P. B. Smith, A. Armas and F. L. Dorman, Forensic Sci. Int., 2014, 234, 50–56.
7 S. Strano-Rossi, L. Anzillotti, E. Castrignanò, F. S. Romolo and M.Chiarotti, J. Chromatogr. A, 2012, 1258, 37–42.
8 B. M. Cawrse, B. Levine, R. A. Jufer, D. R. Fowler, S. P. Vorce, A. J. Dickson and J. M. Holler, J. Anal. Toxicol., 2012, 36, 434–439.

As a modern powerful analysis technology, LC-MS has been utilized widely in the research areas of life science, environmental science[9], and the applications have shown the superior advantages, such as high sensitivity and superior selectivity[10]. In LC-MS, electrospray ionization ion trap mass spectrometry (ESI-ITMS) technique has been applied for the identification of drugs and showed the potential in structural analysis[11]. Drug metabolites often keep the core structure of the parent drug after biotransformation, thus the fragmentation of the parent drug obtained by multi-stage tandem mass spectrometric techniques (MS^n) can be used for the identification of metabolites. So far, LC-ESI-ITMS has been applied widely in the analysis of drugs[12] and metabolites[13].

In the present study, a specific and sensitive method employing liquid chromatography-electrospray ionization ion trap mass spectrometry (LC-ESI-ITMS) was developed and applied in the studies of detection, metabolism and distribution of methylone in rats. The obtained results not only showed the advantages of the approach described here, but also displayed the potential application in addicted relevant cases.

EXPERIMENTAL

Chemicals and reagent

Chromatography grade methanol and acetonitrile were purchased from Shield Co., Ltd (Tianjin, China). Analytical reagent grade acetic acid and ammonium acetate were purchased from Guoyao Group Chemical Reagent Shenyang Co., Ltd (Shenyang, China). Methylone was purchased from the National Institute for the Control of Pharmaceutical and Biological Products (Beijing, China) and only used for research purpose.

Animals

Male Sprague Dawley rats weighing 220-250 g were purchased from Laboratory Animal Services Center, Liaoning University of Traditional Chinese Medicine and acclimated in the laboratory for 7 days prior to the experiments, housed with free access to food and water, on a 12 h light-dark cycle at ambient temperature (22°C–24°C) and roughly 50% relative humidity. Animal welfare and experimental procedures were in accordance with the guide for the care and use of laboratory animals and the related ethical regulations of the National Police University of China.

Drug Administration and Sampling

Ten rats were randomly divided into two groups, one group including 2 rats was regarded as blank control group, and another group including 8 rats was orally administrated at a single dose of 30 mg/kg of methylone dissolved in water. Then the urine samples of all the rats were collected before dosing drug as blank urine samples for metabolism analysis purpose. After that, all the rats were sacrificed by decapitation 24 h after dosing. The urine and blood were collected in tubes, respectively. The urine samples were directly frozen at -20°C until analysis, and the plasma samples were obtained and frozen at -20°C until analysis after centrifuging at

9 P. Xiang, M. Shen and X.Y. Zhuo, LC-MS and application in the analysis of medicine and abused drugs, Shanghai Science and Technology Press, 2009.
10 Y. Q. Lai, X. G. Chen, M. H. Lam and Z. W. Cai, J. Chromatogr. B, 2011, 879, 1086–1090.
11 J. Thunig, L. Fløe, S. Pedersen-Bjergaard, S.H. Hansen and C. Janfelt, Rapid Commun. Mass Spectrom., 2012, 26, 133–140.
12 Y. Y. Xua, D. Y. Si and C. X. Liu, J. Pharm. Biomed. Anal., 2009, 49, 487–491.
13 X. G. Chen, M. Song, Y. Zhu, D. Wu and Y. J. Xu, Anal. Method, 2013, 5, 4764–4768.

10 000 rpm for 10 min. For distribution study, the tissues from the organs such as heart, liver, lung and kidney were removed, respectively, then they were rapidly rinsed with physiological saline solution to remove the blood, then were blotted by filter paper, and stored at -20°C until analysis.

Sample Extraction Processing

To a 100 μL aliquot of urine or plasma sample, 200 μL acetonitrile was added and the sample was centrifuged at 10 000 rpm for 10 min after vortex-mixed for 1 min, the supernatant was delivered, and an aliquot of 10 μL was injected to the LC-MS system for the determination, quantitative analysis and metabolites identification.

All the tissues from the organs were homogenized in 50% methanol-water solution while the ratios were 1:6 (w/v) and centrifuged at 10 000 rpm for 5 min. 100 μL of the supernatant from all the tissue homogenate were processed like the urine and plasma samples.

Preparation of Standard Solution and Samples

Stock solution was prepared using deionized water at a target concentration of 50.0 μg/mL. Different concentrations of calibration standard were freshly prepared in the range of 0.02 μg/mL to 5.00 μg/mL by making appropriate serial dilutions of the stock solution. The calibration curves were constructed by plotting peaks areas versus corresponding concentration of the standard. Spiked samples containing methylone were prepared by diluting different volumes of methylone stock solution in urine, plasma and liver homogenate of control blank rats, and then stored below 4°C prior to use.

LC/MS^n Analysis

LC separation was accomplished with Finnigan Surveyor liquid chromatography system (San Jose, CA, USA) equipped with a Thermo Gold ODS column (150×2.1 mm, 5 μm). The mobile phase consisted of phase A (water, 10 mM ammonium acetate, 0.1% of acetic acid) and B (methanol). The gradient program started with 20% B and held for 1 min, then changed to 90% B within 5 min, and held for 6 min. The flow rate was 0.2 mL/min. The temperature of the column during analysis was maintained at 30°C.

MS analysis was performed on a LXQ ion trap mass spectrometer (Thermo Fisher, USA). The ion trap mass spectrometry was operated with positive electrospray ionization under full-scan MS, MS/MS and MS^3 modes. The flow rates of sheath gas, aux gas and sweep gas were 30.00 mL/min, 8.00 mL/min and 2.00 mL/min, respectively. The voltages of source, capillary and tube lens were 5.00 kv, 1.00 v and 5.00 v, respectively. The capillary temperature was 350°C. Data acquisition and instrument control were performed using Xcalibur software (Thermo Fisher, USA).

RESULTS AND DISCUSSION

Optimization of LC-MS Conditions

Methylone is one of the typical designer drugs, belong to synthetic cathinone derivatives and the structure is shown in Figure 1. According to the corresponding reports[14], methanol and water (10 mM ammonium acetate, 0.1% of acetic acid) were chosen as the mobile phases

14 R. López-Arnau, J. Martínez-Clemente, M.I. Carbó, D. Pubill, E. Escubedo and J. Camarasa, Pro. Neuro-psychoph., 2013, 64–72.

for the LC-ESI-ITMS analysis of methylone and its metabolites mentioned here. Solvent gradient-elution program was established by comparing the peak resolution of methylone and its metabolites obtained from different gradient-elution modes. The $[M+H]^+$ ions of methylone and its metabolites were chosen as parent ions for the fragmentation in MS/MS mode and the prominent ions in MS/MS spectrum was chosen to fragmentate in MS^3 mode. The retention time of methylone under the optimized gradient-elution conditions was 8.01 min, which is shown in Fig. 2 and Table 1. The LC-MS^n spectra of methylone are also obtained and listed in Fig.3 and Table 1. The $[M+H]^+$ ion of methylone was detected at m/z 208.1. The precursor and major product ion of methylone was monitored at m/z 190.1. Furthermore, the major product ion monitored in MS^3 spectrum was also obtained as m/z 160.1.

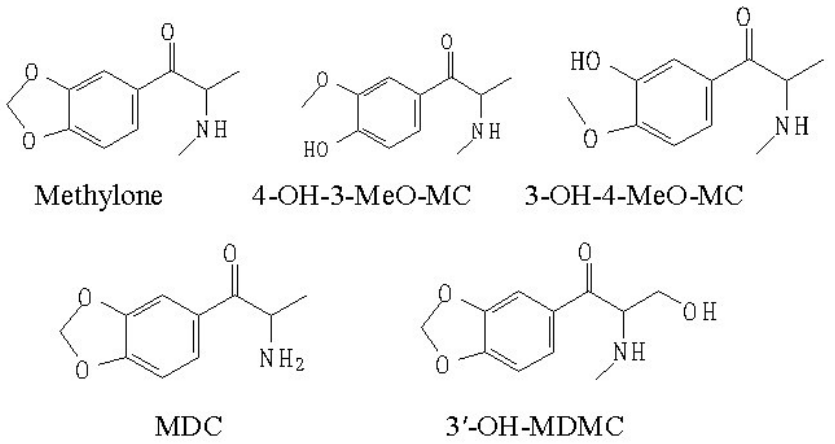


Figure 1: *Chemical structures of methylone and its metabolites*

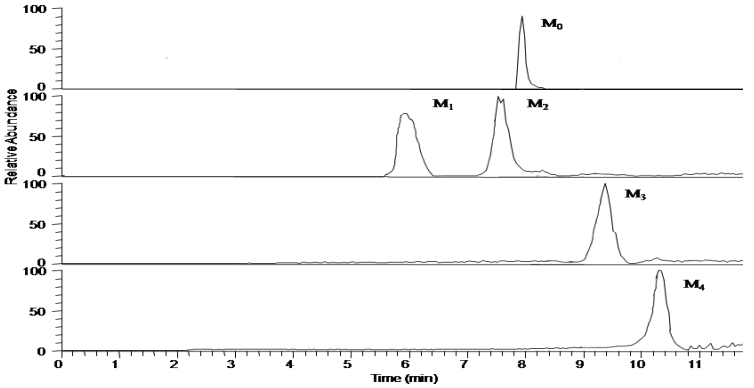
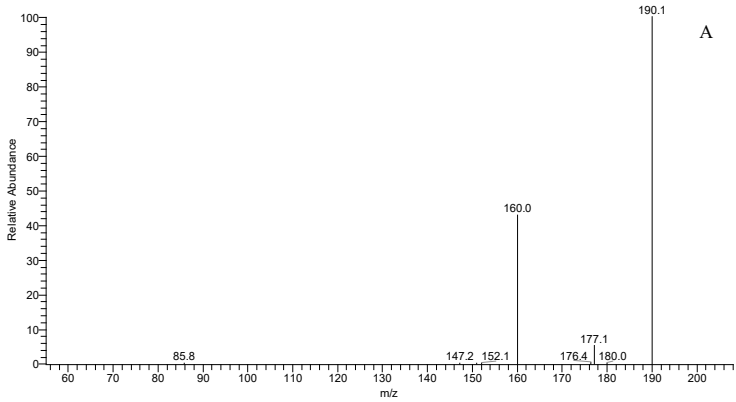
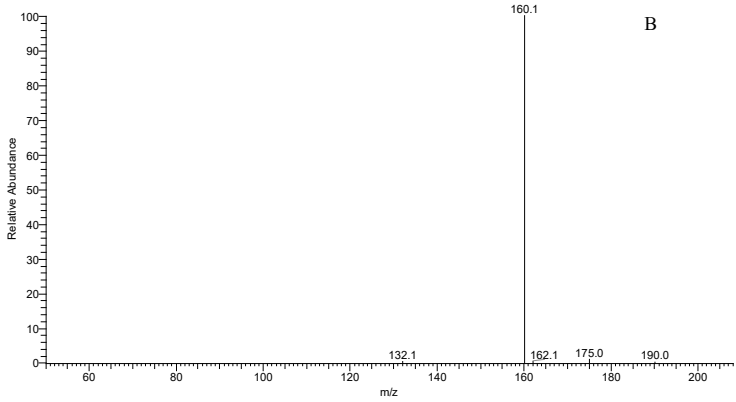
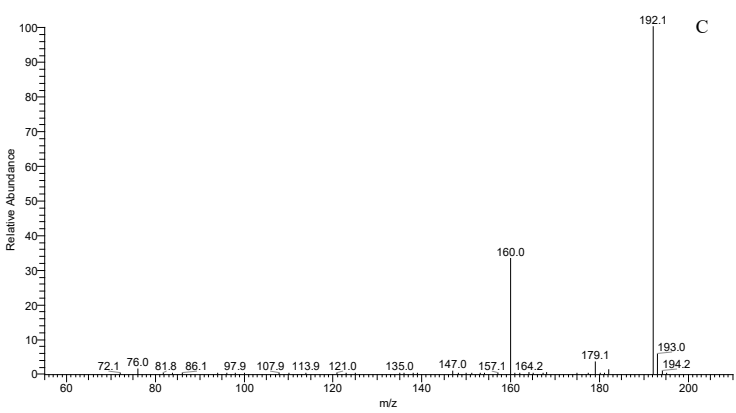
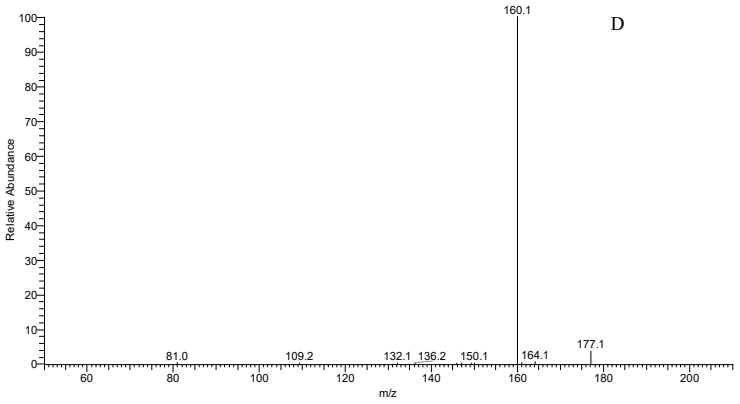


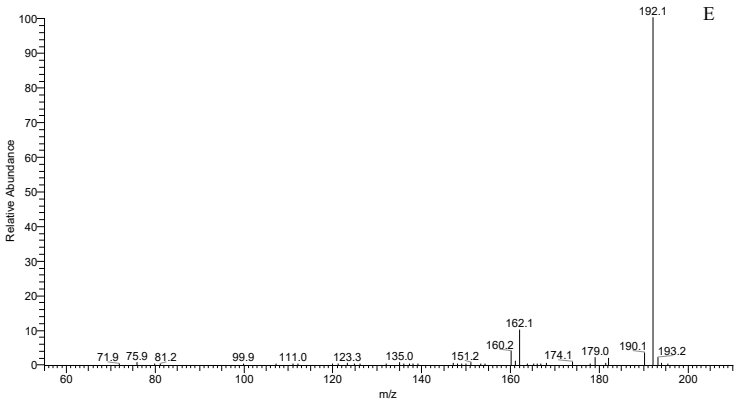
Figure 2: *LC-MS chromatograms of methylone and its metabolites under the optimized gradient-elution conditions*

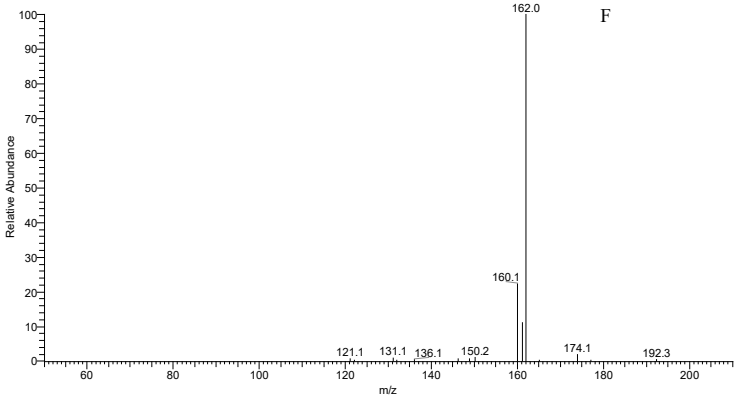

A
190.1
160.0
177.1
85.8
147.2
152.1
176.4
180.0
Relative Abundance
m/z

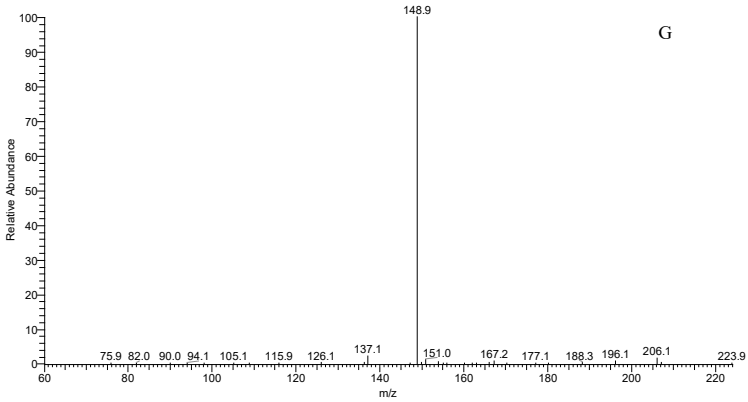

B
160.1
132.1
162.1
175.0
190.0
Relative Abundance
m/z

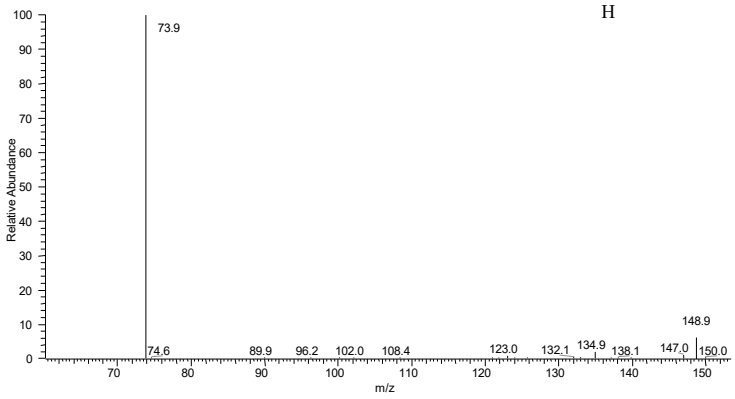

C
192.1
160.0
193.0
194.2
179.1
72.1
76.0
81.8
86.1
97.9
107.9
113.9
121.0
135.0
147.0
157.1
164.2
Relative Abundance
m/z

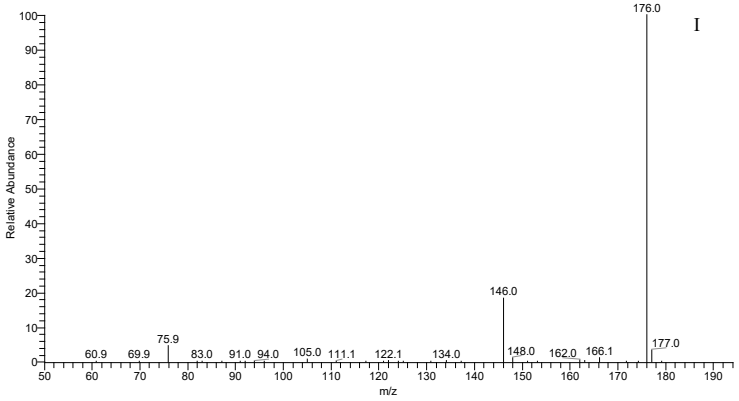

D
160.1
Relative Abundance
81.0
109.2
132.1
136.2
150.1
164.1
177.1
m/z


E
192.1
Relative Abundance
162.1
160.2
71.9
75.9
81.2
99.9
111.0
123.3
135.0
151.2
174.1
179.0
190.1
193.2
m/z


F
162.0
Relative Abundance
160.1
121.1
131.1
136.1
150.2
174.1
192.3
m/z


G
148.9
Relative Abundance
m/z
75.9 82.0 90.0 94.1 105.1 115.9 126.1 137.1 151.0 167.2 177.1 188.3 196.1 206.1 223.9


H
73.9
148.9
Relative Abundance
m/z
74.6 89.9 96.2 102.0 108.4 123.0 132.1 134.9 138.1 147.0 150.0


I
176.0
146.0
75.9
177.0
Relative Abundance
m/z
60.9 69.9 83.0 91.0 94.0 105.0 111.1 122.1 134.0 148.0 162.0 166.1

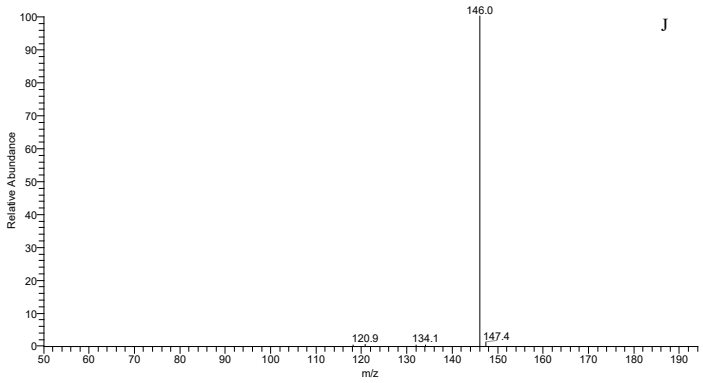


Figure 3: *MS/MS and MS³ spectra of methylone and its metabolites*

(A) MS/MS spectrum of M_0; (B) MS^3 spectrum of M_0; (C) MS/MS spectrum of M_1; (D) MS^3 spectrum of M_1; (E) MS/MS spectrum of M_2; (F) MS^3 spectrum of M_2; (G) MS/MS spectrum of M_3; (H) MS^3 spectrum of M_3; (I) MS/MS spectrum of M_4; (J) MS^3 spectrum of M_4.

Table 1: *Retention times and MS^n ion fragments of methylone and its metabolites*

No	Name	Retention time (min)	$[M+H]^+$	MS/MS	MS^3
M_0	Methylone	8.01	208.1	190.1	160.1
$_M1$	4-OH-3-MeO-MC	5.97	210.1	192.1	160.1
M_2	3-OH-4-MeO-MC	7.63	210.1	192.1	162.0
M_3	MDC	9.41	194.1	148.9	73.9
M_4	3.-OH-MDMC	10.33	224.1	176.0	146.0

Method Validation

Liquid chromatography-tandem mass spectrometry (LC-MS/MS) was utilized for the quantitative analysis of methylone in rat urine, plasma and liver samples. The daughter ion from first fragmentation at m/z 190.1 was chosen for the quantitative analysis ion. Selectivity of the method was tested by comparing the chromatogram of blank control samples with the corresponding spiked extract of methylone. The obtained results showed that there was no background interference to the analysis of methylone in urine, plasma and liver under the optimal LC-MS/MS conditions. The samples were treated and analyzed by LC-MS/MS and the obtained calibration curves of methylone exhibited good linearity with determination coefficients (R^2=0.9982-0.9993) as shown in Table 2.

In order to estimate the limit of detection (LOD) and the limit of quantitation (LOQ), spiked urine, plasma and liver samples at different concentrations were analysed. The LODs and LOQs of methylone in urine, plasma and liver samples developed in the present work are listed in Table 2, which were calculated on the basis of the chromatographic peak for which the signal-to-noise ratio was 3 (S/N=3) for qualitative analysis and 10 (S/N=10) for quantitative analysis, respectively. As shown in Table 2, LODs for methylone in urine, plasma and liver samples were 0.02 μg/mL, 0.01 μg/mL, 0.01 μg/mL, and LOQs were 0.05 μg/mL, 0.03 μg/mL, 0.04 μg/mL, respectively.

Table 2: *Linearity equations, coefficients, linearity ranges, LODs and LOQs of methylone in urine, plasma and liver*

Sample	Linearity equation	Coefficients (r)	Linearity range (μg/mL)	LOD (μg/mL)	LOQ (μg/mL)
Urine	Y=25731X+1749.4	0.9993	0.05-5.00	0.02	0.05
Plasma	Y=13890X+2365.2	0.9987	0.03-5.00	0.01	0.03
Liver	Y=12749X+2671.5	0.9982	0.04-5.00	0.01	0.04

Table 3: *Precisions and recoveries of methylone in urine, plasma and liver*

Sample	Spiked concentration (μg/mL)	Precision (RSD, %)		Recovery (%)
		Intra-day (n=3)	Inter-day (n=9)	
Urine	0.10	5.1	5.8	88.5
	1.0	4.6	5.0	92.1
	3.0	4.2	4.8	85.8
Plasma	0.10	4.6	5.9	82.4
	1.0	4.9	5.2	85.1
	3.0	4.7	5.2	84.9
Liver	0.10	4.5	5.7	81.1
	1.0	4.9	5.1	78.9
	3.0	4.8	4.9	79.9

The precision and accuracy of the method were referred by relative standard deviation (RSD) and recovery. They were both evaluated with the analysis of spiked urine, plasma and liver samples with different concentrations which were set with low, medium and high level of the calibration range as 0.1 μg/mL, 1.0 μg/mL and 3.0 μg/mL for methylone. The intra-day precision was calculated by analysing the samples within one day (n=3), while the inter-day precision was determined by analysing the samples at the same concentrations in three consecutive days (n = 9), and the results are listed in Table 3. The RSD from the intra-day study was generally lower than those from the inter-day analysis which revealed from the results. Both RSDs were less than 5.9% as shown in Table 3, indicating that the method has good precision and repeatability in the quantitative analysis in urine, plasma and liver samples. Meanwhile, the recoveries of methylone in urine, plasma and liver samples were obtained by average of determined concentrations with the known spiked levels as listed in Table 3. The recoveries varied from 78.9% to 92.1% were obtained from the analysing of samples at low, medium and high concentrations. The results indicated that the method provided good accuracy for the analysis of methylone, and also revealed it could be considered as a good candidate for the quickly determination of recently surfaced designer drugs marketed.

In-vivo Metabolism Study

In this study, LC-ESI-ITMS was applied in the metabolism research of methylone in rat urine. Metabolite was preliminary detected if the mass chromatographic peak of an expected $[M+H]^+$ ion was observed in urine of rat dosing methylone, but not in the corresponding sample of rat collected before dosing. Totally four metabolites were detected in urine sample of methylone as listed in Table 1, including 3-hydroxy-4-methoxymethcathinone (3-OH-4-

MeO-MC), 4-hydroxy-3-methoxymethcathinone (4-OH-3-MeO-MC), 3, 4-methylenedioxycathinone (MDC) and 3-hydroxy-methylenedioxymethcathinone (3-OH-MDMC), respectively. The structures of these metabolites are shown in Figure1. Furthermore, in order to confirm the metabolite identification, LC-MS^n analysis was accomplished, the MS/MS and MS^3 spectra were obtained as shown in Figure 2. Meanwhile, the metabolism of methylone in plasma was also discussed and the results were similar to the detection in urine of rats, and also were similar to the reports in references[15],[16].

Distribution

The distribution of methylone was investigated following a single oral administration to eight rats at 0.30 mg/kg. LC-ESI-ITMS was employed for the quantitative analysis of methylone in urine, plasma and tissues including lung, kidney, liver and heart of rats, while the concentrations of methylone in all the tissues were calculated via the calibration curve of methylone in rat liver, as shown in Figure 4. Methylone could be detected in lung, kidney, liver and heart, but the concentrations in these tissues were lower than in urine and plasma. The concentration detected in urine was the highest, and then in plasma, lung, kidney, liver and the concentration in heart was the lowest. Based on the results urine or blood should be regarded as the best sample to be selected in the determination of methylone in forensic and clinically addicted relevant cases.

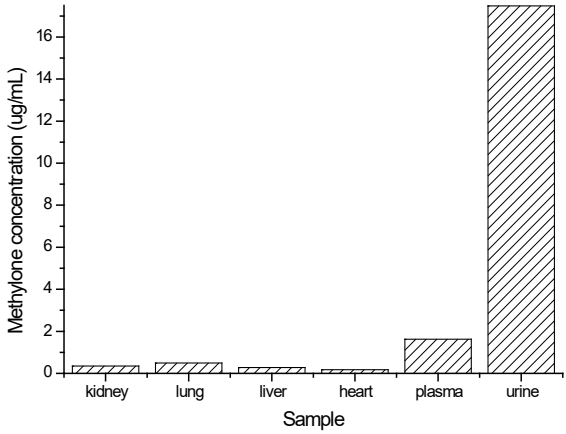


Figure 4: *The distributions of methylone in rats*

CONCLUSION

In this study, the described LC-ESI-ITMS method provided detection, metabolism and distribution analysis of methylone in rat. The accurate, specific, selective and sensitive analytical procedure was successfully applied for the analysis of spiked rat urine, plasma and liver samples of methylone, the identifications of metabolites in rat urine besides the distribution of methylone. The results of the analysis of methylone in urine, plasma and liver showed that the method had good precision and repeatability. Totally four metabolites of methylone were obtained in rats by analyzing urine specimens after administrating to rats with LC-ESI-ITMS. The experimental results showed that the potential advantages of this approach in the identification and quantitative analysis of designer drugs in addicted relevant cases.

15 E. Fornal, J. Pharm. Biomed. Anal., 2013, 81–82, 13–19.
16 C. L. German, A. E. Fleckenstein and G. R. Hanson, Life Sci., 2014, 97, 2–8.

ACKNOWLEDGEMENT

The financial supports of the Faculty Research Grant from the Key Laboratory of Evidence Science of the Ministry of Education (No. 2014KFKT05) and the Ministry of Public Security of China (No. 2015JSYJB09) in this study are acknowledged.

REFERENCES

1. A. M. Leffler, P. B. Smith, A. Armas and F. L. Dorman, Forensic Sci. Int., 2014, 234, 50–56.
2. B. M. Cawrse, B. Levine, R. A. Jufer, D. R. Fowler, S. P. Vorce, A. J. Dickson and J. M. Holler, J. Anal. Toxicol., 2012, 36, 434–439.
3. C. L. German, A. E. Fleckenstein and G. R. Hanson, Life Sci., 2014, 97, 2–8.
4. D. P. Katz, D. Bhattacharya, S. Bhattacharya, J. Deruiter, C. R. Clark, V. Suppiramaniam and M. Dhanasekaran, Toxicol. Lett., 2014, 229, 349–356.
5. L. J. De Felice, R. A. Glennon and S. S. Negus, Life Sci., 2014, 97, 20–26.
6. E. Fornal, J. Pharm. Biomed. Anal., 2013, 81–82, 13–19.
7. J. Thunig, L. Fløe, S. Pedersen-Bjergaard, S.H. Hansen and C. Janfelt, Rapid Commun. Mass Spectrom., 2012, 26, 133–140.
8. K. Kovács, A. R. Tóth and E. M. Kereszty, Orv Hetil., 2012, 153, 271–276.
9. N. N. Daeid, K. A. Savage, D. Ramsay, C. Holland and O. B. Sutcliffe, Sci. Justice, 2013, 54, 22–31.
10. P. Xiang, M. Shen and X.Y. Zhuo, LC-MS and application in the analysis of medicine and abused drugs, Shanghai Science and Technology Press, 2009.
11. R. López-Arnau, J. Martínez-Clemente, M.I. Carbó, D. Pubill, E. Escubedo and J. Camarasa, Pro. Neuro-psychoph., 2013, 64–72.
12. S. Strano-Rossi, L. Anzillotti, E. Castrignanò, F. S. Romolo and M.Chiarotti, J. Chromatogr. A, 2012, 1258, 37–42.
13. X. G. Chen, M. Song, Y. Zhu, D. Wu and Y. J. Xu, Anal. Method, 2013, 5, 4764–4768.
14. Y. Q. Lai, X. G. Chen, M. H. Lam and Z. W. Cai, J. Chromatogr. B, 2011, 879, 1086–1090.
15. Y. Y. Xua, D. Y. Si and C. X. Liu, J. Pharm. Biomed. Anal., 2009, 49, 487–491.

UDC: 343.983:623.746-519

THE PERSPECTIVES OF APPLYING UAV (UNMANNED AERIAL VEHICLE) IN THE CRIMINAL INVESTIGATION

Nikolay Demidov, PhD[1]
Volgograd Academy of the Russian Internal Affairs Ministry

Abstract: The technologies of UAV (Unmanned aerial vehicle) are widely spread in the different spheres of human activity nowadays. Among military and civil usage also could be mentioned law enforcement application. There are a huge number of implementations of UAV in all spheres of policing: from surveillance, patrolling and crowd control to crime evidence detecting. This new technology gives a lot of advantages to the law enforcement agencies, but also causes some juridical questions. The targets of this article are: observing the perspectives of future implementation of UAV in the criminal investigation and marking some questions of their law regulations, standards and procedures.

Keywords: UAV, forensic science, criminal investigation, human rights, criminal procedure, crime scene search

INTRODUCTION

The implementation of new technologies in law enforcement activity is an important part of modern scientific research. The emergence of new knowledge in forensic science and other applied sciences contributed to the development of police science, enabled effective use of these advances in the detection and investigation of crimes, prevention and punishment. Here should be mentioned the contributions of different scientists: the appearance of fingerprinting, invent of biometrics in forensic science, the implementation of forensic photography, revolution in the production of genetic examination, the advent of computer technology in the field of crime investigation, statistics and data banks. All of these scientific achievements in conjunction with the development of forensic science made it possible to achieve great results and success in solving complicated crimes, such as serial murders, the economic crimes, the crimes in the sphere of computer information etc. Unfortunately, along with the progress of new technologies there are the new types of crimes appeared, such as: the fraud in the financial sector, the computer technologies crimes, transnational organized crime, organized international drug trafficking and etc.

Nowadays one the top of scientific discussion is the implementation of robotic technology with elements of artificial intelligence, such as the technology of unmanned aerial vehicles (UAV). The use of UAVs has been increasing since they were first introduced. As of early 2014, more than 50 countries have UAVs in their arsenal; a growing number of countries seek to obtain them in the near future; the number of countries in which UAVs are produced has increased. The number of UAVs in operation has seen a drastic rise, as has the number of military strikes (e.g. between 2004 and 2007 the US military carried out nine drone strikes,

1 E-mail: n_demidov@hotmail.com.

while that number reached 118 strikes in 2010). It can be expected that the number of UAVs that are actively deployed will increase in the future[2].

Now we are experiencing another technological boom effected also by the new methods of production, in particular 3 D printing technology. The author participated in the application of the police drone technology for the last 3 years. It should be noticed that this technology is still under development, requires additional scientific researches, inventing new technologies in the field of creating drones with sufficient battery capacity and flight stability, software reliability, data and maintenance security, utilization of these types of aircraft, testing and implementation in to the practice. This is a matter of the near future: many international companies engaged in intensive development in this sphere, almost every day there is information about new types of drones, new areas of application, practical battery capacity. However, despite such a rapid development of technology, the enthusiasm of developers and users of drones should be noted that from a legal point of view, there are many unresolved issues.

The purpose of this article is to identify the main direction of this technology, also to identify strengths and weaknesses, identify the legal issues governing this activity. The author is aware that the stated topic is quite comprehensive and requires further elaboration, however, based on the experience of the recent years today we could put this subject to a public scientific discussion.

Unmanned aerial vehicle is the product of dual-usage. Originally developed technology within the framework of military technology gradually gained importance in the civil work and law enforcement. At present, more and more areas of social activity use unmanned aircraft technology (drones). A key advantage of it is the possibility of remote sensing, monitoring areas, obtaining the necessary audio-visual and other data and transport of materials in complex difficult conditions.

Unmanned aircraft systems (UAS) are an aircraft and its associated elements which are operated with no pilot on board. Remotely piloted aircraft systems (RPAS) are a set of configurable elements consisting of a remotely piloted aircraft, its associated remote pilot station(s), the required command and control links and any other system elements as may be required, at any point during flight operations. RPAS are a sub-set of UAS. Synonym «drone» is a small-sized unmanned aerial vehicle (floating), the device is equipped with a central processing unit, sensors for orienteering, remote controllable and capable of performing a variety of complex manned tasks, including in conditions of remote areas, in dangerous and inaccessible areas, making them an ideal way obtain the necessary information as part of the search and observation activities.

UAVs come in a wide variety, but can be divided into classes based on size, range, and capacity for autonomous flight. While most are controlled remotely by a human pilot on the ground, some can fly along pre-set coordinates or patterns, or land if they lose contact with the pilot. The author proposes a classification of professional police drones, in accordance with their use in law enforcement activity. Depending on this use, you can select the following types of police drones:

1. "The operation drones" designed to monitor and capture crowded events, riots and during special police operations. The main requirements for this category: the simplicity of management, flexibility, the information security protocol, altitude and flight speed, the ability to stabilize in the air, panoramic and detailed photo and video broadcasting to the command post, the battery capacity.

2 Wagner, Markus, Unmanned Aerial Vehicles (March 24, 2015). Max Planck Encyclopedia of Public International Law, Rüdiger Wolfrum, ed., Oxford University Press, Forthcoming; University of Miami Legal Studies Research Paper No. 15-12. Available at SSRN: http://ssrn.com/abstract=2584652

2. "The inquiry drones" designed for search and detection of objects and people in a large area. To this category is important to the ability of a long flight over long distances with the transmission of information in real-time, all-weather operating conditions, the ability to maneuver and implement high-quality signal transfer of audio and video in conditions of poor visibility and night time, the possibility of a modular equipment with additional sensors, such as thermal vision to detect from the air of places of illegal production of hydroponic drugs.

3. "The forensic drones" designed to obtain procedural information and detailed survey of scanning areas with the investigative actions in order to obtain the information of criminal procedure and the taking of evidence in a criminal case. For this category of importance is the speed of deployment, flexibility, the possibility of a flight on a given route, the ability to carry out a qualitative survey the terrain and objects in high resolution, producing 3d shooting as well as receive other data in difficult weather conditions and poor visibility.

In recent years, the drones are used as a component of geo-informational systems that can be used effectively as part of the observation of the monitoring system. UAVs can rapidly produce geo-references (GPS accurate) or 3D maps that are more detailed and faster than satellite imagery. This mapping enables improved logistics, awareness of informal communities, damage assessments, disaster risk reduction or early warning activities, agricultural monitoring to promote food security, flood monitoring, etc. This type of mapping requires specialized equipment, software and training. In law enforcement have been using UAVs for patrolling and monitoring the criminal zones, monitoring of places of mass gathering of people, holding mass sports and entertainment events, demonstrations, spontaneous marches. Indispensable tool for special measures to ensure security in crowded places, holding rallies, demonstrations, in the field of Crowd Control.

Peacekeeping and military actors are also increasingly interested in using UAVs to support mission mandates, including the protection of civilians. The United Nations Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO) recently began using its own long-range UAVs for reconnaissance and data-gathering tasks, and has made these capacities available to humanitarian agencies[3]. Also should be given an example of the effective use of UAVs within suppress mass disorders and special operations in UN peacekeeping missions (in particular in the UN mission for stabilization in Haiti (MINUSTAH). Initially, for these purposes for crowd control and control of the operational situation in the area was used as the operational airborne surveillance military helicopters military contingent missions using high-resolution cameras with a direct signal broadcast in the operational headquarters, in real time despite the effectiveness of this technique revealed significant deficiencies in particular: the high cost of exploiting helicopters, maintenance, time lag from the time of receipt of the initial information and the subsequent departure of the helicopter in the area, as well as the vulnerability of helicopters is easy to detect targets by unlawful elements and a possible attack on him. The drones do not have all of these negative characteristics, capable to be deployed immediately to the area, monitoring the zone and transmit information to the control center in real time for quite a long period of time (depending on by UAV type, battery capacity, flight range and weather conditions), to change the patrol area as a result of the current operational environment, fly up to the object of observation at a fairly close distance, keep streaming media while remaining undetected, and can also be used under conditions of poor visibility in the dark, heavy weather conditions. This operation requires a minimum staff, only the operator of the drone and in some cases an assistant are qualified to operate this device. A drone operator is a person, organization or enterprise engaged in, or offering to engage in a drone operation. A qualification of drone's operator is a topic of great importance, however this is not the purpose of the article and requires separate consideration.

3 https://docs.unocha.org/sites/dms/Documents/Unmanned%20Aerial%20Vehicles%20in%20Humanitarian%20Response%20OCHA%20July%202014.pdf

The author, together with the Russian architect's group, had developed a multidisciplinary scientific project «Immunity Urban Safety System» for participation in the international competition of the UN "Habitat", in which the surveillance drones are serve as a sensor element of global security system to effectively prevent various threats at an early stage, including the threat of terrorist attacks by analogy with the surveillance cameras on the system safe city. As a means of mobile surveillance and at the same time an element of a possible attack warning systems, drones interact with law enforcement agencies and civil society in real-time transmitting urgent information[4].

Recently UAV technology is primarily limited to the sphere of surveillance: monitoring and recording audiovisual and other information on the terrain, which is caused by limitations of modern drone's technology (small capacity of modern batteries, management complexity UAV in the far distance, the instability in flight especially in difficult weather conditions, as well as on difficult terrain, the fragility of the structural elements, etc.). Now in Russian Federation from 2014 (starting with the Olympic Games "Sochi-2014"), composed of specialized aviation police units in many regions of the country, along with the usual helicopters for monitoring road conditions, aerial reconnaissance, anti-poaching, etc. actively used drones and various types of mobile systems support the actions which are mounted on the base of special vehicles, in the long term, taking into account the development of the UAV technologies, as well as the creation of software for artificial intelligence drones, perhaps any other use, in particular as a distinct element in the search activities, operational-investigative activity, the global security system, the means of production investigation.

However, the utilization of these devices should not be enclosed to the observation function. It is obvious that the use of UAVs is possible in the process of criminal investigation, the operational-search and crime search activities. In particular, in the providing investigative actions as a criminal detention, crime scene search, investigative experiment, a search on the ground, carrying out forensic examinations (such as situational).

Even so, unfortunately the drones are also possible to use for illegal purposes: such as weapons trafficking, illegal monitoring of private facilities, and they can be used by terrorists and criminal groups for their own purposes. There are some documented cases of the usage of drones for the transport of drugs, international analysts have warned of the possibility of delivery of explosives to carry out terrorist acts, and so on. Also it is necessary to point out the misappropriation of drones private organizations and individuals for violation of privacy, illegal obtaining of personal information, violations of rules of operation of the aircraft and the creation of public safety threats in crowded places. In this case, it is important to use the special police measures to deal with such objects. Japan has set up a special office for capturing unwanted drone, neutralizing them[5].

Development of the UAV technology faces a lot of challenges, one of the most important issue - human rights violations in the implementation of UAV in law enforcement. Drones sometimes consider as a new threat for civil society and human rights, especially the implementation of drones in war operations brings depraved reputation for UAV. According to the report of the American Civil Liberties Union (the ACLU) "The war has come home - the excessive militarization of American police" (23 June 2014) states: "Our regions are not areas of fighting and police officers should not treat us as enemies during the war. However, the multi-billion dollar order of military equipment annually allocated by the federal government for the needs of national and regional police departments[6]. Police are already too militarized

4 http://artdk.weebly.com/journal-arch-planetary-urbanism.html
5 LAW ENFORCEMENT GUIDANCE FOR SUSPECTED UNAUTHORIZED UAS OPERATIONS https://www.faa.gov/uas/regulations_policies/media/FAA_UAS-PO_LEA_Guidance.pdf
6 https://www.aclu.org/report/war-comes-home-excessive-militarization-american-police

and appearance of new powerful UAV technology may leads to mass human rights violations. Accomplishment of drones in law enforcement activity especially in crowd control and surveillance must be controlled and limited by human rights watching organizations.

Definitely further implementation of this technology requires its legislative regulation. Now, the use of UAVs is not well regulated and contrarily regulated in the international and national law. In the European Union, the European Aviation Safety Agency (EASA) developed "The concept of operation of the UAV"[7], according to which the drones are divided into three categories: OPEN, SPECIFIC and CERTIFIED. Open category does not require the permission of the aviation authorities to operate, but this type of drone flights have not carried out close to airports and places where people live, the flight altitude is limited to 150 meters, the use of drones carried out by the police surveillance. To use devices belonging to a special category must obtain permission of the aviation authorities, drone operators need to assess the safety of the flight, taking into account the airworthiness, the characteristics of use of the device, the competence of personnel, as well as the problems associated with the use of airspace. Certified category is for the UAV that can carry out flights in unrestricted airspace with controlled aircraft. The weight of such devices must be greater than 150 kg. Operators of such drones must have a special license, and the unit should receive a specific type of certificate, certificate of airworthiness and a noise certificate.

The US Federal Aviation Administration (FAA)[8] requires the registration of small unmanned aerial vehicles weighing from 250 grams to 25 kg. Those who run the UAV must be age 13 years or older, to provide their personal data. Owners drones when registering will receive a certificate with a special number, which should be applied to the UAV to make it clearly visible. When operating the UAV their owners are obliged to be in possession of a certificate in paper and electronic form. Office drones possible at a height no higher than 122 meters, and is always in the field of view of the operators, it is forbidden to control drones on groups of people over the stadium, for flights within 8 kilometers from the airport you need to get permission to air traffic controllers.

Russian Federal Law "On Police» art. 11 states that "the police in their work is required to use the achievements of science and technology, information systems, communication networks, as well as modern information and telecommunication infrastructure." According to the regulations in the Russian Aerial Code, issued in the beginning of 2016, the state registration shall be subject to all the UAVs weighing over 250 grams. drone crew may consist of one or more external pilots. One of them will be appointed by the owner of the aircraft commander, he decides to take-off, flight and landing UAV, and is responsible for the management of drone.

For regulation the procedure it is important to establish convinced technical and legal standards such as: requirements for the safe use as a UAV, crypto broadcasting protocol, standards for audio-visual filming and streaming, obtaining another forensic information. These standards should be set out in legal documents. But the exact possibility of receiving data using drones should be described in the Code of Criminal Procedure[9] because it is not only the question of collecting the evidence information but also the implementation of artificial intelligence in the criminal procedure.

Also it is necessary to define some specific practices of UAV applications in the field of crime investigation. As an example, we briefly observe the main conditions and benefits of applying police drones in the crime scene of traffic accident in the difficult conditions.

7 https://www.easa.europa.eu/system/files/dfu/204696_EASA_concept_drone_brochure_web.pdf
8 https://www.federalregister.gov/articles/2015/12/16/2015-31750/registration-and-marking-requirements-for-small-unmanned-aircraft
9 «Russian Aerial Code « 19.03.1997 N 60-ФЗ

Legend inputs: the traffic accident is happened in the autumn-winter time, dark period of time, in conditions of reduced visibility, complicated weather conditions, distant from the settlements area, there was a traffic accident on a large plot areas on a busy highway with the participation of a large number of vehicles, there were many victims need emergency, damaged the road surface, resulting in a large number of accident damaged vehicles blocked traffic, guilty by car fled the scene in an unknown direction, the information came from the accident witnesses.

Objectives: crime scene team need to be deployed in the scene at a short period of time, a remote area and the difficult weather conditions direct investigative team, in order to verify the information, confirm the fact of the crime, to conduct urgent investigative actions, especially examination of the scene, to obtain data on the accident situation, set the number of victims and the nature of his injuries, set the eyewitnesses, detect, capture and remove the traces of the crime, to produce photo-video footage, remove the samples for the production of forensic examinations.

The invented solution: the use of special police drone for an accelerated arrival at the scene, obtaining the necessary initial information, evaluation of the situation, determine the extent of the accident and necessary assistance in solving the problem, call the additional services and health care, securing traces of the crime, the production of photo-video recording, transmission other information in real time, and the possible establishment of a possible criminal prosecution and escaped from the scene.

Specifications and features of forensic drone: a modular UAV equipped with the autonomous electric motors, large capacity batteries, obtaining system of flight stabilization and balance, the navigating systems, an autopilot capable on its flight characteristics to the long flight of at least 1 hour with a maximum speed that is resistant to air turbulence, waterproof, with night vision system and land navigation, equipped with a high-resolution large-format cameras, motion sensors, weather and pressure detectors, laser measuring devices, gas analyzers, 3 D scanner module.

The algorithm stages: After receiving of the initial information the drone operator on duty reports the coordinates of the accident drone incident with a view to the direction of the UAV to the scene. Operator for a short time conducting preflight UAV: establishes additional necessary equipment, check the connection and the completeness of the drone, enters the coordinates of the destination, set the encryption key for the transmission of streaming data in real-time and on-board media, put flight program, taking into account the terrain and the weather conditions, conducting the necessary consultations with the investigator and operational staff in order to clarify the priorities during the inspection. After that starts the drone and forwards along the route. During the flight to the alleged scene of the incident controls the UAV and sensors for the possible adjustment of the route, following the consumption of the battery, the correctness of the on-board cameras and sensors. The drone preciously defines its geo position after arriving to the area of the alleged incident, defines the boundary of an accident, after which produces the survey, panoramic and detailed survey according to protocol, transmits photo and video in real time, said the accident zone, carrying circled the front area, the nodal method of inspection. Drone sends information to the command center and receives further instructions from the operator, searches for the braking track, it measures the detects biological traces, micro particles, photographing places of contact interaction of vehicles, their mutual location. After that it scans crime scene using onboard 3 D scanner. Upon completion of the algorithm, and the implementation of additional instructions drone operator is sent to the operator of the disappeared place of possible criminal prosecution carries, passing information to block the road. After the operation the drone back to the base, the operator retrieves the forensic information from the carrier board.

The benefits of application: the main advantage of the use of drones in this environment is the speed of response, flexibility and maximum coverage of the study area in the minimum time, the ability to remotely assess the situation quickly due to the translation, to implement the disclosure of crime in hot pursuit, the pursuit of the offender, to prevent change in the situation before the arrival of the investigating operational group.

Evaluation of the received information: as a result of the information obtained can be used as representation evidence in the criminal case, as an additional source of information for the production of forensic examinations, and 3 D model can be used for the reproduction of the causes and conditions of an accident, an investigative experiment in the future.

CONCLUSION

The implementation in law enforcement of robotic technology with elements of artificial intelligence is one the hot top scientific discussion nowadays, among them such as the technology of unmanned aerial vehicles (UAV). This technology is still under development, requires additional scientific researches, inventing new know-hows in the field of creating drones with sufficient battery capacity and flight stability, software reliability, data and maintenance security, utilization of these types of aircraft, testing and implementation in to the practice. Nevertheless, a key advantage of it is the possibility of remote sensing, monitoring areas, obtaining the necessary audio-visual and other data and transport of materials in complex difficult conditions.

UAVs come in a wide variety, but can be divided into classes based on size, range, and capacity for autonomous flight. The author proposes a classification of professional police drones, in accordance with their use in law enforcement activity. Depending on this use, you can select the following types of police drones: "The operation drones", "The inquiry drones", "The forensic drones". Recent years, the drones are used to apply as a component of geo-informational systems that can be used effectively as part of the observation of the monitoring system. UAVs can rapidly produce geo-references (GPS accurate) or 3D maps that are more detailed and faster than satellite imagery.

However, the utilization of these devices should not be enclosed to the observation function. It is obvious that the use of UAVs is possible in the process of criminal investigation, the operational-search and crime search activities. In particular, in the providing investigative actions as a criminal detention, crime scene search, investigative experiment, a search on the ground, carrying out forensic examinations (such as situational). These capabilities, make this new technology particularly important to security forces, the implementation of drones in law enforcement is based on long time researches and could be promising technology in the nearest future, but it still requires further development of technical parameters and regulatory in law issues.

REFERENCES

1. Wagner, Markus, Unmanned Aerial Vehicles (March 24, 2015). Max Planck Encyclopedia of Public International Law, Rüdiger Wolfrum, ed., Oxford University Press, Forthcoming; University of Miami Legal Studies Research Paper No. 15-12. Available at SSRN: http://ssrn.com/abstract=2584652http://artdk.weebly.com/journal-arch-planetary-urbanism.html
2. LAW ENFORCEMENT GUIDANCE FOR SUSPECTED UNAUTHORIZED UAS OPERATIONS https://www.faa.gov/uas/regulations_policies/media/FAA_UAS-PO_LEA_Guidance.pdf

3. https://www.easa.europa.eu/system/files/dfu/204696_EASA_concept_drone_brochure_web.pdf
4. https://www.easa.europa.eu/system/files/dfu/204696_EASA_concept_drone_brochure_web.pdf
5. https://www.federalregister.gov/articles/2015/12/16/2015-31750/registration-and-marking-requirements-for-small-unmanned-aircraft
6. https://www.aclu.org/report/war-comes-home-excessive-militarization-american-police»
7. https://www.federalregister.gov/articles/2015/12/16/2015-31750/registration-and-marking-requirements-for-small-unmanned-aircraft
8. «Russian Aerial Code « 19.03.1997 N 60-ФЗ.

UDC: 343.983:[001.891.5:005.71(497.16)

THE ACCREDITATION OF FORENSIC LABORATORIES OF SOUTH EAST EUROPE THROUGH THE PROJECT FACILITATED BY THE OSCE MISSION TO MONTENEGRO AND MONTEGRIN FORENSIC CENTRE

Aleksandar Ivanović, PhD[1]
Ministry of the Interior of Montenegro,
Police Directorate, Forensic Centre
Vladimir Ragozin
OSCE Mission to Montenegro
Dragica Vučinić
OSCE Mission to Montenegro

Abstract: It is known that in the recent years the international forensic cooperation constitutes one of the pre-conditions to effectively fight cross-border organized and serious crimes and corruption, therefore the analysis of the forensic evidence must be aligned with the international standards of quality. The European Union (EU) Council Decision 2008/615/JHA of 23 June 2008 'on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime', considers effective data exchange between Member States as essential, and other countries within the terms of the Prüm Treaty Agreement. Moreover, the European Association of Forensic Science Institutions (ENFSI in the later text)[2] has passed an immediate task to all Member States to accredit police forensic laboratories under the international standard ISO 17025 by the end of 2013. As a fully-fledged member of ENFSI since 2009, and having in mind that Montenegro has status of the EU candidate country, the Forensic Centre of the Police Directorate, Ministry of Internal Affairs of Montenegro (FC PD MN)[3] has successfully finalized this process and received accreditation as ISO/IEC 17025 forensic service provider within the estimated time period. During the accreditation process, and after obtaining the same, Forensic Centre of the Police Directorate in close cooperation with the OSCE Mission to Montenegro and with its full support, has initiated a series of projects in the area of the forensic evidence involving the countries of the Southeast Europe.

These projects, conducted in the period from 2013 until 2015, in which the Forensic Centre of Montenegro acted as a mentor laboratory to the similar forensic institutions from the region, aimed at the following: exchanging of knowledge and experience in the field of accreditation according to ISO 17025.

The majority of the project activities in the form of regional meetings, workshops and conferences were held at the premises of the Forensic Centre in Danilovgrad, Montenegro. Moreover, one number of events was organized at the regional forensic centres in: Tirana, Sarajevo, Banja Luka, Belgrade and Skopje. In addition, countries that were involved within the initial phases of this project were Greece, Moldova and Turkey. The main achievements of the long-term OSCE and Forensic centre project have been notified in the course of 2015 when it was noted that the region of the Southeast Europe has greatly advanced in the inter-governmental cooperation when it comes to forensics.

Keywords: forensics, accreditation, ISO/IEC 17025, criminal justice, regional cooperation.

1 E-mail: ialeksandar@t-com.me.
2 http://www.enfsi.eu/.
3 http://www.mup.gov.me/upravapolicije/naslovna/Forenzicki_centar.

INTRODUCTION

Accreditation of forensic operations in the countries of the European Union began for practical reasons. In fact, cross-border crime and terrorism have forced European countries to more intensive and coordinated police co-operation. This collaboration includes, *inter alia*, forensic and operational cooperation, which is the highest and most seen in the transnational exchange of forensic data such as DNA profiles, primarily, followed by fingerprints and other forensic biometric and other data.

This led to a frequent and pertinent situation, enabling that the forensic information obtained in one country are used as evidence in the police investigation, as well as at the court procedure of another country. Consequently, this situation stemmed to introducing a common forensics' standards for all European member states. Obviously, the European Union, as a multinational space that guarantees high standards in the field of rule of law and security was anticipated to respond first by providing tools for introduction of such standards. Therefore, the Council of the European Union adopted Decision 208/615/JHA "Increasing cross-border cooperation, particularly in combating terrorism and cross-border crime" on 23 June 2008[4]. This decision provided framework for effective exchange of forensic databases between the EU countries and subsequently enabled identification of the perpetrators suspected for criminal acts of terrorism and transnational crimes.

With the goal to make the aforementioned decision dependable, operationally and legally standardized, the need occurred to adjust it with the itemized requirements. Situation was fixed with the Council Framework Decision 2009/905/JHA dated of 30 November 2009 on accreditation of forensic service providers carrying out laboratory activities[5]. Decision was directed on providing reliability, usability and compatibility of the forensic data (for now, DNA profiles and fingerprints) from one country to another.

In order to implement goals and provisions of the 2009/905/JHA, all EU Member States have been tasked to have at least one forensic institution accredited by the international quality standard ISO/IEC 17025. Namely, Article 5 of 2009/905/JHA clearly demonstrates this requirement as an imperative in acknowledging forensic examination, analysis, research and expertise, so each Member State must comply with all strict conditions required by quality standard ISO/IEC 17025. As it is prescribed and toughly instructed by Article 7 of the Decision, the EU Member States are required with the following:

1. DNA Laboratories accreditation by 30 November 2013;

2. Dactiloscopy accreditation by 30 November 2015;

3. National legal frameworks have to include Council Framework Decision 2009/905/JHA by 30 May 2018;

4. The Council of the EU will perform control of the implementation of this Decision in the Member States by the end of 2018.

ACCREDITATION OF THE FORENSIC LABORATORIES IN THE BALKANS REGION

The Forensic Centre of the Police Directorate, Ministry of Internal Affairs of Montenegro (FC-UP-MUP) in Danilovgrad and the National Crime-Technical Centre of the Ministry of Interior of the Republic of Serbia in Belgrade, as unique institutions of its kind in Montene-

4 http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014459%202010%20INIT.
5 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009F0905.

gro and Serbia have been full ENFSI members since 2009. The most important pre-condition for the country membership in the ENFSI was the laboratory accreditation in line with the international standard ISO 17025. The aforementioned forensic institutions in Danilovgrad and Belgrade have went through the accreditation process through implementation of the European Commission's monopoly projects on European Mentoring for forensic accreditation[6] started in 2011. Mentoring laboratories in the project EMFA-2 were the Institute of Forensic from Tallinn for the Forensic Centre in Danilovgrad, and the Centre for Forensic Expertise from Zagreb for the National Crime-Technical Centre in Belgrade.

As it was already mentioned in the Introduction, one of the goals of accreditation is synchronization and compatibility of forensic tests and their usage in the fight against organized, mostly transnational crimes. However, some forensic laboratories from the Balkans region are not the members of ENFSI neither they are accredited. The above-mentioned facts, and in particular, the absence of accreditation, opens a challenge in the police work and investigative cooperation between the countries of the Balkan region. Namely, in processing of the cross-border crimes (which are very frequent in this particular region), it is obvious that some forensic data such as DNA profiles, fingerprints, results of drugs expertise, traces of explosives, motor vehicles and the like should have to be exchanged between the criminal justice systems of the respective countries. Unfortunately, this form of police cooperation and forensic data exchange are likely to happen only between the countries which have laboratories accredited to the international standard ISO 17025.

Considering the aforementioned situation, and in order to assist to national partners in strengthening the regional cooperation in the field of criminal justice cooperation with other Western Balkan countries, through harmonization and achieving compatibility of work of forensic laboratories, the Organization for Security and Cooperation in Europe, Mission in Montenegro, Podgorica (OSCE OMIM afterwards) has together with the FCUP-MUP implemented a number of projects in this area. The projects were conducted in line with the OSCE OMIM mandate, priorities of its Security Cooperation and Rule of Law programmes as well as needs defined by the Government of Montenegro, Police Directorate in specific.

The joint OSCE OMIM – FC project "Accreditation of forensic laboratories according to the standard ISO 17025" began in 2013 by boosting networking activities of the forensic laboratories of the Balkans region; producing a mapping plan directed toward laboratories accreditation, and supporting involvement of experts from the ENFSI. ENFSI experts have provided the theoretical and practical education in the field of forensic accreditation according to ISO 17025. The abovementioned project considered the following activities:

- Preparation of documents for quality management control. All management quality control documents were produced in uniform templates, in order to be compatible and usable in all countries participating in the project;

- Authentication of forensic methods. The OSCE OMIM project is implemented in accordance with international standards, and is aligned with the EU legal framework, in particular the Council of Europe Framework Decision 2009/905/JHA, the priority in the paper is given to the validating DNA methods and drugs analyses and

- Preparation and application for accreditation before the relevant National Accreditation Body/es in the particular countries. This project's phase was mainly dedicated to implementation of key provisions of the ISO 17025, Management review and internal audit.

Project participants were the forensic laboratories of the Ministries of Internal Affairs in Ankara, Athens, Banja Luka, Belgrade, Chisinau, Sarajevo, Skopje and Tirana. Educators and mentors in different project phases have been the ENFSI's experts: Mr Nouteboom Wim and

6 http://www.enfsi.eu/projects/other-running-projects.

Mr Mark Dorsteen from the Forensic Institute in the Hague, and Ms Merike Rump from the Forensic Institute in Tallinn.

After several workshops, study visits and expert assessments, this project has brought the following results:

- Forensic Centre in Danilovgrad was accredited by the international quality standard ISO 17025 in December 2014;

- Centre for Criminal Technique in Skopje in 2014, admitted to full membership of ENFSI, with a commitment to complete accreditation process in the next three years;

- Forensic institutions from Tirana, Sarajevo, Banja Luka, and Chisinau have developed general documents for the management quality control, compatible with the international standard ISO 17025, and therefore usable in all countries of the Balkan region.

AKREDITACIONO TIJELO
Crne Gore
ACCREDITATION BODY
of Montenegro
Podgorica

Crna Gora
Montenegro
ATCG – 0037

Na osnovu člana 10. Zakona o akreditaciji dodjeljuje
Pursuant to the Article 10. of the Law on Accreditation issues

SERTIFIKAT O AKREDITACIJI
Accreditation Certificate

kojim se potvrđuje da organizacija
which confirms that

MINISTARSTVO UNUTRAŠNJIH POSLOVA
UPRAVA POLICIJE CRNE GORE
Forenzički Centar
Grupa za hemijska ispitivanja

Li 14.19
akreditacioni broj
accreditation number

zadovoljava zahtjeve standarda
meets requirements of

MEST EN ISO / IEC 17025 : 2011

i kompetentna je za obavljanje poslova ispitivanja
and is being competent for performing the assessment tasks

koji su specifirani u utvrđenom obimu akreditacije
which are specified in the defined scope of accreditation

Datum dodjeljivanja akreditacije: 25.12.2014. god.
The date of the accreditation granting

Akreditacija važi do: 24.12.2018. god.
Accreditation valid until

Direktor
Director
Ranko Nikolić

Figure 1: *Accreditation Certificates according to ISO 17025: Forensic Centre in Danilovgrad.*

By working continuously on the establishment of police cooperation in the countries of the Balkans region, the OSCE OMIM and FC Danilovgrad have jointly implemented a project entitled "Strengthening regional cooperation in the field of forensic science" in the course of 2015. The project included forensic laboratories from Tirana, Sarajevo, Banja Luka and Danilovgrad which are organizationally structured within the Police Directorates of their respective countries. The Forensic Centre in Danilovgrad, as the only accredited laboratory, from

laboratories involved in the project, as well as an active ENFSI member, has been identified as a mentor laboratory to the other interested parties. Therefore, forensic experts in the areas of management in forensics, DNA and narcotics expertise have conducted working visits and missions to "mentee" laboratories with the following objectives and tasks:

- Introduction into document management quality control;
- Introduction into the protection and transmission of electronic forensic data;
- Introduction to the method of receiving and delivery of evidence, establishing the so-called "chain of evidence";
- Introduction to the maintenance and calibration of measured and other forensic equipment;
- Introduction to the method and efficiency of participation in inter-laboratory forensic tests.

Following the analytical processing of the forensic data in the above mentioned laboratories, there was a workshop conducted on the topic "Implementation of forensic standard ISO 17025: Internal audits, corrective and preventive measures" at the Forensic Centre in Danilovgrad. Participants of the workshop were, divided in the theoretical and practical part, all representatives of the said forensic laboratories. The Forensic experts from Danilovgrad presented the importance of internal audits in the forensic laboratories as one of the most important activities of quality control management in the first theoretical part. The objective of the internal audits is to define and determine discrepancies in the work of forensic laboratories. Also, counter measures for removing non-conformities was presented through defined preventive and corrective measures.

After the theoretical part, the workshop had its practical application, which considered the implementation of internal audits in the laboratories of the Forensic Centre in Danilovgrad, in particular in the management of quality control department, DNA laboratory and in the laboratory for chemical testing of drugs. Furthermore, an internal audit has also involved treatment of evidence in the forensic laboratories, or scientifically called "chain of command". This activity was of key importance, since the implementation of preventive and corrective measures excludes the possibility of any suspicion that the evidence might be possibly replaced, modified, changed *post-festum* and/or contaminated.

Workshop participants have been acknowledged with certificates of attendance of the workshop, and this verifies that they can conduct internal audits in their laboratories in relation to the standard ISO 17025. This certificate allows them also to perform "cascade training" and to transfer their knowledge to the colleagues from the same laboratory.

CONCLUSION

Quality standard in the area of forensic testing, research, analysis and expertise is of great benefit to international cooperation in the fight against transnational crime and terrorism. The quality standards cover the entire forensic process from the moment of the crime scene: crime scene examination, laboratory testing, interpretation and reporting of test results, exposure of the forensic opinions during the trial process.

The European Union through the ENFSI association has implemented a project in which all members of ENFSI forensic laboratories have achieved accreditation according to the forensic quality standard ISO 17025. In this way they have achieved compatibility of forensic work and the results of forensic tests on the entire territory of the European Union and other countries which are ENFSI members. Some countries of the Balkan region are still not mem-

bers of ENFSI neither have accredited forensic laboratories yet. This represents a problem in the fight against organized cross-border crime, not only between those countries, but also throughout the Europe. As crime knows no boundaries, the fight for the identification of the perpetrators of the crimes should be done at broader international level. Nevertheless, this international police cooperation must be conducted by internationally recognized, compatible, and moreover reliable methods of work, techniques and technologies which should be revised or repeated if required. This goal might be achieved if all Balkan countries (which are *de facto* part of the European space) are accredited according to ISO 17025.

In working toward fulfilling the above mentioned conditions, the OSCE OMIM and FC Danilovgrad have achieved the following accomplishments over the period from 2013-2015:

- Participants of the project, Forensic Centre in Danilovgrad and the National Crime-Technical Centre in Belgrade were accredited in 2014 according to the international standard ISO 17025. The Crime Technical Centre in Skopje has built up personal and technical capacities in order to obtain accreditation by the same standard. This achievement, together with accredited forensic laboratories in Athens and Ankara (which have been accredited before the particular project) provides an interstate space in which all the forensic examinations, analysis and expert evaluations are carried out in the same way. Therefore, operational exchange of forensic data in the criminal justice systems of those countries is possible and feasible.

- Accomplishing a high professional level of work in forensic laboratories which have not been accredited yet, such as laboratories in Sarajevo, Banja Luka, Tirana, Skopje and Chisinau. Many of these laboratories have expanded the scope of their work and activities in individual expertise, mostly in the expertise of narcotics.

- Implementation of inter-laboratory tests. Joint participation of the Balkan region in inter-laboratory tests is one of the important activities of this joint OSCE OMIM-FC Danilovgrad project, to ensure a high level of professionalism in the forensic laboratory. These testing have to ensure reliability and inter-country recognition of certain forensic tests. Within this particular project, interstate forensic tests have been implemented primarily in the fields of ballistics, followed by chemical and fingerprint tests.

- Progress aimed at usage of forensic methods, techniques and technologies in the fight against terrorism and cross-border crime. It is known that the fight against terrorism and cross-border crime are priority of law enforcement and rule of law institutions. In this regard, forensic laboratories have been actively involved in this issue in latest years. Of course, the contribution of forensic experts must be harmonized with the European Union legislation, and this is especially true for a framework decision of the Council of Europe 208/615/JHA "Increasing cross-border cooperation, particularly in combating terrorism and cross-border crime". The trend is that all European countries comply with these and other decisions of the European Union, not just the Member States. To achieve that aim, the joint OSCE-OMIM and FC Danilovgrad project, presented in this paper, contributes to achieving the objectives set out in the document of the European Union "Council conclusions on the vision for European Forensic Science 2010 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe".

- Work on the validation of test methods of trace DNA and traces of drugs, which made the expertise obtained in any country of the Balkan region (which were covered by this project) usable in other countries. This is of great importance in cases when it is necessary to trace DNA and/or evidence of drug use, which was found during the commission of a crime in one country.

REFERENCES

1. Bjelovuk I., Kesic T., Radosavljevic-Stevanovic N., *The accreditation of forensic laboratories - status and perspectives in Serbia.* Thematic collection of essays *Crime scene investigation of criminal offences* (editor prof. dr. D. Kolaric), Academy of Criminalistic and Police Studies, Belgrade, 2013, pp. 159–172.
2. Caddy, B., Thorpe, J.W. (1998) Communication Skills and Expertise in the Inquisitorial and Adversarial Legal System, ENFSI Meeting Madrid.
3. ENFSI Board (2005), BRD-GEN-003 Code of Conduct.
4. ENFSI DNA Working Group (2010). DNA-Data Management, Review and Recommendations.
5. ENFSI project (2003). QC-CAP-003. Performance Based Standards for Forensic Science Practitioners.
6. ENFSI Standing Committee for Quality and Competence – QCC (2004), QCC_CAP_003 Performance Based Standards for Forensic Science Practitioner.
7. ENFSI Strategic plan 2008–2011 (2008).
8. *EU Council Framework Decision 2009/905/JHA* of 30th November 2009: Accreditation of forensic service.
9. Golja, J. (2004). Kriminalističnotehnično izvedenstvo v Evropi in v Sloveniji. Dnevi varstvoslovja – zbornik, povzetek 98.
10. Golja, J. (2007). Kriminalističnotehnični dokaz. Posvet dokazovanje v težkih primerih, UNI Maribor. Maribor.
11. Golja, J. (2010). Forenzika u Evropskoj Uniji. Expertus Forensis No 14-15. Udruženje sudskih vještaka Crne Gore.
12. Ivanović, A., Merike Rump (2011), ACCREDITATION PROCESS FORENSIC CENTER OF MONTENEGRO TO THE MENTORSHIP OF THE EUROPEAN UNION (Projects EMFA-2). 10th Symposium of forensic sciences. Bratislava. Symposium Journal.
13. Simonović, B. (2009). Standardizacija i akreditacija kao jedan od načina profesionalizacije policijske i kriminalističke službe. Bezbednost No 1-2/2009.

UDC: 343.983:575.113]:005.6

ESTABLISHING QUALITY SYSTEM IN ORDER TO IMPROVE RESULTS OF DNA SAMPLE ANALYSIS DURING FORENSIC PROCESS

Lazar Nesic[1]
Jasmina Vuckovic[2]
Andjelko Maric, MSc[3]
Ministry of the Interior of the Republic of Serbia,
National Crime-Technical Centre

Abstract: Based on biological evidence found on the crime scene, it is possible to perform genetic profiling using modern techniques of DNA analysis. This provides one of the most important scientific evidence. Considering great importance of identifying biological traces, attention has to be directed to the problem of contamination during identifying, collecting, preserving as well as processing DNA evidence. Contamination can occur at any stage of the forensic process, and particularly it can be a significant problem during the forensic examination. As it is impossible to completely eliminate DNA contamination, considering the prevalence of human DNA in living and working environment and growing sensitivity of sophisticated DNA methods, all participants in the forensic process have to be aware of the importance of preserving the integrity of the evidence. For these reasons, it is necessary to take corresponding precautions that will prevent contamination, degradation or destruction of biological evidence during crime scene investigation or during the later stages of the forensic process. Implementation of the quality system will improve the quality of work on the crime scene and in the crime laboratories which will further on provide valid results and reliability of the physical evidence.

In this work there will be presented sources of contamination of DNA samples, the current internationally recognized documents which define minimum preventive measures in order to prevent the loss, destruction or contamination of evidence (securing DNA evidence, the strategy of performing crime scene investigation in order to use the material for DNA profiling that can provide reliable results, ways of keeping and storing biological evidence that will preserve the integrity of the evidence in criminal proceedings), and the way how the occurrence of contamination during the forensic process will be controlled. Detecting contamination source is potentially allowed with this, which facilitates the adoption of efficient improvement and the use of corrective measures, with the aim of improving the results of DNA sample analysis.

With the expansion and improvement of cross-border exchange of biometric data, including DNA, especially in Europe, as a result of the Prüm Decision, the integrity of DNA and exchange of information related to the contamination become increasingly important. Knowledge about the mechanisms how DNA contamination can occur is still in the process of development and it will continue in line with the evolution of the DNA profiling technologies.

Keywords: quality system, biological traces, contamination, the integrity of physical evidence.

1 lazar.nesic@mup.gov.rs
2 jasminavuckovic@gmail.com
3 andjelko.maric@mup.gov.rs

INTRODUCTION

Biological evidence, as carriers of DNA samples, is considered today as the most important evidence admissible in court proceedings. DNA molecule contains genetic information which is unique to each individual, except monozygotic twins. With analysis of DNA molecules it can be performed identification of a person, and in that way it is possible to use those findings in forensics in order to identify offenders. The technology of DNA research has been greatly improved since its establishment. On the other hand, procedures and techniques of collecting and handling evidence do not follow the latest developments in forensic DNA samples analysis, which, as a consequence, often has contamination, degradation, destruction of actual DNA samples found on the crime-scene. The implementation of strict standards how to handle biological evidence in this area will reduce the contamination of DNA and its consequences. Understanding the origin of the contamination and the ability of crime scene technicians to detect, collect and properly assess biological evidence enables preventing the occurrence of contamination and maintaining the integrity of forensic evidence.

In order to achieve valid and reliable results, it is necessary to define and implement forensic procedures of collecting, packaging, labeling, storing, transporting biological evidence to forensic laboratories. Omissions during these procedures can lead to contamination, degradation and loss of biological evidence. In addition, it is necessary to provide a chain of custody of evidence to be established throughout the whole forensic process.

Performance and efficiency of the method can depend on the quality (degree of degradation), purity (presence of foreign particles) and the total amount of DNA molecules in isolator, before performing a genetic analysis, the estimation of these parameters is executed. For these reasons it is necessary to implement a strategy for finding, processing, packaging, analyzing biological material in forensic laboratories and thereby to establish a quality system in forensic laboratories in order to achieve valid results of forensic DNA analysis. Creating a DNA elimination database is recommended as an additional procedure for quality assurance. It is very important to establish a DNA profiling and to enable the use of DNA evidence, its analysis and exchange at national, regional and international level.

EUROPEAN LEGISLATION FOR ESTABLISHING QUALITY OF FORENSIC WORK

Contamination is a serious problem that can destroy evidence and jeopardize criminal proceedings. It isn't possible to clearly eliminate contamination of DNA samples, but with the strategic planning of implementing certain preventive measures there can be prevented problems that may arise during the collection and handling of physical evidence. The principle of quality should be implemented at every stage of the forensic process. Quality management is the process which can improve the validity of the work on the forensic crime-scene. Quality should be established in each phase of the forensic process. Corresponding education and training, documented protocols and procedures and reliable equipment and supplies are part of the quality management process.[4]

Arranging protocols on a crime scene and elaborating procedures in the territory of the European Union are supervised by the European Network of Forensic Science Institutes -

4 Minimum requirements for crime scene investigation, IFSA, 2014.

ENFSI[5] within a special working group[6] - The Quality and Competence Committee[7]. The Committee makes recommendations for creating manuals relating to the competence and protocol procedures for crime scene technicians on the field and in laboratories, the validity and the use of corresponding methods, used in laboratories, developing awareness of the necessity of the quality of proceedings at the international level with respect to international standards in terms of accreditation of forensic laboratories. [8]

In order to prevent contamination, a set of regulations, instructions and manuals are published, which will help to establish quality systems in the field of handling, processing and analyzing DNA samples during the forensic process and thereby to ensure the integrity of biological evidence. The Manual, which the European Network of Forensic Science Institutes published (ENFSI GUIDANCE, GUIDANCE ON THE PRODUCTION OF BEST PRACTICE WITHIN MANUALS ENFSI (01/05/2008)) aims to ensure the principle of quality and access for detecting, recovering, testing and using evidence in forensic purposes, all in accordance with the requirements of ISO 17025 standards. The manual recommends methods and the most appropriate materials for packaging DNA samples.

ENFSI is one of the founding members of the International Forensic Strategic Alliance (IFSA), a global network of regional forensic network in all continents. International Forensic Strategic Alliance (IFSA) [9] has published a document that describes the minimum requirements for collecting DNA, analysis, and interpretation. The objective of documents is to establish fast a quality management system and scientific/ technical capabilities, and it includes the following framework:

1. staff competence;
2. equipment and supplies;
3. collecting, analyzing, interpreting, reporting;
4. procedures, protocols for validation;
5. quality management.[10]

Documents adopted in order to prevent contamination during the forensic process:

- FSR-G-206 is a document issued to provide guidance on how to control and avoid the occurrence of contamination during crime scene investigation, including collecting, packaging, transporting and storing samples before submitting them to forensic laboratories for analysis;[11]

- PAS 337 2012- Specifications for the supplies that are used for collecting, preserving and processing materials for forensic analysis;

5 ENFSI - The most important forensic association in Europe, founded in 1992. Within ENFSI Association there are 17 working groups.

6 Ljustina, A., Bjelovuk, I .: The international police co-operation aimed at improving security and combating environmental crime, Collection of work from the international scientific and professional conferences, Combating Crime and European Integration with emphasis on ecological crime, Trebinje 18-20. March 2014, p.113-124. Banja Luka, College of Internal Affairs, 2014 (Editor in Chief Dr Mile Sikman)

7 The Committee is entrusted with all responsibilities regarding the definition and implementation of quality management systems.

8 Zarkovic, M., Bjelovuk, I., Nesic L. (2010): Scientific evidence and the role of expert in criminal proceedings - European quality standards. Collection of work from scientific-expert conference with international participation: Combating crime and EU integration, Tara, p.235-244, Belgrade, The Criminal Police Academy and the Hanns Seidel Foundation

9 International Forensic Strategic Alliance (IFSA) is a multilateral partnership of six regional networks of operating forensic laboratories: ASCLD, ENFSI, SMANZFL, AICEF, AFSN, SARFS

10 Minimum requirements for DNA collection, analysis and interpretatin; International forensic strategic alliance **(IFSA),** A document for emerging laboratories, October 2014

11 Prevention and detection crime scene, *The Control and Avoidance of Contamination In Crime Scene Examination involving DNA Evidence Recovery,* March 2015

- ISO 18385 2015 *prevention consumables*- minimizing the risk of contamination from human DNA in items that are used for collecting and analyzing biological materials in forensic purposes;

- FSR-P-302 *detection crime scene, consumables, laboratory Protocol: DNA contamination detection –The management and use of staff elimination DNA databases;*

- FSR-G-208 *prevention, detection laboratory The Control and Avoidance of Contamination in Laboratory Activities involving DNA Evidence Recovery and Analysis*- This appendix provides the conditions, guidelines and recommendations primarily on measures against the contamination in the analytical phase of the investigation, that is, control and avoidance of contamination in the laboratory activities that involve handling DNA evidence and analysis.

PROTECTIVE MEASURES FROM CONTAMINATION

Contamination of DNA samples cannot be completely eliminated due to the prevalence of human DNA in living and working environments and growing sensitivity of sophisticated DNA methods. Precise and valid results of DNA samples analyzed by sensitive DNA analytical techniques (PCR) require solving the problem of DNA samples contamination throughout the whole forensic process.

From forensic scientific perspective, the activities can be observed in two phases:

1. phase of crime scene investigation process: finding, collecting, packaging, storing and transporting physical evidence.

2. analytical phase: performed in the laboratory, collected physical evidence is processed in forensic laboratories.[12]

Contamination of biological traces can occur at any stage of the forensic process. The main sources of DNA contamination:

1. forensic staff and their personal protective equipment;
2. contaminated supplies;
3. cross-contamination of DNA samples.[13]

Contamination can occur directly (saliva, dandruff) and indirectly (contamination of the biological sample through gloves).

The process of protection from contamination includes a combination of approaches of minimizing the possibility and risk of contamination and increasing the possibility of detecting contamination that has already occurred during the forensic process. Protective measures include two main areas of affecting:

- preventing contamination (using protective equipment, limiting access to a crime scene, testing the quality of equipment and laboratory areas, decontaminating previously used equipment);

- detecting contamination (the implementation of laboratory controls during the forensic process).[14]

The document FSR-G-206 foresees the following measures against contamination:

- collecting and packaging samples;

- transporting and storing DNA samples before submitting them to the laboratory for subsequent forensic analysis.

12 **FSR G 206**, The Control and Avoidance of Contamination In Crime Scene Examination involving DNA Evidence Recovery, Forensic Sceince Regulator, March 2015
13*Ibid.*
14*Ibid.*

It is necessary to apply the contamination risk assessment and strategy against contamination:

- on a crime scene - managing activities strategically in order to minimize the risk of contamination;
- before arriving at a crime scene: crime scene technicians, protective equipment;
- a strategy which will provide records of previous entries of all people on a crime scene, their activity;
- environmental factors: external conditions affect the risk of contamination;
- deployment of forensic staff, securing and protecting a crime scene.

PREVENTING CONTAMINATION ON A CRIME SCENE

Minimum required crime scene investigation process to perform includes establishing, monitoring and maintaining documented quality management system. [15] Regarding physical evidence, it is extremely important that there be a clear and precisely defined procedure how to handle physical evidence from the moment of detecting objects and traces on a crime scene, through recovering, packaging and transporting to the laboratory until they are presented in court. Therefore, it is necessary to establish a so-called chain of custody[16], that is, the process of documenting how material evidence was collected, analyzed, stored before it is presented in court proceedings. For these reasons, it is essential that there be awareness of personnel involved in the forensic process about preserving the integrity of evidence, taking appropriate actions to reduce the risk of transferring DNA samples on a crime scene or in other stages of the forensic process. Within the framework of training plans and manuals, risks and prevention of contamination are foreseen with specific processes and methods. If there is a doubt that certain evidence is contaminated by the negligent conduct, this circumstance has to be investigated by the professionals who are responsible for analyzing and providing expert opinions, to the extent that is reasonably possible to do so. [17] When there is a doubt that there was contamination, its cause needs to be determined, which is achieved by analyzing the forensic process backwards, step by step. Forensic experts will first assess the possibility of contamination, including contamination theory and understanding the way of contamination. The process of identifying the cause of contamination, conclusions and undertaken subsequent corrective actions will be recorded. All activities within the crime scene investigation have to be under the control of a properly trained person who has gained expertise in understanding the mechanisms of contamination, risk assessment and reduction, detection. This will include a manager with corresponding technical skills (assessment and review of the contamination, maintenance of the log when contamination occurred and periodical review of contamination trends, undertaking measures as a part of the overall process of continuous improvement).

Personal protective equipment has a dual purpose:

- To protect forensic personnel from contacting hazardous substances; and
- To protect biological material not to be contaminated by forensic personnel.

15 Minimum requirements for crime scene investigation, IFSA, 2014

16 Milosevic M., Kesic T., Bjelovuk I.,: The criminal justice system and the quality system in forensic laboratories, the Congress of Court Experts (II with international participation), Opatija 2010, Collection of work

17 Bjelovuk, I., Kesic, T., Radosavljevic-Stevanovic, N.: (2013). The accreditation of forensic laboratories - state and perspectives in Serbia; Thematic collection of work Crime scene investigation (Editor prof. Dr D.Kolaric), The Criminal Police Academy, Belgrade, p. 159-172

Wearing gloves and face masks is essential. Attention should be paid to keeping personal protective equipment in order to enable later sampling and analysis of equipment where it is suspected that there has occurred contamination of protective clothing used on a crime scene. [18]

PREVENTING CONTAMINATION IN FORENSIC LABORATORIES

Document[19] Minimum requirements for DNA collection, analysis and interpretation, issued by the ISA, defines the minimum education and training required for laboratory personnel for performing DNA analysis. The level of required education is based on the nature and complexity of tasks that need to be performed. There has to be a documented training curriculum within the laboratory, which will be used as a guideline for the assessment of technical skills and knowledge required for performing DNA analysis.

Every object or a trace, DNA profile carrier, has to be adequately preserved in order to maintain the quality and integrity of the evidence. The personnel that performs DNA sample analysis must have corresponding personal equipment: laboratory coats, disposable gloves, face masks, and all that with the aim of reducing the risk of contamination. Personnel will wear disposable gloves during DNA analysis. It is necessary to wear two pairs of gloves: the outer pair of gloves will be changed or thoroughly cleaned with a proven method for removing DNA effectively whenever they come in contact with contaminated surfaces (for example, opened evidence package, touching the face). [20]

Establishing a quality system in forensic laboratories stipulates the existence of certain technical conditions that have to be periodically monitored. Those conditions are related to the following: the existence of continuous power supply, air-conditioned laboratories, hermetically sealed windows, refrigerators and freezers for the storage of biological materials and supplies, clean water and properly separated premises. Biological samples will be stored in the premises protected from bacterial contamination, cross-contamination, heat and sunlight. Some biological samples may require to be freezed to prevent samples degradation. The access to biological materials has to be secured and controlled. The storage of biological samples and supplies have to be separated. [21] The laboratory needs to have instructions which control proper maintenance and servicing of instruments and equipment. Documenting will record cleaning and decontamination of facilities and equipment.

The conditions that must be established are related to the use of equipment in the laboratory. Tests and analysis of biological materials have to be performed in physically separated, clean laboratories, on decontaminated surfaces. Samples recovered from a crime scene, and reference samples should never be processed at the same time. After the samples, recovered from a crime scene, are processed, it is necessary to decontaminate work surfaces, and then to process the reference samples. Equipment and instruments used during items examination will be cleaned before and after each use in order to prevent contamination.

18 **FSR G 206**, The Control and Avoidance of Contamination In Crime Scene Examination involving DNA Evidence Recovery, Forensic Science Regulator, March 2015
19 Minimum requirements for DNA collection, analysis and interpretationn; International forensic strategic alliance (**IFSA),** A document for emerging laboratories, October 2014
20 **FSR-G-208,** The Control and Avoidance of Contamination in Laboratory Activities involving DNA Evidence Recovery and Analysis Forensic Sceince Regulator, 2015
21 (**IFSA),** October 2014.

DNA ELIMINATION DATABASE

In addition to forensic personnel, carriers with the risk of contamination can be the personnel engaged in manufacturing supplies, instruments and equipment. DNA contamination during the manufacturing process of forensic equipment and instruments can pose a major problem that directly affects the results of forensic DNA samples analysis. The task for manufacturers of DNA instruments and equipment is to undertake preventive measures, including the establishment of elimination database, automated contamination check. If the companies that manufacture equipment do not undertake certain measures to prevent contamination, it can lead to possibly incorrect forensic results. [22]

An example *The Phantom of Heilbronn*[23] proves that contamination can be a big problem during forensic investigations and it can lead investigation in the wrong direction. Therefore, it is important to implement standards relating to manufacturing and use of sterile supplies and equipment and to establish a DNA database of personnel in the process of manufacturing laboratory equipment and instruments. [24]

In 2014 the first draft of the standard ISO/DIS 18385[25] was published (Minimizing the risk of DNA contamination in products used to collect and analyze biological material for forensic purposes). Implementation of ISO/DIS18385 provides conditions for manufacturing equipment which is used when biological material needs to be collected during forensic DNA analysis. Products covered by the scope of this standard are consumable materials used for collecting evidence such as containers for packaging physical evidence with biological traces, as well as products used during performing DNA samples analysis such as test tubes, protective suits, gloves, masks and other consumable material. This standard is focused on the implementation of procedures related to health care and harm protection. The draft standard is currently being considered by the ISO participating member states.

Elimination base is considered as a precondition to achieve accreditation.[26] Establishing DNA elimination database quality system of forensic examination and analysis will be improved. It is often necessary to use elimination samples to determine whether the evidence comes from a suspect or any other person. Numerous forensic databases are established in order to solve the so-called global "cold cases" [27].

Within the Prüm Convention and the new Schengen Information System the specific handling with DNA and fingerprints in national databases are defined. The European Union offers a variety of options to facilitate the exchange of information between national organizations for law enforcement. The Prüm Decision[28] stipulates establishment and access to nation-

22 Balk, Carly (2015) "Reducing Contamination in Forensic Science," *Themis: Research Journal of Justice Studies and Forensic Science*: Vol. 3: Iss. 1, Article 12.
Available at: http://scholarworks.sjsu.edu/themis/vol3/iss1/12

23 "A woman without a face", The Phantom of Heilbronn, one of Germany's most sought-after women who had been leaving the biological traces in 40 crimes across Europe between 1993 and 2009. After research, it was discovered that the phantom woman was a woman who had worked in a factory for manufacturing swabs used in examination process.
http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1033&context=themis

24 Balk, Carly (2015) "Reducing Contamination in Forensic Science," *Themis: Research Journal of Justice Studies and Forensic Science*: Vol. 3: Iss. 1, Article 12.
Available at: http://scholarworks.sjsu.edu/themis/vol3/iss1/12

25 *ISO/DIS 18385 - Minimizing the risk of DNA contamination in products used to collect and analyze biological material for forensic purposes*

26 Codes of Practice andConduct, *Protocol: DNA contamination detection –Themanagement and use of staff elimination DNAdatabases FSR-P-302, 2014*

27 "Cold case" refers to a crime that has not been completely solved, but based on the new information and DNA sample analysis it can lead to decisive results of the investigation.

28 The decision on the national exchange of fingerprints and DNA profiles

al automatic databases of DNA profiles, fingerprints database, which will allow the country to ensure the availability of reference data. The availability of personal data and other information relating to the reference data are regulated by the national legislation. Contracting parties will provide access to reference data from the automated systems for identification of fingerprints where the subject can not be directly identified. [29] Prüm decisions, among other things, defines the level of data protection, data processing, accuracy and time for data storage, technical and organizational measures for the protection and security of data, the rights of the data subject.

The Schengen Information System (SIS) is now the most widely used information system for data exchange. The competent national authorities may use the information system for the purpose of issuing alerts on wanted or missing persons and facilities, both within and outside the European Union. SIS was updated at the beginning of 2015 in order to improve the exchange of information on suspected terrorists. [30] Council of the European Union made a legally binding instrument on simplifying the exchange of information and intelligence - the Swedish initiative that stipulates the exchange of information and intelligence; deadlines for submitting information and intelligence; means of communication and languages; protection, confidentiality and withholding of information or intelligence.

In 2001 INTERPOL was the first who published Handbook on DNA data exchange and practice. In order to meet the growing needs, INTERPOL has developed several tools for DNA data exchange. This includes the international DNA database, international search, bilateral exchanges and resources to secure standardized electronic transfer. [31] In 2015 INTERPOL has published recommendations for the establishment of national DNA databases, created for Member States that wish to establish a national DNA database. All activities related to the establishment and use of DNA database need to have a legal basis. Legislation should regulate collecting and using DNA profiles in the database, as well as provide guidance on the legal definitions of terminology, procedures for collecting samples, the conditions for storage/ destruction of DNA profile, information security in the database. [32] Interpol is committed to establishing international technical standards and systems in order to improve opportunities for successful cross-border cooperation.

National DNA databases have become one of the most effective means of providing information about unknown offenders. Databases have different organizational structures, depending on the national legislation in every country. [33] In 2015 ENFSI DNA Working Group published a document which defines recommendations for the management of DNA databases, including the criteria for inclusion, deletion and handling of DNA profiles.

FSR-P-302[34]*,* protocol provides requirements and recommendations for managing and using elimination database as the primary means of detecting contamination. Regulation FSR-P-302 stipulates the destruction of unused DNA materials that will be kept no longer than six months. The information which will be available and put into the database is in accordance with Prüm Decision.

29 Prüm Convention http://register.consilium.europa.eu/doc/

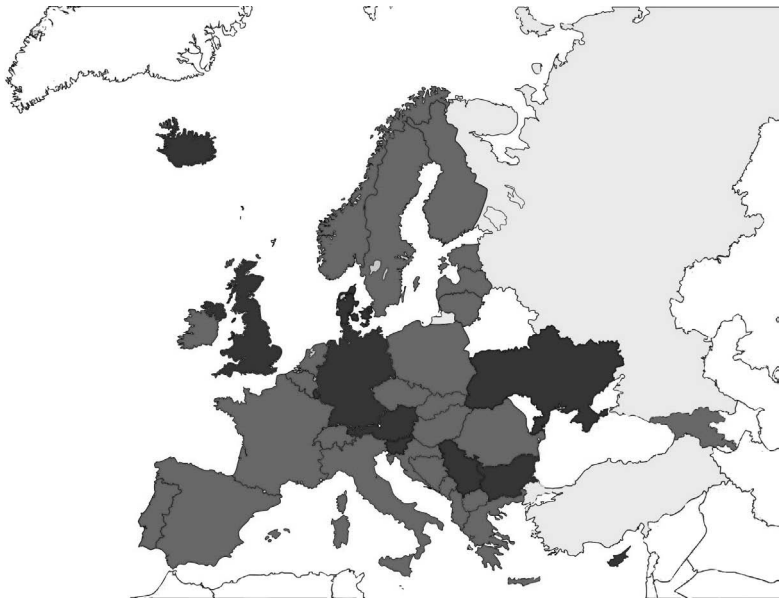
30 Comunication from the commission to the european parlament, the council, the European economic and socil commite and the commite of regions, European Commission, The European Agenda on Security, Strasbourg, 28/4/2015

31 Recommendations from the INTERPOL DNA Monitoring expert group, Second edition 2009

32 INTERPOL: DNA database , DNA monitoring expert group, 2015

33 Schneider M. P.: Expansion of the European Standard Set of DNA Database Loci—the Current Situation, Institute of Legal Medicine, University Hospital of Cologne, Germany, 2009

34**FSR-P-302,** Codes of Practice and Conduct, *Protocol: DNA contamination detection – The management and use of staff elimination DNA databases FSR-P-302, 2014*



Fugure 1: *Programs of DNA database that different European countries use - CODIS (red), independent DNA databases (blue), countries where there isn't any DNA database (yellow). Northern Ireland and Scotland have their own DNA databases, although their profiles are also in the National DNA Database of Great Britain*[35]

Within the National database of DNA profiles of Great Britain (NDNAD) there is an elimination database of forensic personnel that was established in 2000. Since 2003, a requirement for receiving new forensic personnel is to provide a DNA sample for registration in the "Police elimination database" (PED) and since October 2012, these profiles have been compared with a national DNA database as a part of the verification process. [36] There is no violation of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms if DNA samples are taken with the consent of a candidate.

A study performed in 2010 in Austria shows the rate of reported and confirmed contamination of 0.36%. Establishing the National "Police elimination database" (PED) in 2009, the number of detected contamination during the testing period 2000 - 2009 increased from 0.36% to 0.51%. For the period between 2010 and 2014, the number of contamination is 0.87%. Since the tool "Profile Comparison" GeneMapperT software[37] was installed in 2013, the identification of contamination has been improved. This improvement increased the rate of identified contamination for 1.2% in period 2013-2014.

35 DNA-database management review and recommendations. ENFSI DNA Working Group, April 2015
36 Ibid.
37 GeneMapperTM software (Life Technologies)

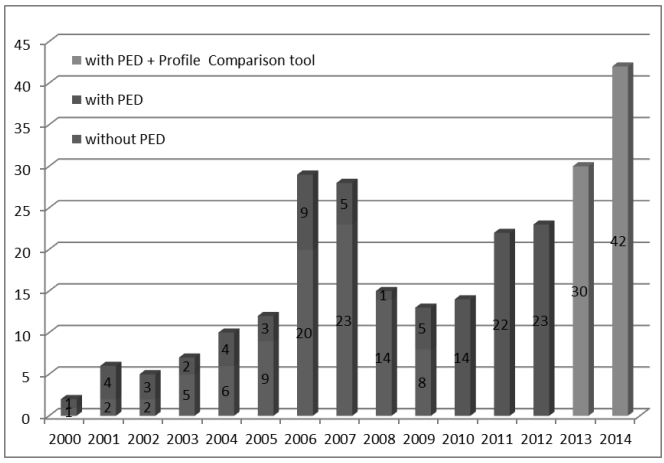


Figure 2: *Detected contamination incidents in the period between 2000 and 2014, before implementing PED (blue) and after (red), as well as combining the PED and tools "Profile Comparison" (green)*[38]

The results of this study show the potential and importance of reference databases which contain DNA profiles of police officers. The ostensible increase in the rate of contamination over the years does not point to an actual increase in the number of contamination, but it points to improved preventive measures for detection. [39]

The future use of the potential of DNA profiling is reflected in the innovative technique of forensic analysis - Forensic DNA Phenotyping - FDP. This method represents a new way of forensic use of genetic material that provides the ability to determine the physical features using only genetic material. FDP can identify gender with 100% accuracy, hair color, the color of the iris, height of a person, and many other physical features with a percentage accuracy of 70%.[40] This innovative technique of DNA profiling could be a powerful tool for forensic, historical and medical research. Forensic DNA Phenotyping refers to predicting physical appearance of unknown persons or unknown deceased (missing) persons directly from biological material found on the crime scene. "Biological witness" - FDP can direct the investigation when it is not possible to identify a person by current profiling using comparative analysis of DNA. [41] This technique is not accepted as evidence in court because some countries have completely banned the use of DNA phenotyping. Belgium and Germany do not allow the use of forensic FDP. The Netherlands restricts predicting features that are publicly visible as hair and eye color. [42]

38 Cemper-Kiesslich, J.; Dunkelmann, B.; Kreindl, G.; Müller, E.; Neuhuber F.; Pickrahn, I.; Zahrer, W.: Contamination when collecting trace evidence—An issue more relevant than ever?, Forensic Science International: Genetics Supplement Series, Department of Legal Medicine, University of Salzburg, Austria October 2015. http://dx.doi.org/10.1016/j.fsigss.2015.09.238

39 Neuhuber F. , Pickrahn I. , Dunkelmann B. , Müller E. , Kreindl G. , Zahrer W. , Cemper-Kiesslich J.: Contamination in Obtaining Trace Evidence – an Issue More Topical Than Ever? ; Institute of Legal Medicine, University of Salzburg, Austria, 26th Congress of the International Society for Forensic Genetics; 26th Congress of the International Society for Forensic Genetics Krakow, Poland August 31 – September 5, 2015 available at http://www.isfg.org/files/ISFG2015_Progr_abstract_HQ.pdf

40 Manfred Kayser: THE BIOLOGICAL ASPECTS OF FORENSIC DNA PHENOTYPING, Erasmus University Medical Center Rotterdam, Forensic DNA Phenotyping (FDP)

41 Manfred Kayser: Forensic DNA Phenotyping: Predicting human appearance from crime scene material for investigative purposes, Forensic Science International: Genetics, 18 (2015) 33–48

42 Polack, A.: Building a Face, and a Case, on DNA, 2015. http://www.nytimes.com/2015/02/24/science/building-face-and-a-case-on-dna.

Future innovative techniques and the existence of unidentified DNA profile database and possibility to exchange data on a global level, would greatly improve forensic research. However, the limits of scientific knowledge in the field of molecular biology and the question of ethics preclude the acceptance of this technique in order to prove in legal proceedings.

CONCLUSION

Valid results of forensic DNA analysis in the process of identification requires established quality system throughout the whole forensic process. Implementing the quality system will result in the improved quality of work on a crime scene and in forensic laboratories, which will ensure the integrity of biological traces. Once a laboratory system is established, it will continue to be controlled and continuously improve service quality through the process of accreditation according to international standards. Identification importance of DNA samples found on a crime scene is huge and therefore it is necessary to ensure the quality and integrity of the DNA evidence and to implement a system of measures against contamination. With these precautions, the contamination will be prevented, aw well as degradation or destruction of biological traces during the phases of crime scene investigation and during the analytical phase of the forensic process. The problem of contamination of DNA samples is not only within the framework of forensic process, but also outside it - contamination of equipment and instruments in the manufacturing process. For these reasons, an elimination database of DNA profiles is required which will be used to detect and remove the cause of the contamination. Preserving the integrity of DNA during the forensic process and the exchange of information related to the contamination will contribute to directing the investigation and solving crimes. Improving cross-border cooperation in the area of exchanging DNA data and information based on the Prüm Decision establishes a crucial basis in the fight against all forms of crime in Europe.

The existence of forensic DNA database is an important research resource in contemporary criminal justice systems. Storage, use and global exchange of DNA profiles allows comparison of samples found on a crime scene with reference samples. This enables automatic identification of a suspect. In order to obtain a DNA database it is necessary to meet the technical and technological, legal and ethical aspects.

REFERENCES

1. Balk, Carly (2015) "Reducing Contamination in Forensic Science," *Themis: Research Journal of Justice Studies and Forensic Science*: Vol. 3: Iss. 1, Article 12. Available at: http://scholarworks.sjsu.edu/themis/vol3/iss1/12
2. Bjelovuk, I., Kesic, T., Radosavljevic-Stevanovic, N.: (2013). *The accreditation of forensic laboratories - state and perspectives in Serbia*; Thematic collection of work Crime scene investigation (Editor prof.Dr D.Kolaric), The Criminal Police Academy, Belgrade, p. 159-172
3. Cemper-Kiesslich, J.; Dunkelmann, B.; Kreindl, G.; Müller, E.; Neuhuber F.; Pickrahn, I.; Zahrer, W.: Contamination when collecting trace evidence - An issue more relevant than ever?, Forensic Science International: Genetics Supplement Series, Department of Legal Medicine, University of Salzburg, Austria, October 2015. Available at: http://dx.doi.org/10.1016/j.fsigss.2015.09.238
4. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of regions, European Commission, **The European Agenda on Security,** Strasbourg, 28/4/2015

5. DNA-database management review and recommendations. ENFSI DNA Working Group, April 2015
6. FSR G 206, The Control and Avoidance of Contamination In Crime Scene Examination involving DNA Evidence Recovery, Forensic Science Regulator, mart 2015
7. FSR-G-208, The Control and Avoidance of Contamination in Laboratory Activities involving DNA Evidence Recovery and Analysis Forensic Science Regulator, 2015
8. FSR-P-302, Codes of Practice and Conduct, *Protocol: DNA contamination detection –The management and use of staff elimination DNAdatabases FSR-P-302, 2014*
9. ISO/DIS 18385 - Minimizing the risk of DNA contamination in products used to collect and analyze biological material for forensic purposes
10. INTERPOL: DNA database , DNA monitoring expert group, 2015
11. Manfred Kayser: THE BIOLOGICAL ASPECTS OF FORENSIC DNA PHENOTYPING, Erasmus University Medical Center Rotterdam, Forensic DNA Phenotyping (FDP)
12. Manfred Kayser: Forensic DNA Phenotyping: Predicting human appearance from crime scene material for investigative purposes, Forensic Science International: Genetics, 18 (2015) 33–48
13. Markanovic, M., Kosic, D., Kojic: *The use of DNA analysis in the process of identification of perpetrators; Safety - Police - Citizens*, year VII, no. 3-4/11458-465
14. Minimum requirements for crime scene investigation, IFSA, 2014
15. Minimum requirements for DNA collection, analysis and interpretation; International forensic strategic alliance (**IFSA),** A document for emerging laboratories, October 2014
16. Minimum requirements for crime scene investigation, IFSA, 2014
17. Milosevic M., Kesic T., Bjelovuk I.,: *The criminal justice system and the quality system in forensic laboratories*, the Congress of Court Experts (II with international participation), Opatija 2010, Collection of work
18. Pollack, A.: Building a Face, and a Case, on DNA, 2015 Available at: http://www.nytimes.com/2015/02/24/science/building-face-and-a-case-on-dna
19. Prevention and detection crime scene, *The Control and Avoidance of Contamination In Crime Scene Examination involving DNA Evidence Recovery,* March 2015
20. Prüm Convention http://register.consilium.europa.eu/doc/
21. Polack, A.: Building a Face, and a Case, on DNA, 2015. Available at: http://www.nytimes.com/2015/02/24/science/building-face-and-a-case-on-dna.
22. Recommendations from the INTERPOL DNA Monitoring expert group, Second edition 2009
23. Schneider M. P.: Expansion of the European Standard Set of DNA Database Loci - the Current Situation, Institute of Legal Medicine, University Hospital of Cologne, Germany, 2009
24. Ljustina, A., Bjelovuk, I .: *The international police co-operation aimed at improving security and combating environmental crime*, Collection of work from the international scientific and professional conferences, Combating Crime and European Integration with emphasis on ecological crime, Trebinje 18-20. March 2014, p.113-124. Banja Luka, College of Internal Affairs, 2014 (Editor in Chief Dr Mile Sikman)
25. Zarkovic, M., Bjelovuk, I., Nesic L. (2010): Scientific evidence and the role of expert in criminal proceedings - European quality standards. Collection of work from scientific-expert conference with international participation: Combating crime and EU integration, Tara, p.235-244, Belgrade, The Criminal Police Academy and the Hanns Seidel Foundation.
26. http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1033&context=themis

UDC: 343.982.34:004.932.2

COMPARISON OF RED OIL FINGERPRINTS ON MULTI COLOR BACKGROUND BY USING THE SPECTRAL IMAGING AND DIGITAL IMAGE PROCESSING TECHNOLOGY

Wang Dan, MA[1]
National Police University of China, Shenyang

Abstract: To extract the red fingerprint on EMS postal express envelope, the paper compared the results of the spectral imaging and digital image processing technology. The paper comprehensively describes the process in the application of complicated fingerprint extraction. Although the fingerprint is in good condition, there is interference by design chromatic stripe and red, yellow, and blue white colour background which increases the level of difficulties of the extraction work. Using digital image processing techniques and spectral imaging examination, a more satisfactory result can be obtained. The paper analyzes each processing step with detailed instructions, the similarities and differences between two different methods, advantages of each method and provides contribution for further similar cases.

Keywords: EMS envelope; red paint fingerprint; multi-colour background; the spectral imaging; digital image processing technology

INTRODUCTION

Spectral Imaging (Spectral imaging technology records objects within a certain range spectrum through the spectral imager inspection.) Dense uniform distribution of multiple narrow bands of monochromatic light reflexes brightness distribution or fluorescence intensity distribution formed by monochromatic light by using a set of a spectral image of special optical testing method. Spectral image sets objects in a collection and so on containing intervals. Spectral image records images of each image point. Counterpart brightness value information still contains material spectral information. [2]Each monochromatic image records objects in the corresponding wavelength of light degree distribution information; the combination of monochromatic images record the brightness of objects in all selected monochrome band distribution information. Using special spectral analysis and processing software, we can analyze the spectral image collection and processing and thus achieve what we need for test results and actual cases of spectral images; trace substance present spectrum is often traces and background material. Produced by mixed spectrum, you can use removed background spectrum in the mixed spectral analysis software, leave traces of matter spectrum, and define the background as a colour value, and after mixing, the spectrum is defined as a larger colour value and background contrast; digital image processing mainly uses the image in the spatial domain and frequency domain features and the screen image to obtain material evidence. In

1 E-mail: 857925823@qq.com.
2 Su Weighing: Training Tutorial of Criminal Image and Video Technique [M]. People's Public Security University of China Press.2010

the spatial domain processing we can use histogram tools such as the contrast, brightness, processing, as well as the layer and channels, and other functions of image processing in order to achieve the needed result. A lot of the masses image processing software has very good performance in the spatial domain processing.

Searching for new optical testing method of forensic science and broadening application range of spectral imaging technology. Academic papers and documents were collected to master advanced tendencies about spectral imaging domestic and overseas in forensic science area. Experiments were conducted to prove the ability of spectral imaging in testing difficult physical evidence. Spectral imaging technology can successfully solve various evidence identification problems including fingerprints, writing material, trace evidence and biologic evidence. According to the results of the experiment, spectral imaging has strong abilities in forensic science field. Spectral imaging technology has widely researched space and important practical applications which will open up a new optical testing method in forensic science.

The paper presents EMS postal express marks of a red envelope as an example, as well as the processing of the spectral imaging and digital image processing technology to do a comparison. Test conditions when the print is very good, but the background hinders stripes and text with blue, yellow and white colour. A more satisfactory result can be obtained using digital image processing technique and spectral imaging technology inspection. The paper presents the use of digital image processing and the use of spectral imaging inspection. Each processing step uses detailed instructions, compares the difference between two different methods, thus getting closer to a satisfactory result, analyzing the similarities and differences between two different methods to deal with, and analyzing the advantages of each method and optical inspection for similar evidence.

The paper analyzes the treatment of using Photoshop software to achieve processing fingerprints of such multi-hued background interference.[3] The use of Photoshop software to handle this process is relatively complex. The comprehensive utilization of the channel at the time of treatment, layers, and functional constituencies in order to get a satisfactory treatment effect defines concrete steps, which are as follows: red ink fingerprints post Express envelope will be the area of digital camera into the computer; the formation of the original image is to be processed; the original image is shown in Figure 1. For similar samples we can also use a scanner to scan the input; if the scanning resolution is best, it should be not less than 500dpi to ensure that the front and rear handle has a good imaging results. Fingerprints scanned original image format is not strictly limited, usually to save the JPG, BMP, etc. Photoshop software is easy to recognize.

Figure 1

Figure 2

3 ShuhuiGAO. "Digital red ultraviolet photographic extract potential on a smooth object refers towlines of the comparison research" [J]. Journal of Xinxiang police college, 2010,

Open Photoshop software in Figure 1-1 of the original image, as shown in Figure 2 to get the picture after the use of cutting tools cutting parts where the fingerprints are.

Select the image to be processed as shown in Figure 1-2, and enter the "Window" menu, select "Channel" option so that the original image appears in RGB mode, set out below and turn red channel (R), the green channel (G), the blue channel (B) of the option. Open a new blank image of Photoshop software, the same resolution as the original image, the image size is not smaller than the original image, choose white background content.

In the original image channel dialog box, select the blue channel option, as shown in Figure 3, and then in the "Image Adjust" menu select "inverted", shown in Figure 4. Select an image to copy it to a new blank image, as shown in Figure 5 Shows; we get the inverted image under the blue channel of the image.

Figure 3

Figure 4

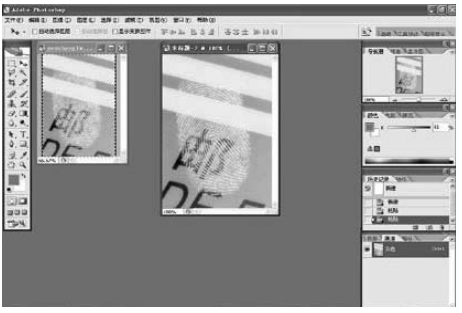


Figure 5

Figure 6

In the original image channel dialog box, select the green channel options, shown in Figure 6. All images which are selected will be copied to the new image, which requires inverting completely the cover what just made and without bias, as shown in Figure 7.

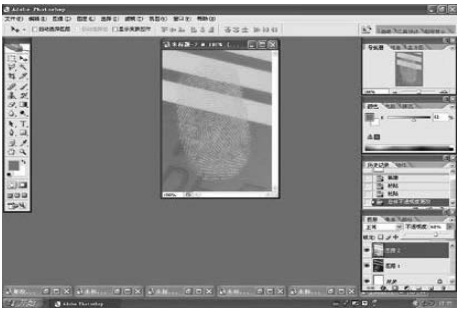


Figure 7

Figure 8

Select the new image (in this case it has two new layers above), click on the "Layers" option, thus setting out the two new layers and a background layer will be created. The two new layers of options were selected as "normal". Then adjust the opacity of the layer of the green channel of the original image; the background characters tend to disappear and hand-stamped lines have been highlighted. Continue to adjust until the fingerprint region of the text disappears; merge all layers, shown in Figure 8.

After merging layers, use the selection tool bright background Obscure line region selection, shown in Figure 9, the region do feathering. Pay attention to the feathering value that cannot be too general to be in five or less feathering on duty, as in Figure 10.

To perform domain inversion processing, shown in Figure 11, use the Levels tool to select the area for processing, shown in Figure 12. Adjust levels, until the tone background and the background outside the constituency are basically the same constituency after the abolition of the constituency as shown in Figure 13.

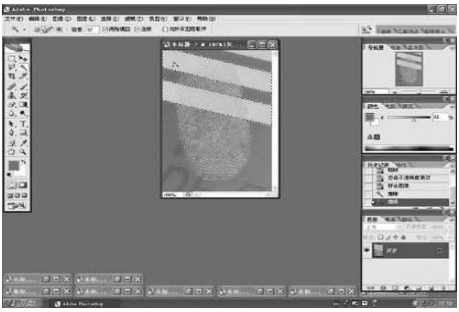


Figure 9

Figure 10

Figure 11

Figure 12

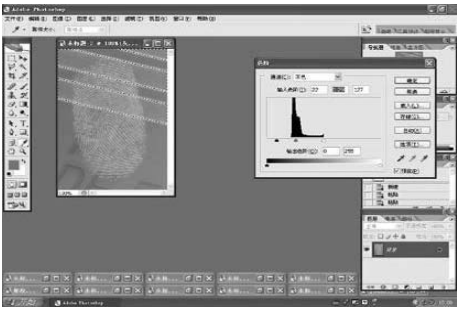


Figure 13

Figure 14

Use the Brightness / Contrast tool to adjust the entire image, shown in Figure 14 in accordance with appropriate adjustments to the image shown in Figure 15. Brightness and contrast until satisfactory fingerprint image obtained by Figure 16 shows the effect of treatment; then save it.

Figure 15

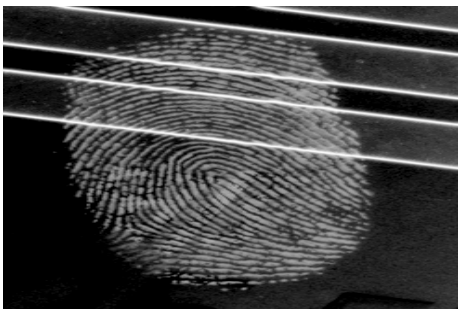


Figure 16

During the method treatments, the choice of the channel should choose the most contrast fingerprint image; disparity two channels are superimposed, so as to fusion at the time of background text fingerprints remain in certain contrast in order to make a better effect.

UTILIZATION OF SPECTRAL IMAGING TECHNOLOGY TO TEST TREATMENT

Herein the paper focuses on spectral imaging devices used for Cambridge Research & Instrumentation, Inc.[4] (CRI) produced Nuance-macro visible imaging spectrometer, which receives a spectral range of 420nm-720nm, using the spectral analysis software for analysis and processing software that comes with the device. Concrete steps for testing the use of spectral imaging technology to shoot and analyze the process are as follows:

Use spectral imager, in the "bright field" (Bright field) mode where the parts of fingerprints were taken from 420nm to 720nm, interval 10nm, obtain spectral image set of the fingerprints in the system; software interface is displayed in the form of pseudo-colour,[5]as shown in Figure 17. In CCD hardware settings such as selecting 8 -bit depth to the TIFF file format saves spectral image set; then the set of spectral images is saved in a folder. You can use ordinary plug-in software from 420nm to 720nm in Figure 31, shown as Figure 18.

4 XiaopingSun, Jingling. "All band material evidence examination CCD system applied in the field of criminal photography." Video- Technology. 2003

5 Ian Jun: Simple Tutorial of Criminal Photography [M]. People's Public Security University of China Press. 2002

Figure 17

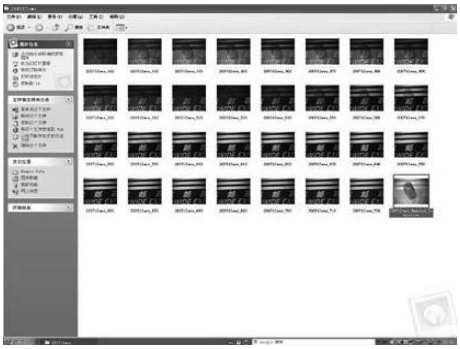


Figure 18

After saving the spectral image set, you can directly use the spectral image analysis software "Load Cube" to select the appropriate set of spectral images that directly open spectrum for image analysis and processing, shown in Figure 19.

After selecting spectrum feature (Spectra) in the toolbar, the corresponding spectroscopic processing interface appears. You can set to open on the spectral image corresponding spectroscopic processing operations for the faint fingerprints on the monochrome background, just to define a background colour value for the ridge to define a contrasting colour of the background to conduct a "de-mix" (Unix) operation to obtain satisfactory results. In order to facilitate the accurate assignment selected points on the spectrum, you can set the display image to enlarge. For obtaining a complex multi-tone background handprint, you need multiple manual "to mix" (Unix) operation. First, the yellow background is defined as white, mixed spectral fingerprints on a yellow background are defined as red. Use the "manual calculation spectrum" (Manual Compute Spectra) to calculate spectra. To obtain spectral values after mixing, it is defined as green, as shown in Figure 21.

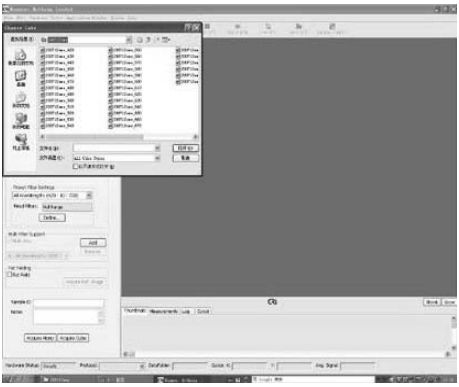


Figure 19

Figure 20

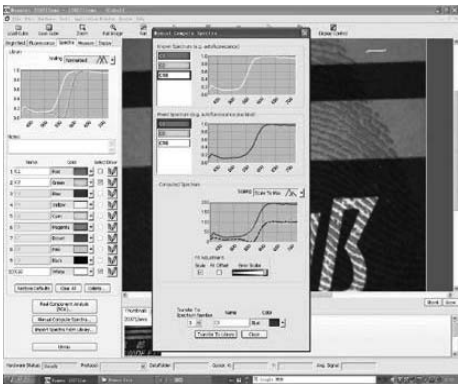


Figure 21

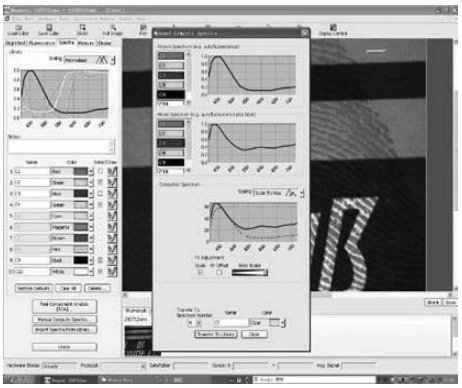


Figure 22

The fingerprint on blue and white background and the background of mixed spectrum is defined as different numbers, using manual calculation spectrum (Manual Compute Spectra) mix with spectrum to calculate mixed spectral values, as shown in Figure 23 and 24.

After three manual spectrum calculations operation were applied (Manual Compute Spectra) to obtain the spectral values of the three mixed number and three different values of the background spectrum, the background values of all three light colours defined value[6], such as white, while the three ones to mix spectral definition black after being bonded (UNIX) showed the results as in Fig. 25.

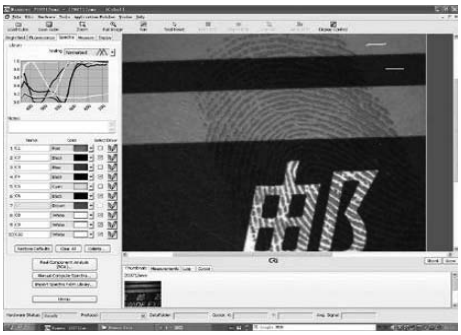


Figure 23

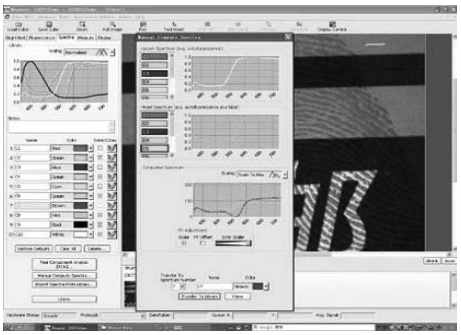


Figure 24

6 ZhuangHua, Huang Zhiming: Dichroism Polarization Photography by Digital Camera [J]. Criminal Technology, 2005 (2)

Figure 25

Figure 26

There may also be three values defined as the background dark tone values, such as black,[7] while the three spectral unfixing ones defined after a white, "unfixing" (Unix) operation[8] obtained the results shown in Fig. 26. If you want to mix the results after the operation, you can zoom in to view the display screen, shown in Figure 27. When the display is satisfied with them, save the corresponding results, as shown in Figure 28, to get mixed test results.

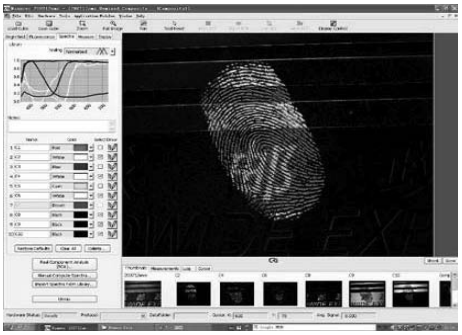


Figure 27

Figure 28

THE DIFFERENCE BETWEEN THREE DIGITAL IMAGE PROCESSING AND SPECTRAL IMAGING TESTS

For obtaining EMS envelopes with coloured handprints on samples, although the background patterns are complex, consistent hue of each colour, and therefore the use of digital image processing and spectral imaging tests, can show satisfactory test results, but certain difference still exist. They are as follows:

3.1 Processing techniques can be tested by using digital image. It does not require high shooting device or image acquisition tools. You can use a digital camera, for flat samples, as well as a scanner to scan input. For spectral imaging technology, the test requires specialized test equipment.

7 ShuhuiGAO. "Digital red ultraviolet photographic extract potential on a smooth object refers towlines of the comparison research" [J]. Journal of Xinjiang Police College.
8 Zhou Bali. Physical Evidence Verification Photography [M]. Beijing Policeman Education Press1999

3.2 Tests done by using digital image processing software can use popular software such as Photoshop image processing software. Specialized image processing software for processing can also be used, and spectral imaging techniques must be used exclusively for spectral analysis and processing.

3.3 The use of digital image technology acquisition is a single image that can be JPEG, BMP, TIFF and other image processing software that easily accept the file format, and the results of spectral imaging technology obtaining a set of spectral images contain multiple images.

REFERENCES

1. Ian Jun: Simple Tutorial of Criminal Photography [M]. People's Public Security University of China Press. 2002: 56-58
2. Su Weighing: Training Tutorial of Criminal Image and Video Technique [M]. People's Public Security University of China Press. 2010: 12-17
3. ShuhuiGAO. "Digital red ultraviolet photographic extract potential on a smooth object refers towlines of the comparison research" [J]. Journal of Xinxiang Police College, 2010: 77-78
4. Xiaoping Sun, Jingling. "All band material evidence examination CCD system applied in the field of criminal photography." Video technology. 2003:168-172
5. Zhou Bali. Physical Evidence Verification Photography [M]. Beijing Policeman Education Press1999
6. ZhuangHua, Huang Zhiming: Dichroism Polarization Photography by Digital Camera [J]. Criminal Technology, 2005 (2)
7. Zhang Shoji, Zhang Chunking. Trace Verification Volume of Chinese Criminal Science and Technique Collection [M]. People's Public Security University of China Press. 2004 (1): 29-31

UDC: 351.75:004.932]:004.08

THE RESEARCH OF SURVEILLANCE VIDEO STORAGE PLATFORM DEVELOPMENT STRATEGY

Fangzhou He, MA[1]
National Police University of China, Shenyang

Abstract: With the expanding of surveillance video investigation technology application, the construction scale of surveillance video becomes more and more complex. Consequently the surveillance video storage platform needs to be improved and such situation also causes the problem of massive data storage, which involves solving and realizing some new problems, such as unstructured data analysis, video retrieval and the extending application of video big data, which also requires a well-designed surveillance video platform. In order to provide a suitable solution for solving the storage problem of video big data, this paper discusses the current situation of video data storage, and provides a development strategy of surveillance video storage platform.

This paper explores the current surveillance video storage environment, and then provides suitable solutions and techniques for enhancing the current surveillance video storage platform. The rest of this paper is structured as follows: In section 1 we investigate the current situation of surveillance video storage. In section 2 we discuss the suitable platform development mechanism. In section 3 we analyse the implementation of platform function. In section 4, we propose the framework design of the platform. In section 5, summary and conclusion are presented.

Keywords: Massive data storage, Video big data, Surveillance video storage platform.

INTRODUCTION

A well-designed city surveillance video system can protect people, property, and help fighting the criminals, but one of the major barriers businesses encounter installing a comprehensive surveillance video solution has been the complexity and high cost associated with building the network, IT and storage infrastructures that follow the rapid expansion.

Concerns over security, crime, and terrorism boost the creation of massive surveillance video infrastructures—increasing the demand for video storage. Surveillance video storage solution should provide a complete line of external storage systems designed to meet today's challenges. The main targets focus on costs, capacity, speed, and durability. Reducing the costs of the hard disk drives, increasing the application of the surveillance systems and a higher return of investments due to scalability and flexibility play a major role in shaping the future of surveillance video storage solutions. Even though the government organizations and enterprises have implemented the storage solutions for surveillance data, due to regulations of longer storage of the data, these organizations and enterprises are switching to more scalable storage solutions. Many companies are providing cost effective solutions for surveillance storage which can store data for several years cost effectively and securely[2].

1 E-mail: ceo_xp@msn.com.
2 F Porikli, F Bremond, SL Dockstader. Video Surveillance: Past, Present, and Now the Future. IEEE Signal Processing Magazine, 2013, 30(3):190-198.

Based on the challenges of surveillance video storage, this paper tries to analyse the current situation of city surveillance video system, and then provides a set of suitable solutions in order to satisfy the future video storage requirements.

CURRENT SITUATION OF CRIMINAL CASE VIDEO STORAGE

Ever since the beginning of the era of big data, the current technical problem is how to classify and retrieve the massive video data of a public security body. Today, there is no unified national standard relating to criminal case video storage, so most of video investigation departments still rely on traditional artificial classification and single storage solution, which name criminal case video based on case property or timestamp, and store massive video data on personal computer or removable hard disk (see Figure 1).

Figure 1: *Current situation of criminal case video storage*

Such traditional way of video storage brings a lot of problems, such as storage inefficiency, high cost, low storage capacity, poor confidentiality, redundant data and inability of the system to support the distributed application. It cannot adapt to current development trend of video investigation technology thus becoming a barrier of video data statistics, management of related cases, and fast retrieval of criminal case video material[3]. This phenomenon also points that the current criminal case video management method cannot satisfy the needs of the video investigation work:

- The capacity of surveillance video is bigger than before, thus the video investigation department lacks a fast retrieval method of clues, through the artificial management solution of video data this department cannot compare clues and share resource effectively.

- Different kinds of video format and lack of unified video index management and play platform lead to inefficient video view, and limit the use efficiency of video data.

- Video data is difficult to be shared, due to adoption of a single machine store method, video data is difficult to be shared across regions, which lead to extend the case investigation period.

3 H Kim,S Lee, Y Kim. Weighted Joint-Based Human Behavior Recognition Algorithm using Only Depth Information for Low-Cost Intelligent Video-Surveillance System. Expert Systems with Applications, 2015.

- History video data accumulate over a long period, due to the lack of effective video compress storage and video data storage mechanism, this brings a huge pressure on arranging criminal case video data.

PLATFORM DEVELOPMENT MECHANISM

Based on the above discussions, currently we need to establish perfect video data storage platforms for solving the problem of video big data storage. Criminal case video storage platform should adopt the modular design presumption of video data and video investigation applications being relatively independent. The purpose of criminal case video storage platform is to facilitate the adjustment and upgrade platform at any time, adapt the changing of storage requirements, ensure the technology can be constantly updated, and maintain the advanced nature of platform[4]. Based on such purpose, the development of criminal case video storage platform should follow the mechanisms below:

- To establish the corresponding standard, mainly reflected in the unifying compulsive standard of video coding, opening Interface of application and compulsive standard of logic layer. Standards should also include regulations about criminal case video storage method and management.

- To emphasize the practicability of platform development. According to the needs of design and actual demands of public security organization, develop the forward-looking video data storage platform, satisfy the current and future needs of video investigation work.

- To emphasize platform management. To establish a criminal case video storage platform which is unified, hierarchical rights management, and flow control and scheduling flexibility.

- To enhance application. To establish unified, standard, open calling interfaces, which can be invoked by system applications. To develop plan video surveillance support system and police and video linked system for enhancing the application range of criminal case video storage platform.

Due to the lack of the same video monitoring platform development standard and complex video surveillance system, the development of criminal case video storage platform should deal with the following problems:

- The format of video surveillance. The source of criminal case video is complex, the criminal case video comes from the system of public security organization, also comes from the system of society, and different vendors adopt different video surveillance codec formats.

- Improving the capacity of video data sharing. The traditional way of dispersed video storage method limits the efficiency of seeking, managing and combining related cases.

- Enhancing the efficiency of video retrieval. Currently, the retrieval of criminal case video still relys on investigator's artificial video browsing and seeking suspected target, such working mode is time-consuming, strenuous and inefficient.

THE IMPLEMENTATION OF PLATFORM FUNCTION

In order to satisfy the development mechanism of criminal case video storage platform, solve the above problems effectively, and improve the efficiency of video case detection, the development of criminal case video storage platform must be able to effectively classify video

4 N Nitta, R Akai, N Babaguchi. People Counting Across Non-overlapping Camera Views by Flow Estimation Among Foreground Regions. Human Behavior Understanding in Networked Sensing, 2014.

data, quickly seek the video materials, and realize video intelligent retrieval for enhancing the efficiency of solving criminal cases. Thus, the criminal case video storage platform should realize the following functionalities:

- Management of criminal case video data. Centring on the video detection business model, which includes the management processes of case registration, case sharing, case query, collaborative working, related case analysis, investigation and research, close case, electronic portfolio, and so on (see Figure 2). End users can operate the criminal case video data directly based on relevant permissions for improving the security and management efficiency of the platform.

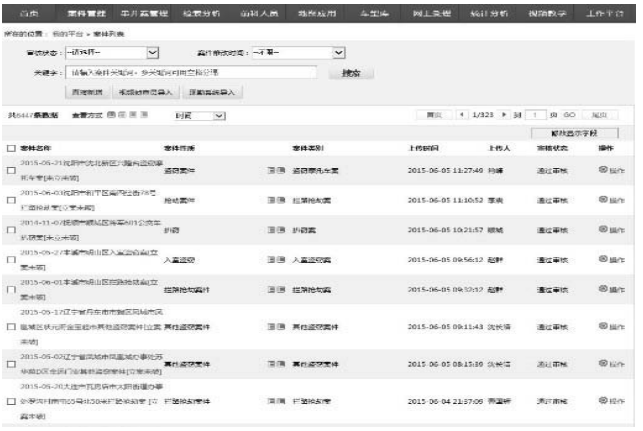


Figure 2: *Management of criminal case video data*

- Video data research and determination. Adopting intelligent analysis technology, video investigators can search relevant videos based on the suspect, suspicious vehicle, commit crime habits, and so on (see Figure 3). It provides key materials and technical information for analysing and researching criminal cases, and improving the efficiency of video query.

Figure 3: *Video data research and determination*

- PGIS time and space analysis. Labelling related case clues on the PGIS electronic map, and showing the trace of suspected target according to time sequence (see Figure 4). Such analysis way helps to trace suspected target through video, and lock suspected target quickly.

Figure 4: *PGIS time and space analysis*

FRAMEWORK DESIGN OF PLATFORM

In the design of criminal case video storage platform's framework, it has separation, hierarchy and load balancing techniques to ensure the platform operate stable, easy to develop and maintenance (see Figure 5). Separation technology separates media stream and control management, adopt customized development model, using independent control and data processing, and supporting very large scale application and flexible extension. Hierarchy technology divides platform into access layer, streaming media layer, management control layer, and business application layer, adopts standard communication protocol among different layers, the implementation technology of each layer can evolve independently[5]. So it is convenient to upgrade the system, extend, and import new features. Load balancing technology adopts the intelligent dynamic load balancing algorithm, adjust the load of platform dynamically

5 R Kasturi, R Ekambaram. Person Reidentification and Recognition in Video. Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications, 2014.

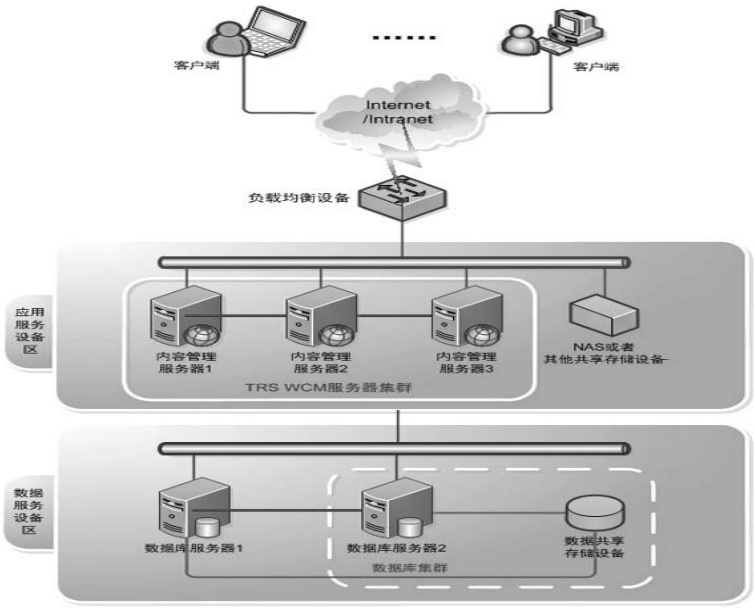


Figure 5: *Framework of criminal case video storage platform*

The database of criminal case video storage platform should be based on Internet, all levels of video investigation departments must adopt unified standard for developing database, store and manage of all kinds of video data centrally, realize searching, seeking and retrieving of criminal case video under the resource sharing mode. Focus on development of criminal case video database and application, realize rapid integration, indexing, related cases combination, and sharing of criminal case video data through establishing video summarization and labelling. At the same time, the relevant video management specification must be established for labelling, editing, arranging and uploading criminal case video in time. Criminal case video are stored in database for a long time, distributed and expandable cloud computing centre can satisfy the need of high efficiency and structured processing of massive video data.

High speed optical fiber network should be adopted for video data centralized storage area of criminal case video storage platform, which connects disk array and storage server[6]. FCP/SCSI protocol as the storage access protocol, the entire video data storage platforms should be networking, opening, virtualization and intelligence, and realizes the high speed, security, and shared storage mode of criminal case video data.

6 X Wang. Intelligent multi-camera video surveillance: A review. Pattern Recognition Letters, 2013, 34(1):3-19.

CONCLUSION

This paper tries to study the inadequacy of criminal case video storage, propose Criminal case video storage platform to relieve the pressure of storage problem of video big data in the investigating work. The study of Criminal case video storage platform meets the practical needs of current video investigation work and covers the shortages of criminal case video storage. It provides the whole technological solution to meet the age of full HD intelligent video surveillance system and video big data.

REFERENCES

1. F Porikli, F Bremond, SL Dockstader. Video Surveillance: Past, Present, and Now the Future. IEEE Signal Processing Magazine, 2013, 30(3):190-198.
2. H Kim, S Lee, Y Kim. Weighted Joint-Based Human Behavior Recognition Algorithm using Only Depth Information for Low-Cost Intelligent Video-Surveillance System. Expert Systems with Applications, 2015.
3. N Nitta, R Akai, N Babaguchi. People Counting Across Non-overlapping Camera Views by Flow Estimation Among Foreground Regions. Human Behavior Understanding in Networked Sensing, 2014.
4. R Kasturi, R Ekambaram. Person Reidentification and Recognition in Video. Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications, 2014.
5. X Wang. Intelligent multi-camera video surveillance: A review. Pattern Recognition Letters, 2013, 34(1):3-19.

UDC: 662.951.23:546.11

CONTRIBUTION TO THE PRODUCTION AND USE OF HYDROGEN IN ECOLOGICAL, SAFETY AND FORENSIC APPROACH

Svetlana Živković-Radeta[1]
"RALO BLUE SYSTEMS SRL", Bolzano
"R&Relectronic", Belgrade

Abstract: Global needs today are at a very high level both in environmental, safety and in industrially reasonable sense. Every day, the planet Earth is facing major problems of pollution of the atmosphere and the high production of CO_2 which is the cause of the greenhouse effect and global warming. The combustion of fossil fuel monitored emissions, which is the highest percentage of CO_2, CH_4, N_2O.[2],[3] Hydrogen has the best performance compared to any known fuel. The Safe Flame EU project addresses key safety issues in the huge global market of brazing. The Safe Flame technology has three unique features which bring major safety improvements to the sector, decreasing the risk of accidents and the cost of insuring operators, buildings and transportation vehicles. The Safe Flame approach eliminates the need for any stored gases, removing explosion hazards and improving process portability. On the other hand - Hydrogen as a GC/MS carrier and buffer gas for the use in forensic laboratories. Hydrogen has been shown to be an effective replacement for helium as a carrier and buffer gas in GC–MS.[4] From the water, hydrogen can be extracted by chemical reaction of aluminium, electrolysis or extraction of fossil fuels. Several types of hydrogen cells are designed, which are more or less efficient and have their own strengths and weaknesses. The biggest problem is the thermal response of meaning - the loss of invested energy. At the request of industry, cells for hydrogen production must be: energy-efficient, long-term operation without forced cooling, linear characteristic and easily manageable. The experimental result is one very important step in technological development - efficiency HHO cells is 156 W for 1 LPM. The point of such a security system at the level of global application is an invaluable addition to all the benefits, the prediction of environmental protection is widespread. What we have so far done is project safe flame - a prototype model that is in use.

Keywords: electrolysis, hydrogen, energy efficiency, safety, ecology, forensics.

---

1 Coordinator and Research Associate, szgranule@gmail.com
2 E. Specht, T. Redemann, N. Lorenz, Simplified mathematical model for calculating global warming through anthropogenic CO_2, *International Journal of Thermal Sciences, Volume 102, April 2016, Pages 1-8*
3 L. Remuzgo, C. Trueba, J. M. Sarabia, Evolution of the global inequality in greenhouse gases emissions using multidimensional generalized entropy measures *Physica A: Statistical Mechanics and its Applications, Volume 444, 15 February 2016, Pages 146-157*
4 C. N. Nnaji, et al, Hydrogen as a GC/MS carrier and buffer gas for use in forensic laboratories, *Science & Justice, Volume 55, Issue 3, May 2015, Pages 162-167*

INTRODUCTION

In all high temperature processes, manufacturing processes, there is a need to use some sort of fossil fuels.The oxidation is generally an exothermic reaction in which heat energy is released. Fuel type, most of the fossil origin, dictates the amount of energy released, the height of the temperature and the amount of harmful products of combustion. Popularity of fossil fuels is well known, also consequences of use fossil fuels are very well known. Ideal fuel that can be used is the simplest element of the Periodic system of elements - hydrogen.

Helium has quickly become expensive and limited commodities (period of use for another 30 years). Limitations on heliumusage may soon take effect, as it is used in several areas including magnetic resonance imaging (MRI), magnetocephalography (MEG), welding, and as a buffer gas for many chemistry and biology related analysis techniques. Currently, gas-quadrupole ion trap mass spectrometry (GC-MS) is used helium as a carrier gas for GC and buffer gas for ion traps MS. Gas chromatograph-mass spectrometer (GC-MS) is the primary workhorse for the analysis of narcotics and explosives in forensic laboratories.[4]

WHAT IS SAFE FLAME?

Project Safe Flame the EU deals with the crucial issue of security within the area of enormous global soldering. The processes of soldering, welding, cutting materials have a wide range of industrial applications: in various devices for cooling, air conditioning, shipbuilding, railway warehouses, car repair, jewelry, dental techniques and polishing. The Safe flame consortium represents about 1,000 small and large companies that have been used for these processes, employs 125,000 people in Europe and has an annual turn over of 20 billion euros. Soldering and many other flames processes using highly flammable gas, stored in high pressure cylinders, such as methylacetylene, propane, butane, methane, oxygen. Safe Flame technology has three unique features that bring great improvements in the security sector, reducing the risk of accidents and the cost of insurance operators, building and transport.[5]

Safety

Each year in the European Union there are hundreds of serious incidents caused by gas cylinders of acetylene, propane and oxygen. These gases are routinely used in over 100,000 individual applications for the use of fuel gas and oxygen flames burners for welding, cutting and soldering parts like. in refrigeration and air conditioning systems. Only in the UK, there were about 100 incidents a year in which the acetylene cylinders cause of the fire. For these bottles is known that the explosion repartitioning the many parts and act as shrapnel bombs. In addition to fire and dangerous explosions, shrapnel can penetrate the wall of the transport container (ISO standard). Because of these obvious safety reasons, the cost of insurance carriers and vehicles carrying gas cylinders can be extremely high. Safe Flame EU project aims to bring a great benefit to security and costs in this sector.[5]

Technology

Safeflame technology consists of three separate characteristics which together represent great progress in the industry. This is the first time that this a set of functions become available. Safe Flame device generates HHO gas using water and power supply. HHO gas is burned in the burner and offers advantages over acetylene and propane. Oxygen and hydrogen are generated separately, and mixtures thereof precisely controlled during the stoichiometric oxidation

5 The Safeflame EU Project [online], dostupno na: http://www.safeflameproject.eu (05.02.2015.)

and reduction flame - innovation provides a unique benefit in soldering applications. Length of flame and heat flux can be adjusted by adjusting the current input power to the HHO cell - which have been made more flexible customer solutions. Safe Flame approach eliminates the need for any storage of gas, removes the explosive hazards is portable and easy to process. Key features include high flame temperature, high value heat flux and uniform heat transfer with quiet operation. The system is supplied with a mains voltage of 230V, easy to use and operate. Do not use acetylene, oxygen gas cylinders are not and there is no danger of explosion. The flame is stoichiometric adjustable, therefore suitable for welding different materials such as copper, aluminum, steel and others in the automotive and aviation industry. Low costs of electricity for a typical soldering operation and low consumption of water. Short payback period compared with other applicative gases achieved the avoided costs of insurance and transportation of gas cylinders and purchase bottles with oxygen and short time when changing gas cylinders.[5]

USE OF HYDROGEN IN FORENSIC LABORATORY

Hydrogen as carrier gas increases the overall resolution and speed of analysis. Ions diameter of volume of 1, 2, 4, 6, 8 and 10 mm are used in the intensity comparison. Ion diameter of 10 mm showed the highest intensity for illicit drugs and explosives. Hydrogen gas may cause slight variations in the mass spectrum, usually as an M+1 peak.[4]

A custom set of ions is produced in order to improve research and products that use hydrogen as buffer gas following the electronic ionization quadrupole ion traps with the mass spectrometer compared to helium. Analysis of illegal drugs such as cocaine, codeine, and oxycodone, and explosives such as TNT, RDX, and HMTD, the ion diameter of the output choke of 1 mm, 2 mm, 4 mm, 6 mm, 8 mm and 10 mm was carried out by GC / MS. The great similarity between the hydrogen and helijumovog spectrum of narcotics and explosives provides evidence that hydrogen can be efficiently used as a buffer gas in the ion trap mass spectrometer.[4]

Presented comparisons illustrate the reduction in the need for helium as the carrier gas and the buffer. Hydrogen is a highly efficient carrier gas because it increases the speed of analysis - reduced retention time and increased resolution GC by about 150%. The viscosity of hydrogen is lower than that of helium, however, this results in faster chromatographic separation. Ion traps using buffer gas to cause collision damping and thus increase the mass resolution and sensitivity. Lower molecular weight buffer gas to prevent a significant momentum change, such as small displacement and velocity after the collision with the analyte ions, minimizes losses of captured ions. In this case, helium and hydrogen are ideal buffer gases, as well as in rapid response to the background gases.[4]

The balance between reactivity and sensitivity will influence the choice of ion volume. Changing from a 1 mm to a 2 mm diameter exit orifice ion volume would enable an immediate transition, and the use of a 10 mm exit orifice would provide optimal intensities when switching to hydrogen for illicit drug analysis and energetic materials in forensic laboratory settings. The more delicate samples require open ion volumes, whereas hardier samples can be optimized in order to achieve higher sensitivity. Hydrogen gas may cause some slight variations in the mass spectra, usually as increased ion–molecule reaction chemistry; the formation of N_2H^+ ion supports this claim. With the increasing cost and depletion of helium, hydrogen is a suitable replacement for GC–QITMS as both a carrier gas and a buffer gas. This will be particularly true with the advent of databases built around using hydrogen in these systems rather than helium, furthering the ability to use hydrogen in a forensic laboratory setting. [4]

ELECTROLYSIS - APPLICATION AND JUSTIFIABILITY

Hydrogen has the best performance in relation to any known fuel. The oxidation of hydrogen, as a product of burning, gives water. Oxidation of hydrogen is released the greatest amount of energy and temperature are in the range 1500 ° C - 4500 ° C. As the smallest element with one proton and one electron of hydrogen, it is the most aggressive element that is completely unstable. This segment generated the biggest problem in the exploitation of hydrogen fuel. Production of pure hydrogen, also followed by the problems of transport and use.[6]

Hydrogen can be separated in several ways. The water can be extracted by chemical reaction of aluminum by electrolysis or extraction of fossil fuels.[7,8] The cheapest way to obtain hydrogen is the electrolysis of water. Electrolysis of water has been known from the early 19th century. Of course, each of these operations has its drawbacks. Electrolysis of water is not a simple reaction. Gas production should be optimized, and scientists are still working to resolve these problems.

The problems are: efficiency, exothermic reaction, the electrode material, the use of electrolyte, the sustainability of the system, and hydrogen storage.[9], [10], [11]

Several types of hydrogen cells are designed, which are more or less efficient and have their own advantages and disadvantages. The biggest problem is the thermal response of meaning - the loss of input energy. Empirical method was attempted in all, with the oversight of the fact that was repeated in experiments. All attempts gas produced food based on the principle of overshoot of electrons between two electrodes in a coupled system with a lot of neutral elements. Such a system is not natural and inevitable loss occurs in the form of heat. Heat growth in the system is a problem that leads to a decline in the efficiency of the system and at the end of his uselessness.[12]

EXPERIMENTAL RESULTS AND DISCUSSION

The solution is obtained by inverse logic. The connection electrode is designed by different principle. The design of the cell for hydrogen production is made according to industry standards. At the request of the industry, the cell for hydrogen production must be: energy-efficient, long-term operation without forced cooling, linear characteristic and easily manageable.

---

6 S. Niaz, T. Manzoor, A. H. Pandith, Hydrogen storage: Materials, methods and perspectives *Renewable and Sustainable Energy Reviews, Volume 50, October 2015, Pages 457-469*

7 S. Nistor, et al, Technical and economic analysis of hydrogen refuelling. Appl Energy (2015), http://dx.doi.org/10.1016/j.apenergy.2015.10.094

8 G. Gahleitner, Hydrogen from renewable electricity: An international review of power-to-gas pilot plants for stationary applications *International Journal of Hydrogen Energy, Volume 38, Issue 5, 19 February 2013, Pages 2039-2061*

9 D. Aili, et al, Porous poly (perfluorosulfonic acid) membranes for alkaline water electrolysis *Journal of Membrane Science, Volume 493, 1 November 2015, Pages 589-598*

10 J-H. Kim, et al, Low-cost and energy- fficient asymmetric nickel electrode for alkaline water electrolysis *International Journal of Hydrogen Energy, Volume 40, Issue 34, 14 September 2015, Pages 10720-10725*

11 D. Ferrero, et al, Reversible operation of solid oxide cells under electrolysis and fuel cell modes: Experimental study and modelvalidation *Chemical Engineering Journal, Volume 274, 15 August 2015, Pages 143-155*

12 A. Göllei, P. Görbe, A. Magyar, Measurement based modeling and simulation of hydrogen generation cell in complex domestic renewable energysystems, *Journal of Cleaner Production, Volume 111, Part A, 16 January 2016, Pages 17-24*

Designed segment system cells, which during the experiment showed a very good performance as well as the design of solutions based on completely different principles than previous models, and in accordance with the electrodynamic theory.

Unlike other materials making up the electrodes, platinum is the best element and, of course, very expensive. Testing inexpensive, it was material that meets all relevant requirements. Corrosion resistance, good surface conductivity and durability are the most important characteristics of the materials that were used for making electrodes. For the production of electrode a type of industrial stainless steel 904 L is used, which meets the necessary requirements. Its price is economically justified, the costs are about twenty times smaller compared to platinum. Testing electrode corrosion and erosion lasted over a year.

Installation of modules and connections between the plates is a solution to many problems arising from this type of HHO cells. Static-dynamic conductivity, avoided „ the phenomenon of " heat cells. The efficiency of the cell is brought to a very high level of which is approximately 1:1. The reason for such a good relationship in the production of gas is on the border of exothermic and endothermic reactions during electrolysis.

Special electronic system for energy management for the needs of the cell is developed, which controls the work. Experimental measurement and testing was used with the memory effect of the electrolyte and its polarization, resulting in a 10% increase in the production of HHO gas on the resonant frequency constant current flowing through the cell.

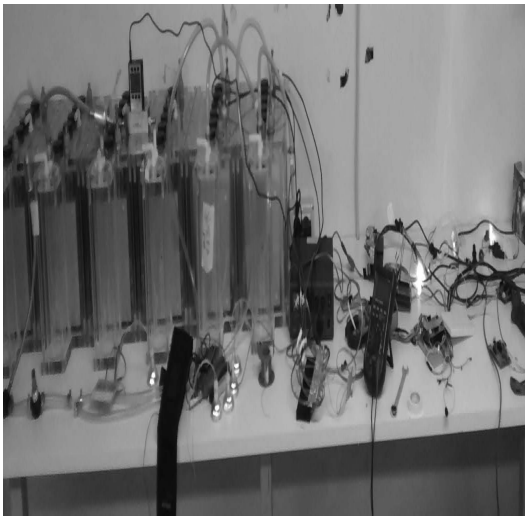


Figure 1: *Construction and programming HHO Cells*

Prototype HHO cells (Figure 1) has been tested under all conditions of long-term work. The measurement result HHO gas production compared to consumption of the energy is carried out in real time.

The efficiency of the cells may be declared in tests at 1: 1 and in some measurements, depending on the variant of the electronic management of 1: 1.2. After various physical modification of the structure of the cell with the harmonized spectrum molarity of electrolyte, the initial power of 225 W required to produce 1 LPM (liters per minute) HHO gas, electronically-time-frequency manipulation comes up to 175 W for 1 LPM. In other works, the results are

4.5-5 kWh /m^3 of hydrogen gas.[13] If the manipulate two cells at the same time, the effect of 156 W to 1 LPM (3.9 kWh / m^3) of hydrogen gas.

These results were achieved at low concentrations of electrolytes KOH, at a pressure of 1.3 bars, and were not experimented with higher concentrations and at high pressures. It is possible to get much better results with further optimization of experimental parameters.

The design of the electronic management cell was developed at the request of industry, depending on the purpose. We used a low-budget development version which is relatively easy to be applied to series production.

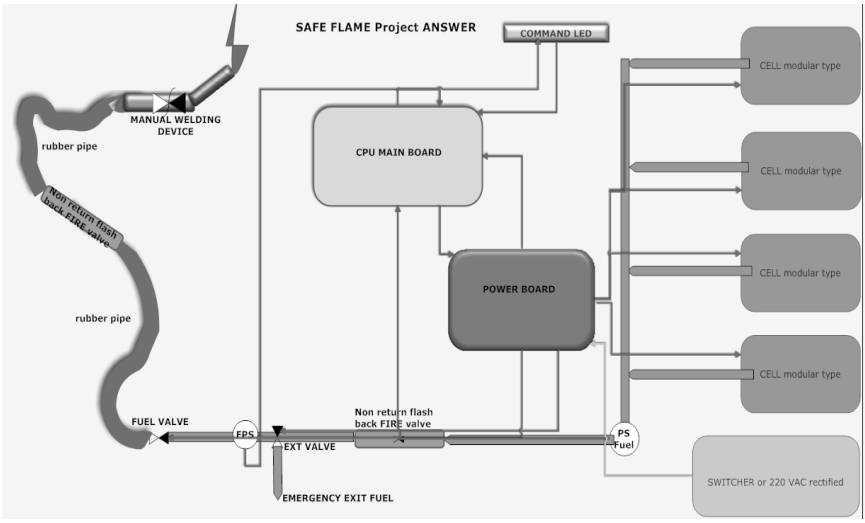


Figure 2: *Diagram design Safe Flame project for industrial applications*

Precisely designed linear output HHO gas.

Finally, the last detail, the system is designed for gas welding and cutting of the material, which is shown in Figure 2. Tests were carried out all of the system security procedures. The risk of ignition or explosion is reduced to a minimum. The system is designed so that it can be powered by solar energy, batteries or power line.

Operational attributes Safeflame prototype devices shown in Figures 2, 3, 4:

- This prototype is designed as a modular system that depends on the level of industrial requirement.
- Operation of the system is based on sensors and actuators.
- Complete HHO production process depends on two pressure sensors (type MXP6400A), which are placed in front of and behind the fire protection valves.
- For safety reasons, the main and secondary fire valves are installed.
- Through the potentiometer the pressure of 1.3 bars can be adjusted to 3 bar, wherein the said pressure limit values of the housing cell.
- Typology of HHO gas production is conditioned by the manufacturing process.
- When the pressure is below 1.3 bars processor retains the outlet valve closed and generates a sound signal as the announcement that the system is not yet ready.

13 A. Cruden, et al, Development of new materials for alkaline electrolysers and investigation of the potential electrolysis impact on theelectrical grid *Renewable Energy, Volume 49, January 2013, Pages 53-57*

- At the time of equalization of pressures between the two sensors, the system is ready for use.

- Starting the HHO gas production at the time when the processor detects a differential pressure difference (open manual valve burner).

- The PWM (pulse width modulation) calculation is built slow P regulator (gain by force - feedback).

- When manually shut the burner, the system now stops producing gas.

- The production of gas is directly managed by the PWM control on the pressure target.

- Output safety valve is open only in two cases: if the pressure exceeds the limit value or the user wants to shut down the entire system.

Figure 3: *Prototype Safe Flame*

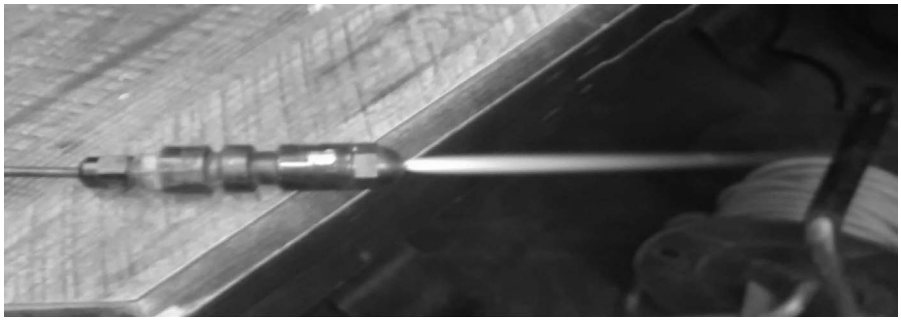


Figure 4: *The flame of the burner uses only 750W of electricity.*

CONCLUSION

The meaning of such a security system at the level of the global application is invaluable and addition to all the benefits, prediction of environmental protection is far-reaching.

Hydrogen has been shown to be an effective replacement for helium as a carrier and buffer gas in GC- MS. Hydrogen has already been studied and confirmed to be a superior carrier gas compared to helium in GC, and our experiments show that hydrogen is an equally ade-

quate buffer gas for mass spectrometry. With the use of hydrogen generators, both gases are safe for laboratory use; however, hydrogen is renewable, abundant, and significantly more inexpensive.[5]

It is necessary to develop a system based on the direct use of electricity from the grid without inverters, because they bring losses. Develop a model of modular type, where the cell structure is simple to manufacture and fulfills all the necessary conditions. Control electronics developed as a universal modular system that can be used in all applications.

In this field of science presented different results, so it is only a confirmation of previous results, this paper - empirical experimental methods. It is possible to get much better results further optimization of experimental parameters.

REFERENCES

1. Aili D., et al; Porous poly (perfluorosulfonic acid) membranes for alkaline water electrolysis, Journal of Membrane Science, Volume 493, 1 November 2015, Pages 589-598
2. Cruden A., et al; Development of new materials for alkaline electrolysers and investigation of the potential electrolysis impact on theelectrical grid, Renewable Energy, Volume 49, January 2013, Pages 53-57
3. Ferrero D., et al; Reversible operation of solid oxide cells under electrolysis and fuel cell modes: Experimental study and modelvalidation Chemical Engineering Journal, Volume 274, 15 August 2015, Pages 143-155
4. Gahleitner G.; Hydrogen from renewable electricity: An international review of power-to-gas pilot plants for stationary applications, International Journal of Hydrogen Energy, Volume 38, Issue 5, 19 February 2013, Pages 2039-2061
5. Göllei A.; Görbe P.; Magyar A.; Measurement based modeling and simulation of hydrogen generation cell in complex domestic renewable energy systems, Journal of Cleaner Production, Volume 111, Part A, 16 January 2016, Pages 17-24
6. Kim J-H., et al; Low-cost and energy efficient asymmetric nickel electrode for alkaline water electrolysis International Journal of Hydrogen Energy, Volume 40, Issue 34, 14 September 2015, Pages 10720-10725
7. Niaz S.; Manzoor T.; Pandith A. H.; Hydrogen storage: Materials, methods and perspectives Renewable and Sustainable Energy Reviews, Volume 50, October 2015, Pages 457-469
8. Nistor S., et al; Technical and economic analysis of hydrogen refuelling. Appl Energy (2015), http://dx.doi.org/10.1016/j.apenergy.2015.10.094
9. Nnaji C. N., et al, Hydrogen as a GC/MS carrier and buffer gas for use in forensic laboratories, Science & Justice, Volume 55, Issue 3, May 2015, Pages 162-167
10. Remuzgo L.; Trueba C.; Sarabia J. M.; Evolution of the global inequality in greenhouse gases emissions using multidimensional generalized entropy measures, Physica A: Statistical Mechanics and its Applications, Volume 444, 15 February 2016, Pages 146-157
11. Specht E.; Redemann T.; Lorenz N.; Simplified mathematical model for calculating global warming through anthropogenic CO2, International Journal of Thermal Sciences, Volume 102, April 2016, Pages 1-8
12. The Safeflame EU Project [online], dostupno na: http://www.safeflameproject.eu (05.02.2015.)

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

343.85(082)
007:004.056(082)
343.533::004(082)
343.9(082)

МЕЂУНАРОДНИ научни скуп "Dani Arčibalda Rajsa" (2016 ; Beograd)

Thematic Conference Proceedings of International Significance. Vol. 3 / International Scientific Conference "Archibald Reiss Days", Belgrade, 10-11 March 2016 ; [organized by] Academy of Criminalistic and Police Studies ; [editors Đorđe Đorđević ... et al.] = Tematski zbornik radova međunarodnog značaja. Tom 3 / Međunarodni naučni skup "Dani Arčibalda Rajsa", Beograd, 10-11. mart 2016. ; [organizator] Kriminalističko-policijska akademija ; [urednici Đorđe Đorđević ... et al.]. - Belgrade : Academy of Criminalistic and Police Studies = Beograd : Kriminalističko-policijska akademija, 2016 (Belgrade = Beograd : Pekograf). - XII, 643 str. : ilustr. ; 24 cm

Tiraž 200. - Preface: str. VIII. - Napomene i bibliografske reference uz tekst. - Bibliografija uz svaki rad.

ISBN 978-86-7020-358-7

ISBN 978-86-7020-190-3 (za izdavačku celinu)

1. Up. stv. nasl. 2. Kriminalističko-policijska akademija (Beograd)

a) Криминалитет - Сузбијање - Зборници b) Информациона технологија - Безбедност - Зборници c) Рачунарска технологија - Злоупотреба - Зборници d) Криминалистика - Зборници

COBISS.SR-ID 226082060