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, 7-9. novembar 2017.*
*Belgrade, 7-9 November 2017*

**TEMATSKI ZBORNIK RADOVA MEĐUNARODNOG ZNAČAJA**

**THEMATIC CONFERENCE PROCEEDINGS OF INTERNATIONAL SIGNIFICANCE**

**TOM III**
**VOLUME III**

Kriminalističko-policijska akademija
Beograd, 2017
Academy of Criminalistic and Police Studies
Belgrade, 2017

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

Editor-in-Chief
BILJANA SIMEUNOVIĆ-PATIĆ, PhD
Academy of Criminalistic and Police Studies

Editors
ALEKSANDAR BOŠKOVIĆ, PhD, Academy of Criminalistic and Police Studies
DAG KOLAREVIĆ, PhD, Academy of Criminalistic and Police Studies
NENAD RADOVIĆ, PhD, Academy of Criminalistic and Police Studies
SAŠA MILOJEVIĆ, PhD, Academy of Criminalistic and Police Studies
TANJA KESIĆ, PhD, Academy of Criminalistic and Police Studies
RADOMIR ZEKAVICA, PhD, Academy of Criminalistic and Police Studies

Thematic Proceedings Reviewers
JOVAN ĆIRIĆ, LLD, Constitutional Court Judge, Serbia
MILAN ŠKULIĆ, LLD, Constitutional Court Judge, Serbia
ĐURAĐ BUDIMIR, PhD, University of Westminster, London, United Kingdom
IMRE RUDAS, PhD, Obuda University, Budapest, Hungary
GORAZD MEŠKO, PhD, Faculty of Criminal Justice and Security, Ljubljana, University of Maribor, Slovenija

Computer Design
MILOŠ IVOVIĆ
JOVAN PAVLOVIĆ
DRAGOLJUB MILUTINOVIĆ

Impression
200 copies

Print
Univerzal, Čačak

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

© 2017 Academy of Criminalistic and Police Studies, Belgrade

ISBN 978-86-7020-387-7
ISBN 978-86-7020-190-3

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

Glavni i odgovorni urednik
Prof. dr BILJANA SIMEUNOVIĆ-PATIĆ
Kriminalističko-policijska akademija

Urednici
Prof. dr ALEKSANDAR BOŠKOVIĆ, Kriminalističko-policijska akademija
Prof. dr DAG KOLAREVIĆ, Kriminalističko-policijska akademija
Prof. dr NENAD RADOVIĆ, Kriminalističko-policijska akademija
Prof. dr SAŠA MILOJEVIĆ, Kriminalističko-policijska akademija
Prof. dr TANJA KESIĆ, Kriminalističko-policijska akademija
Prof. dr RADOMIR ZEKAVICA, Kriminalističko-policijska akademija

Recenzenti Zbornika radova
Prof. dr JOVAN ĆIRIĆ, sudija Ustavnog suda Republike Srbije
Prof. dr MILAN ŠKULIĆ, sudija Ustavnog suda Republike Srbije
Prof. dr ĐURAĐ BUDIMIR, Univerzitet u Vestminsteru, London, V. Britanija
Prof. dr IMRE RUDAŠ, Univerzitet Obuda, Budimpešta, Mađarska
Prof. dr GORAZD MEŠKO, Fakultet za bezbednosne studije, Ljubljana,
Univerzitet u Mariboru, Slovenija

Tehničko uređenje
MILOŠ IVOVIĆ
JOVAN PAVLOVIĆ
DRAGOLJUB MILUTINOVIĆ

Tiraž
200 primeraka

Štampa
Univerzal, Čačak

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

© 2017 Kriminalističko-policijska akademija, Beograd

ISBN 978-86-7020-387-7
ISBN 978-86-7020-190-3

HONORARY COMMITTEE

Goran Bošković, PhD, Academy of Criminalistic and Police Studies, President
Biljana Simeunović-Patić, PhD, Vice Dean of the Academy of Criminalistic and Police Studies
Dragana Kolarić, LLD, Constitutional Court Judge
Tijana Šurlan, LLD, Constitutional Court Judge
Jovan Ćirić, LLD, Constitutional Court Judge
Sima Avramović, LLD, Dean of the Faculty of Law University of Belgrade
Ivica Radović, PhD, Dean of the Faculty of Security, University of Belgrade
Major-General Goran Zeković, Head of the Military Academy, University of Defence, Belgrade
Branislav Đorđević, PhD, Director of the Institute of International Politics and Economics, Belgrade

International members

David D. Stephens, PhD, School of Criminal Justice, Michigan State University, USA
Olivier Ribaux, PhD, Director of the School of Criminal Justice, University of Laussane, Switzerland
Norbert Leitner, PhD, President of the Association of European Police Colleges (AEPC),
Director of SIAK, Vienna, Austria
José García Molina, PhD, Director of National Police Academy, Ávila, Spain
Hao Hongkui, PhD, President of the National Police University of China, Shenyang, China
Major-General Vladimir Tretyakov, PhD, Chief of the Volgograd Academy of the MoI of Russia
Major-General Valeriy Vyacheslavovich Sereda, PhD,
Rector of the Lviv State University of Internal Affairs, Ukraine
Major-general Vladimir Bachila, PhD, Head of the Academy of MoI of the Republic of Belarus
Piotr Bogdalski, PhD, Rector of Police Academy, Szczytno, Poland
Lucia Kurilovská, PhD, Rector of the Academy of the Police Force, Bratislava, Slovakia
Jozef Meteňko, PhD, Academy of Police Force, Bratislava, Slovakia
Daniel-Costel Torje, PhD, Rector of the Police Academy "Alexandru Ioan Cuza", Bucharest, Romania
Simion Carp, PhD, Rector of the Academy "Stefan cel Mare", MoI of the Republic of Moldova
Zoltán Rajnai, PhD, Bánki Donát, Óbuda University, Hungary
Andrej Sotlar, PhD, Dean of the Faculty of Criminal Justice and Security, Ljubljana, Slovenia
Ivan Toth, PhD, Dean of the University of Applied Sciences Velika Gorica, Croatia
Nikola Dujovski, PhD, Dean of Faculty of Security, Skopje, Macedonia
Predrag Ćeranić, PhD, Dean of the Faculty of Security Science, University of Banja Luka, BiH
Nedžad Korajlić, PhD, Dean of the Faculty for Criminal Justice, Criminology and Security Studies,
University of Sarajevo, BiH
Velimir Rakočević, PhD, Dean of the Faculty of Law, Podgorica, Montenegro
Rajko Peković, Dean of the Police Academy, Montenegro

PROGRAMME COMMITTEE

Prof. dr Đorđe Đorđević, KPA, predsednik
Prof. dr Milan Žarković, KPA
Prof. dr Dag Kolarević, KPA
Prof. dr Dane Subošić, KPA
Prof. dr Obrad Stevanović, KPA
Prof. dr Saša Milojević, KPA
Prof. dr Saša Mijalković, KPA
Prof. dr Boban Milojković, KPA
Prof. dr Aleksandra Ljuština, KPA
Prof. dr Radomir Zekavica, KPA
Prof. dr Aleksandar Bošković, KPA
Prof. dr Tanja Kesić, KPA
Prof. dr Zoran Đurđević, KPA
Prof. dr Nenad Radović, KPA
Doc. dr Dragoslava Mićović, KPA
Prof. dr Dragan Randelović. KPA
Prof. dr Nikola Milašinović, KPA
Prof. dr Smilja Teodorović, KPA
Prof. dr Stevo Jaćimovski, KPA
Prof. dr Miroljub Blagojević, KPA
Prof. dr Nenad Koropanovski, KPA

POČASNI ODBOR

Prof. dr Goran Bošković, Kriminalističko-policijska akademija, predsednik
Prof. dr Biljana Simeunović-Patić, Kriminalističko-policijska akademija
Prof. dr Dragana Kolarić, sudija Ustavnog suda Republike Srbije
Prof. dr Tijana Šurlan, sudija Ustavnog suda Republike Srbije
Prof. dr Jovan Ćirić, sudija Ustavnog suda Republike Srbije
Prof. dr Sima Avramović, dekan Pravnog fakulteta Univerziteta u Beogradu
Prof. dr Ivica Radović, dekan Fakulteta bezbednosti Univerziteta u Beogradu
General-major Goran Zeković, načelnik Vojne akademije Univerziteta odbrane, Beograd
Prof. dr Branislav Đorđević, direktor Instituta za međunarodnu politiku i privredu, Beograd

Članovi iz inostranstva

Prof. dr David D. Stephens, Škola za kriminalistiku, Državni univerzitet u Mičigenu, SAD
Prof. dr Olivier Ribaux, direktor Fakulteta za kriminalistiku, Univerzitet u Lozani, Švajcarska
Dr Norbert Leitner, predsednik Asocijacije evropskih policijskih koledža (AEPC),
direktor Policijske akademije u Beču (SIAK), Austrija
Dr José García Molina, direktor Nacionalne policijske akademije, Avila, Španija
Prof. dr Hao Hongkui, predsednik Nacionalnog policijskog univerziteta Kine, Šenjang, Kina
General-major prof. dr Vladimir Tretjakov, načelnik Volgogradske akademije MUP Rusije
General-major doc. dr Valerij Vjačeslavovič Sereda,
rektor Državnog univerziteta unutrašnjih poslova, Lavov, Ukrajina
General-major prof. dr Vladimir Bačila, načelnik Akademije MUP Belorusije
Prof. dr Piotr Bogdalski, rektor Policijske akademije, Ščitno, Poljska
Doc. dr Lucia Kurilovska, rektor Policijske akademije, Bratislava, Slovačka
Prof. dr Jozef Metenko, Policijska akademija, Bratislava, Slovačka
Prof. dr Daniel-Costel Torje, rektor Policijske akademije „Alexandru Ioan Cuza“, Bukurešt, Rumunija
Prof. dr Simion Carp, rektor Akademije “Stefan cel Mare”, Moldavija
Prof. dr Zoltan Rajnai, Banki Donat, Univerzitet Obuda, Mađarska
Prof. dr Andrej Sotlar, dekan Fakulteta bezbednosti, Ljubljana, Slovenija
Prof. dr Ivan Toth, dekan Univerziteta Velika Gorica, Hrvatska
Prof. dr Nikola Dujovski, dekan Fakulteta bezbednosti, Skoplje, Makedonija
Doc. dr Predrag Ćeranić, dekan Fakulteta bezbjednosnih nauka, Univerzitet u Banjoj Luci, BiH
Prof. dr Nedžad Korajlić, dekan Fakulteta za kriminalistiku, kriminologiju
i sigurnosne studije, Univerzitet u Sarajevu, BiH
Prof. dr Velimir Rakočević, dekan Pravnog fakulteta, Podgorica, CG
Rajko Peković, direktor Policijske akademije, Danilovgrad, CG

PROGRAMSKI ODBOR

Đorđe Đorđević, PhD, ACPS, President
Milan Žarković, PhD, ACPS
Dag Kolarević, PhD, ACPS
Dane Subošić, PhD, ACPS
Obrad Stevanović, PhD, ACPS
Saša Milojević, PhD, ACPS
Saša Mijalković, PhD, ACPS
Boban Milojković, PhD, ACPS
Aleksandra Ljuština, PhD, ACPS
Radomir Zekavica, PhD, ACPS
Aleksandar Bošković, PhD, ACPS
Tanja Kesić, PhD, ACPS
Zoran Đurđević, PhD, ACPS
Nenad Radović, PhD, ACPS
Dragoslava Mićović, PhD, ACPS
Dragan Ranđelović, PhD, ACPS
Nikola Milašinović, PhD, ACPS
Smilja Teodorović, PhD, ACPS
Stevo Jaćimovski, PhD, ACPS
Miroljub Blagojević, PhD, ACPS
Nenad Koropanovski, PhD, ACPS

# 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 cooperation with the Ministry of Interior and the Ministry of Education, Science and Technological Development of the Republic of Serbia, School of Criminal Justice, Michigan State University in USA, School of Criminal Justice University of Laussane in Switzerland, National Police Academy in Spain, Police Academy Szczytno in Poland, 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, Faculty of Security Science University of Banja Luka, Faculty for Criminal Justice, Criminology and Security Studies University of Sarajevo, Faculty of Law in Montenegro, Police Academy in Montenegro and held at the Academy of Criminalistic and Police Studies, on 7, 8 and 9 November 2017.

The International Scientific Conference "Archibald Reiss Days" is organized for the seventh time in a row, in memory of the founder and director of the first modern higher police school in Serbia, Rodolphe Archibald Reiss, after whom the Conference was named. The Thematic Collection of Papers contains 131 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, Bangladesh, Abu Dhabi, Greece, Hungary, Macedonia, Romania, Russian Federation, Serbia, Slovakia, Slovenia, Czech Republic, Switzerland, Turkey, Ukraine, Italy, Australia 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 provide us with the analysis of the criminalistic and criminal justice aspects in solving and proving of criminal offences, police organization, contemporary security studies, social, economic and political flows of crime, forensic linguistics, cybercrime, and forensic engineering. 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, October 2017 *Programme and Organizing Committees*

# 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 IX

### Effects of Physical Activity on Anthropological Status in Security Agency Personnel

Topic V

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

# INTELLIGENCE-LED POLICING IN THE MINISTRY OF INTERIOR OF THE REPUBLIC OF SERBIA

**Zoran Djurdjevic, PhD**
The Academy of Criminalistic and Police Studies [1]
**Branko Lestanin**
MoI of the Republic of Serbia, Police Department Kraljevo

**Abstract**: The traditional reactive model of policing has proven to be insufficiently effective in countering crime and protecting fundamental rights and freedoms of citizens. The request of society that police must respond more efficiently and rationally, contributed to the strengthening of intelligence and analytical functions in policing, specifically Intelligence-Led Policing (ILP). Given that this is a new model of policing that is only being introduced into the practice of the Serbian police, there is no large number of papers in the scientific and professional literature in the Republic of Serbia. In addition to the introduction and conclusion, the paper consists of three interrelated logical units. Initially, the subject of the analysis was the normative legal framework for the establishment of ILP in the Serbian Law on Police. Below are the basic concepts and philosophy of policing guided by intelligence and the way in which basic criminal-intelligence products are used in organizing and directing policing on key security issues, which constitutes the essence of the ILP. In the end, concrete conclusions are proposed for the establishment of the ILP. Recognizing the ILP as a successful model of police work since 2005, the introduction of this model has begun with the Swedish police. The Minister of the Interior established a working group tasked with establishing ILP in the Serbian police and developing a manual on ILP.

**Keywords**: law, police, analysis, analytical product, criminal intelligence cycle.

## INTRODUCTION

The strategic goal of the Ministry of Interior is to build a modern, efficient, functional and highly professional police force. The precondition for transformation into a modern, efficient, effective, democratic and responsible police is to build professional capacities that will continuously work on upgrading work, performing basic tasks, protecting basic rights and freedoms of citizens and supporting the rule of law, following up contemporary trends in the development of science and profession. Today's law enforcement agencies face a number of security challenges. The increase in the crime rate, especially organized, caused the public pressure on the police to take something new, differently, more efficiently and economically more rationally, in addition to the then applied traditional policing model, which in the short term would reduce the number of criminal offenses.[2] In particular, police officers face increasing demands from society and professional challenges to achieve a higher level of efficiency with the limitation of resources. In addition, the situation is compounded by rapid social, in particular economic change and the misuse of information technology by the perpetrators. The rapid development of technologies, globalization and the exponential growth of the glob-

1 Zoran Djurdjevic, PhD, E-mail: zoran.djurdjevic@kpa.edu.rs.
2 Ratcliffe, J. H. (2007). *Integrated intelligence and crime analysis: enhanced information management for law enforcement leaders*. Washington: Police Foundation, p. 2.

al market have created greater opportunities for criminal activities, which are at the same time more difficult to detect. The perpetrators, criminal groups efficiently use fragmented organizations of the area and sophisticated technology for committing criminal offenses and gaining high profits.[3] The consequences of criminal offenses are growing ever more unacceptable to society, so that a more dominant, reactive approach is increasingly changing into proactive. The goal is to influence the dominant criminality factors and prevent committing of criminal offenses.[4]

It is generally accepted that the policing has changed dramatically over the last twenty years. **Crime is an increasingly global problem**. Current forms of policing and cooperation, including international ones, are no longer sufficient; new operational models of cooperation are more and more discussed, which include the formation of transnational operational units.[5] The European Commission is based on its anti-crime activities, the security of the EU and global security are interconnected and conditioned categories. The European Security Agenda 2015–2020 has defined measures to improve information sharing and operational co-operation, as well as to provide support to member states in funding, training and crime research.[6]

In the process of accession to the EU, the Republic of Serbia committed itself to reform and reorganize state administration, including the Ministry of Interior and the police. The fight against organized crime and corruption is the most important point in pre-accession negotiations with the EU. Chapters 23 (Judiciary and Fundamental Rights) and 24 (Justice, Freedom and Security) require the introduction of certain new ways of policing. By adopting the Law on Police [7] in 2006 a new model is being introduced to the police, community policing (article 6, 17 and 18. of the Law on Police). However, practice has shown that not only in Serbia but also in other countries, the community policing is not sufficient to prevent and reduce crime in accordance with the requirements of the society. Therefore, an increasing number of police have started to introduce ILP into their practice. In the new Law on Police ILP is recognized as one of the policing models that can, together with other models, influence the reduction of crime and establish better protection of the rights and freedoms of citizens. In 2005, the Ministry of the Interior and the Swedish National Police Board established cooperation in the area of ILP[8].

Scientific and professional public do not have the same opinion as to which model of policing is best, which of the most famous policing models most effectively influences the reduction of crime and bringing the crime rate to an acceptable level for citizens and the community (traditional reactive model, community policing[9], ILP, problem orienting policing[10],

3 United Nations, 13th United Nations Congress on Crime Prevention and Criminal Justice, *New and Emerging Forms of Crime: Threats the World must Reckon with*, Doha, 12–19 April 2015. www.un.org/en/events/crimecongress2015/, accessed on: 23/08/2015.
4 Djurdjevic, Z., Radovic, N. (2015a). *The EU's strategic directions for countering crime and their significance for the Republic of Serbia*. Serbian Political Thought, 22(4):276.
5 *Ibid.*
6 *Ibid.*
7 "Official Gazette of Republic of Serbia", No. 101/2005, 63/2009 – decision of CC, 92/2011 & 64/2015.
8 Since the beginning of 2016, a new project has been launched with the Swedish police called "Implementation of the Intelligence-Led Policing in the Ministry of the Interior in 2016–2018". See more in: Lestanin, B, Nikac, Z, (2016). *Comment of the Law on Police*, Poslovni biro, Belgrade, p. 83.
9 More info in: Vojinovic, M., (2004). *Community policing*, Bezbednost (46)3:432–452; Nikac, Z. (2009), *Community policing,* The Academy of Criminalistic and Police Studies (ACPS), Belgrade.
10 More info in: Goldstein, H. (1979). *Improving policing: A problem-oriented approach*, Crime & Delinquency (2)25:236–258; Goldstein, H. (1990). *Excellence in problem-oriented policing*, McGraw-Hill, New York; Spelman, W., Eck, J.E. (1987). *Problem-oriented policing*, US Department of Justice, National Institute of Justice.

SARA[11], criminal mapping[12], Compstat[13], Broken windows theory,[14] etc.). However, we must point out that the above models do not exclude each other, but represent a different approach, different ways to address security issues.

## NORMATIVE FRAMEWORK FOR THE ESTABLISHMENT OF ILP

Following the positive legislation of the Republic of Serbia (RS), the basic and main legal act that is important for the establishment of the ILP is the Serbian Constitution[15]. In the first place is Art. 18 of the Constitution which provides for the immediate application of human and minority rights guaranteed by the Constitution, generally accepted rules of international law, ratified international treaties and laws. The law may prescribe the manner of exercising these rights only if it is expressly provided for in the Constitution or if it is necessary for the realization of a particular right due to its nature, in which case the law must in no way affect the substance of the protected right. Art. 27 guarantees every citizen the right to personal freedom and security. Art. 41 prescribes that the confidentiality of letters and other means of communication is inviolable. Derogations are permitted only for a limited period of time and based on a court decision, if necessary for the purpose of conducting criminal proceedings or for the protection of the security of the RS, in the manner prescribed by law (Criminal Procedure Code–CPC, etc.). Art. 42 guarantees personal data protection. The collection, keeping, processing and use of personal data is governed by law. It is forbidden and punishable to use personal data outside the purpose for which they were collected, in accordance with the law, except for the purposes of conducting criminal proceedings or the protection of the security of the RS, in the manner prescribed by law.

The Law on Police[16] (LP) is a systemic legal act that, in a comprehensive and precise manner regulates, among other things, police and police affairs (policing). The Police Directorate is the only organizational unit, that is, a body within the Ministry of the Interior, which is primarily responsible for the conduct of police affairs as well as for certain internal affairs. Police and internal affairs are carried out on the territory of the RS through organizational units in the headquarters, police departments and police stations. Novelty in the LP and in Art. 24 are tasks related to strategic documents, regarding the development of the Strategic Assessment of Public Security and the Strategic Plan of the Police. These two documents are part of a broader concept and governance model in the Intelligence-Led Police (ILP). When we

11 Scanning, Analyzing, Responding, and Assessing. More info in: http://www.cops.usdoj.gov/pdf/vets-to-cops/e030917193-CP-Defined.pdf, accessed on 20/03/2015, http://www.cops.usdoj.gov/pdf/e06011157.pdf, accessed on 20/03/2015.

12 More info in: Djurdjevic, Z., Radovic, N. (2015b). *Kriminalisticka operativa*, ACPS, Belgrade. pp. 328–338; Markovic, J., Christopher, S., (2002). *Criminal mapping and policing in democratic societies*, Bezbednost (44)4:641–652; Butorac, K., (2011). *Geography Of Crime – Criminological And Criminalistics discourses*. Police and Security (20)3:363–379; Cacan, A., (2010). *Geographic profiling as a criminal investigative methodology in criminal investigation of serial crimes*. Criminal Justice Issues (10)3–4:155–173; Laverty, I., MacLaren, P. (2002). *Geographic profiling: A new tool for crime analysts*. Crime mapping news, (3)4:5–8.

13 More info in: http://www.compstat.umd.edu/what_is_cs.php, accessed on 20/03/2015; Henry, V. E. (2006). *Managing crime and quality of life using CompStat: Specific issues in implementation and practice,* Resource material series, No. 68, 129th International Senior Seminar Visiting Experts' Papers, 117–132.

14 More info in: Wilson J.Q., Kelling G.L. (1982). *Broken windows: The police and neighborhood safety,* The Atlantic Monthly (3)249:29–38, http://www.manhattan-institute.org/pdf/_atlantic_monthly-broken_windows.pdf, accessed on 20/06/2016; Harcourt B.E., Ludwig J., (2006). *Broken Windows: New Evidence from New York City and a Five-City Social Experiment*, The University of Chicago Law Review (73)93:2–47.

15 "Official Gazette of Republic of Serbia", No. 98/2006.

16 "Official Gazette of Republic of Serbia", No. 6/2016.

talk about the affairs of the Police Department (PD), the novelty in the LP are the operations related to operational documents, that is, the development of the Operational Assessment of Public Security and the Operational Plan of the PD which must be in accordance with the strategic documents issued by the Police Directorate[17].

Art. 34 of the LP in paragraph 1 provides a provision of a practical character obliging the police to apply ILP in its work and in carrying out police tasks which enables adequate data exchange and cooperation between state authorities in the field of suppression and combating organized crime and corruption both at national and international level, which is one of the many conditions in the pre-accession negotiations with the EU (Chapter 24). While it is very difficult to give a comprehensive definition of the ILP, which will be discussed later, the provision of paragraph 2 provides that the ILP is a way of managing police affairs based on criminal intelligence. According to paragraph 2, which mentions the formulation of "criminal intelligence", paragraph 3 defined it as a set of collected, assessed, processed and analyzed data, which is the basis for making decisions on performing police tasks. The simplest way to explain this term is the formula: "fresh" or "raw" information + processing/analysis = criminal intelligence. All what police officers gather on the ground during operational work, open source information, data from other state authorities and all of those related to public security are raw data that will be processed and analyzed in one place[18].

The process of passing laws that are important for the establishment of the ILP has not yet been completed. Namely, Art. 252 of the PL prescribes that the police may, for the purpose of performing tasks within the scope of the MoI, process personal data and keep records that will be prescribed by a special law. This special law was at a public hearing, but the law has not yet been adopted, and by that time Art. 75–82 of the old LP (provisions on the collection, processing and use of personal data and records) are still valid.

In addition to the enumerated laws, in the context of the ILP, the following should be mentioned: the provisions of the Law on the Basis of Regulation of Security Services of the Republic of Serbia[19], The Law on Organization and Jurisdiction of State Authorities in the Suppression of Organized Crime and Corruption and Other Particularly Serious Crimes[20], The Law on Personal Data Protection[21], The Law on Secrecy of Data[22], The Law on Free Access to Information of Public Importance[23], CPC[24], etc. Here, international legal acts ratified by our state must be mentioned, which constitute an integral part of our country's positional legislation, such as the European Convention for the Protection of Human Rights on Fundamental Freedoms[25] but also those unrecorded as part of the standards for police treatment such as: European Code of Police Ethics – Recommendations (2001) 10, Resolution No. 690 of Parliamentary Assembly of the Council of Europe – Declaration on the Police (1979), Convention on Police Cooperation in SE Europe (2006), European Security Strategy (2003), and others.[26]

Last but not least, all accompanying by-laws for the execution of the enumerated laws (regulations, rule books) as well as internal acts of the MoI (manuals and mandatory instructions) are essential for the establishment of the ILP. The analysis of the provisions of normative and in-

17 Lestanin, B, Nikac, Z, *Op. cit.* pp. 56–58.
18 *Ibid.*
19 "Official Gazette of Republic of Serbia", No. 116/2007 & 72/2012.
20 "Official Gazette of Republic of Serbia", No. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 – other law, 45/2005, 61/2005, 72/2009, 72/2011 – other law, 101/2011 – other law & 32/2013.
21 "Official Gazette of Republic of Serbia", No. 97/2008, 104/2009 – other law, 68/2012 – decision of CC & 107/2012.
22 "Official Gazette of Republic of Serbia", No. 104/2009.
23 "Official Gazette of Republic of Serbia", No. 120/2004, 54/2007, 104/2009 & 36/2010.
24 "Official Gazette of Republic of Serbia", No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 & 55/2014.
25 "Official Journal of Serbia and Montenegro – International agreements", No. 9/2003 & 5/2005.
26 Lestanin, B, Nikac, Z, *Op. cit.* p. 83.

ternal acts under the jurisdiction of the MoI considers that it is necessary to amend certain legal and internal acts. The Rulebook on policing should include more detailed provisions on the unified conduct of police affairs (who is responsible, how to coordinate, control, decision-making, etc.), the formation and functioning of the Strategic Management Group and the Operational Management Group (OMG), provisions on analytical products, regarding strategic and operational assessment (content, deadlines, who is developing, how, etc.), strategic and operational plan (content, deadlines, who makes it, in what way etc.), the profile of the target or the profile of an interesting person, deadlines, who makes it, how, etc.) and profile of the problem (content, deadlines, who makes it, how, etc.)[27]. The by-laws (or internal) regulation that provides more precisely the procedure and manner of daily deployment of police officers must certainly contain provisions that support not only the ILP, but also the model of community policing, problem oriented policing, etc. It is important to stress here that the daily scheduling must be done on the basis of the OMG's decision and based on the current (daily) assessment. Specific tasks issued in written orders for the execution of an official task also need to be in line with the OMG's decision and the current (daily) assessment. We need to look at the internal acts regulating information and reporting, sectoral policing, manner of work of the organizational units of MoI on crime prevention, on operational work of the police, on collection and other processes related to data on crime suppression through the use of IT.

## CONCEPT AND PHILOSOPHY OF ILP

There is no universally accepted definition for ILP. However, the basic idea is clear – the direction of policing, from a tactical to a strategic level, including government policies, must be based on criminal intelligence products.

The model originated in the early 1990s in Great Britain, after which, with some modifications, it was taken over by other countries, among which the first were EU and US.

An initial and essential element is the improvement of intelligence and the provision of intelligence-analytical information to the police, based on which security problems can be identified and appropriate decisions directed towards prevention, strategic and operational behavior of the police, its organization and allocation of resources made. ILP is the only policing methodology that uses intelligence as a primary means.[28] It is a managerial philosophy, a business model or theory that is based on objective identification of problems and directing the policing to problems, first of all, from the aspect of the possibility of preventing their occurrence. ILP is focused on strategic management, effective implementation of the strategy directed at serious offenders.[29] This specifically means changing *the philosophy from the criminal act towards the perpetrator into the philosophy of a registered, potential perpetrator in order to prevent the commission of a criminal offense*.

27 More info in: Djurdjevic, Z., Radovic, N., (2015b) *Op. cit.* pp. 404–412; Manojlovic, D., Jovic, V., (2004). *National crime intelligence service,* Bezbednost (46)3:419–430; Cavkov, M., *et al,* (2014). *Criminal intelligence manual*, DCAF Institute, Ljubljana, pp. 81–84.

28 Bell P., Congram M., (2013). *Intelligence-Led Policing as A Strategic Planning Resource in the Fight against Transnational Organized Crime*, International Journal of Business and Commerce (2)12:5,9 http://eprints.qut.edu.au/63093/1/IJBC-13-ILP_Strategy21202.pdf, accessed on 26/01/2015.

29 Ratcliffe J.H., (2008). *Pocket guide to intelligence led policing*, Willan Publishing: Cullompton, Devon, http://www.smartpolicinginitiative.com/sites/all/files/resources/ILPpocketguide.pdf, accessed on 26/01/2015.

ILP is based on the use of intelligence analysis for decision making aimed at preventing and reducing criminal rate using an effective policing strategy and external partner projects derived from a single database.[30]

ILP is a concept that supports all aspects of policing, from the neighborhood policing and joint-partnership work to investigation of serious and organized crime and terrorism[31]. Within the framework of the National Intelligence Model[32] (NIM) in the United Kingdom effective and efficient collection, recording, dissemination and retention of information allows the identification of material that can be assessed in terms of intelligence and allows decision-making in accordance with priorities and tactical options.[33] ILP is a collaborative-based philosophy based on the improvement of intelligence operations in order to help understand the changes in the operating environment in order to enable law enforcement agencies to quickly adapt to new circumstances. This philosophy supports decision-makers that require intelligence to improve their "judgment" and enable them to make better decisions regarding crime control strategy, resource allocation, and tactical operations.[34]

ILP is a business process for the systematic collection, organization, analysis and use of intelligence that serves as a guide for strategic, operational and tactical decisions in law enforcement agencies. The ability to collect, examine, critically review and compare the vast amount of information enables law enforcement agencies to better understand the patterns of crime and identify individuals, groups and locations where crimes and offenses are most often committed. For police officers on the ground, ILP demands that they become better at gathering information on the ground and better in using processed intelligence-products.[35] The implementation of the ILP requires the shift from the police "who gather evidence after the events" to the policing which implies the constant collection of relevant data and the provision of their input into the appropriate databases, as well as the use of data obtained from intelligence analysts and from relevant databases in implementation of on-going operations.[36] Despite its various meanings, ILP provides managers and executives in law enforcement agencies with valuable intelligence products that are used for decision making, strategic management and more efficient resource allocation. The lack of information results in an inefficient allocation of resources and a lesser ability of agencies to detect and prevent the commission of criminal acts.[37]

30 Ratcliffe J.H., (2003). *Intelligence-led policing*, Australian Institute of Criminology, p. 3. www.aic.gov.au/media_library/publications/tandi/ti248.pdf, accessed on 26/01/2015.
31 More info in: Clarke P., (2016). *Intelligence-led Policing in Counter-Terrorism: A Perspective from the United Kingdom*, in ed. Wither, J.K, Mullins S., Combating Transnational Terrorism, Procon, Sofia, pp. 149–162.
32 James A., (2011). *The Influence of Intelligence-Led Policing Models on Investigative Policy and Practice in Mainstream Policing 1993-2007,* Department of Social Policy of the London School of Economics and Political Science, London, http://etheses.lse.ac.uk/221/, accessed on 30/01/2015.; More info in: Djurdjevic, Z., Radovic, N., *Op. cit.* (2015b) pp. 357–379;
33 ACPO, Centrex, (2007). *Practice Advice: Introduction to Intelligence-Led Policing*, p. 3. http://www.acpo.police.uk/documents/crime/2007/200708-cba-intelligence-led-policing.pdf, accessed on 30/01/2015.
34 Fuentes J.R., (2006). *New Jersey State Police Practical Guide to Intelligence-led Policing*, Center for Policing Terrorism at the Manhattan Institute, p. 4. http://www.njsp.org/divorg/invest/pdf/njsp_ilp-guide_010907.pdf, accessed on 30/01/2015.
35 U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, (2009). *Navigating Your Agency's Path to Intelligence-Led Policing*, Washington, DC pp. 3., 4. and 7. https://it.ojp.gov/docdownloader.aspx?ddid=1082, accessed on 26/01/2015.
36 Fuentes J.R., *Op. cit.* p. 36.
37 Wade C.L., (2010). *The California Law Enforcement Community's Intelligence-Led Policing Capacity*, Naval Postgraduate School, Monterey, California, p. 1., https://www.hsdl.org/?view&did=11524, accessed on 30/01/2015.

## FOCUSING THE POLICING ON THE BASIS OF CRIMINAL INTELLIGENCE PRODUCTS

The efficiency and effectiveness of the ILP is based on the continuous collection of quality information useful for preventing and detecting criminal offenses and misdemeanors, finding their perpetrators and other data related to police affairs.

The step further represents a planned, designed and targeted collection of data focused on the development of strategic and operational assessments (basic documents of the ILP in the policing). The Police Directorate of the Ministry of the Interior of the Republic of Serbia has developed the Strategic Assessment of Public Security[38]. Based on the Strategic Assessment of Public Security, the Strategic Plan of the Police Directorate is adopted and based on the Strategic Plan and operational assessments of the PD, the operational plans of the PD are adopted. A proactive approach in carrying out police tasks and directing resources to the greatest security issues is in full compliance with the primary tasks of the police, protection of fundamental rights and freedoms. At the highest, strategic level, the management and management tasks are carried out by the Strategic Management Group, and at operational level, by the Operational Management Groups. One of the key tasks of the Strategic Groups is identifying the most significant security threats, setting priorities and resources to be used. From this type of work, a plan of targeted information collection is emerging, which is the essence of criminal intelligence.[39]

Strategic assessment is also the basis for the development of an operational assessment, which contains information on the prognosis of the manifestation of selected priorities in the field of police departments for one year. In addition to national priorities, in the operational assessment, the forecast of the manifestation and typical security problems of each police department, if identified in the analysis, is carried out. The strategic and operational plan clearly defines the activities, the bearers of the activity, the time period of realization and the indicators of the activity. In addition, the operational plan may also include indicators for evaluating the results of the undertaken activities, the status of the activity (if the activity is not fully realized) and the indicators related to the necessary finance for undertaking activities.

In accordance with the identified priorities and planned activities in the operational plan, each organizational unit creates a tactical assessment of the projection of a security problem manifestation that is defined as a priority and elaborates its tactical plan. Based on the tactical assessment in the tactical plan, the activities to be undertaken are elaborated, for example the specific security problem (problem profile) and the security target (target profile).

These are criminal intelligence products produced by the organizational unit of the police in charge of criminal intelligence analytics. They give a clear, unequivocal picture of the bearer of criminal activity, describe in more detail series of criminal acts, the focus of crime, problems related to violation of public order on a larger scale. It should be noted that the Criminal Intelligence Model in Croatia envisages other "products" such as a control strategy and requests for the collection and processing of criminal intelligence data that elaborate objectives and tasks from strategic and tactical assessments in the direction of developing priorities and disposing of existing resources.[40]

38 Police Directorate, Strategic Assessment of Public Security, 2017, Belgrade.
39 Brnetic D., Kralj T., (2009). *Support by the police to parties in the proceedings and other parties according to the new criminal procedure act with an overview of the experiences of police actions related to victims and witnesses*, Croatian annual of criminal law and practice (16)2:475–519, https://bib.irb.hr/datoteka/474181.zbornik.pdf, accessed on 03/04/2015.
40 *Ibid.*

The essence of the ILP is, based on criminal intelligence, to make decisions on the conduct of operational police activities, set priorities and define strategic and operational goals in countering crime, especially organized crime, corruption and serious crimes, based on the special principle of the formed management groups at the strategic and operational level. In addition, the ILP provides operational policing and tasks in a more systematic way, which involves the use of available resources, the collection, analysis and use of data and information on crime in the most effective way, in order to achieve better results in countering crime and ensure better security of citizens and the community in whole.[41]

The criminal-intelligence process is the way in which raw information becomes a criminal intelligence. There is no uniform definition of the criminal intelligence process in professional and scientific literature. For the purposes of this paper, we can adopt the following definition: "The Criminal Intelligence Process (CIP) is a procedure which systematically uses the methodology of scientific research, in accordance with the previously defined task, to collect, process and analyze information with the aim of production of intelligence products based on which rational decisions are made on the organization of work and the use of police resources in countering security threats."[42]

The CIP consists of several phases for which there is no single position in the professional and scientific literature. The CIP in the state police of New Jersey generally consists of five permanent phases: Planning and Direction, Collection, Analysis and Production, Dissemination[43] and Evaluation[44]. According to A. Ivanovic, CIP includes the following: 1) criminal intelligence research initiative; 2) issuing an intelligence task; 3) collection of criminal intelligence data[45]; 4) assessment of collected criminal intelligence; 5) arranging (clearing) the received intelligence material; 6) integration of intelligence material; 7) analysis of consolidated intelligence; 8) performing operatively useful conclusions (converting intelligence into a finished intelligence product); 9) distribution of intelligence to users; 10) reassessment (re-evaluation)[46]. According to D. Korac, CIP consists of maximum six input/output phases: planning and organizing, collecting, processing, analysis and production, dissemination (sharing) and feedback[47].

For a better understanding of CIP and even ILP itself, it is important to mention the "3-i model". The essence of the "3-i model" is that the CIP takes place in three mutually related directions: 1) a criminal intelligence analyst interprets (analyzes) the criminal environment by using exact methods and collected and processed data and information; 2) the criminal intelligence analyst presents the intelligence products made and "influences" the thinking of decision-makers in decision-making; and 3) decision-makers, using intelligence products, "impact" the criminal environment in order to dismantle it (criminal groups) and reductions (crimes)[48].

In accordance with our model, the CIP is a set of three interconnected sub processes: 1) Management within the operations; 2) Criminal intelligence activities; and 3) Planned opera-

41 Klisaric M., Kostadinovic N., (2016) *Intelligence led policing-manual*, MoI RS, Belgrade, Foreword.
42 Djurdjevic, Z., Radovic, N., (2015b) *Op. cit.* p. 382; Compare with: Andonov O., Stankovic Pejanovic V., (2014). *Criminal intelligence: Theoretical and practical approach in modern police activity,* Vojno delo (66)3:147–159. http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2014-jesen/66-2014-3-10-Andonov.pdf, accessed on 03/04/2015.
43 *Aut. rem.* scheduling, delivery or distribution of analytical products to last-users.
44 Joseph R. Fuentes, *Op. cit.* p. 6
45 Compare with: Manojlovic D., (2005) *Crime intelligence work*, Bezbednost (47)1:108–119.
46 Ivanovic A.R., (2014). *Criminal intelligence in the function of protecting national security*, Perjanik, (12)31:60. http://www.policijskaakademija.me/perjanik/31.pdf, accessed 21/06/2016.
47 Korac, D., (2010). *Intelligence cycle in intelligence agency*, Criminal Justice Issues (10)1-2:70–71 http://krimteme.fkn.unsa.ba/index.php/kt/article/view/36/Full%20Text, accessed on 21/06/2016.
48 Ratcliffe, J.H., (2003). *Op. cit.* pp. 3–4.

tional policing. More detailed CIPs consists of 12 basic functions, as follows: 1) Strategic and operational planning; 2) Request; 3) Planning of criminal intelligence; 4) Collecting (data); 5) Processing; 6) Analysis; 7) Delivery; 8) Deciding; 9) Planning operational policing; 10) Implementation; 11) Monitoring; and 12) Evaluation and management of quality[49]. In addition to the listed segments, an important feature of the CIP is the international operational police cooperation in data (intelligence) exchange[50].

The key element of ILP is definitely an analysis. According to the definition of INTERPOL, criminal intelligence analysis[51] is the identification of criminal phenomena and the provision of understanding of data on crime and other potentially relevant data aimed at the successful implementation of laws and combating crime by the police and courts.[52] At the tactical level, the analysis can be used to gain local community support and policing through problem solving, crime prevention and all kinds of investigations. The policing through troubleshooting is the form of the ILP which involves the collection of all available crime data, the determination of the scope of the problem through data analysis and the provision of potential solutions to decision makers. At the strategic level, some of the same data collected for tactical purposes can be combined with other information for the "production" of crime assessment and to develop potential long-term solutions to these problems.[53]

All state authorities that implement laws, and especially those in the field of security, are engaged in intelligence work. On the one hand, the intelligence and security services have the basic task of timely and thoroughly gathering information important for national security and security of the state. On the other hand, the police are tasked with protecting citizens and their property from all forms of endangering their security, protecting the basic rights and freedoms of citizens guaranteed by the Constitution and the laws of the Republic of Serbia. Police are engaged in crime-intelligence work that is strictly standardized, which takes care of the protection of the rights and freedoms of citizens and is exclusively focused on crime and other security-related phenomena that can lead to endangering the safety of citizens[54]. Viewed from the normative-practical angle, the Serbian police, in their work on combating crime, collect data through classical operational work or through intelligence research. Operational work includes the use of legal powers, applying the principles of criminalistics and the use of operational tactical and technical measures and actions, as well as the police working methods. An intelligence research is a set of police activities that, with the implementation of all available operational tactical and technical measures and police actions, are directed to systematically collecting intelligence about a particular incriminated phenomenon, an event, a person, and an organized criminal group for which processing is necessary for a longer period of time. An intelligence research cannot be conducted by all police officers, but rather by the specialized service of the Criminal Intelligence Service and the Covert Investigators in the Criminal Police Directorate of MoI RS[55].

49 Klisaric, M., Kostadinovic, N., *Op. cit.* p. 8
50 More info in: Nikac, Z., (2015). *International police cooperation*. ACPS, Belgrade.
51 More info in: Andonov O., Stankovic Pejanovic V., *Op. cit.*
52 http://www.interpol.int/INTERPOL-expertise/Intelligence-analysis, accessed on 03/04/2015.
53 Peterson M.B., (1997). *The Role of Analysis in Intelligence-led Policing.* In International Perspectives on Policing in the 21st Century, IALEIA, Lawrenceville, New Jersey, https://members.ialeia.org/files/other/ILP%20intl%20perspectives.pdf, accessed on 26/01/2015.
54 More info in: Andonov O., Stankovic Pejanovic V., *Op. cit.* and Fatic A., (2011). *Criminal intelligence and traditions of civil and human rights,* in ed. Social Aspects of Organized Crime, Institute for International Politics and Economy, pp. 11–22.
55 Mandatory instruction on the operational work of the police, an internal act of MoI.

## CONCLUSION

ILP can be defined as a model of police management which involves the use of collected and analyzed information through analytical products when making decisions at all levels of management (strategic, operational and tactical) in order to more efficiently use human, material, technical and financial resources in order to prevent and reduce crime and other security-related issues.

In order for the policing to be truly guided by intelligence, the first phase of this model would have to be readiness to interpret the criminal environment. The second phase requires an intelligence structure that is ready to identify and influence decision makers. At the end of the ILP, decision makers need to have enough enthusiasm and skills to explore ways to reduce crime and have a positive impact on the criminal environment.[56] An organizational unit that would deal with strategic analysis tasks for the needs of the police, analysis of collected information, production of analytical products and generally ILP support should be part of the Police Directorate, which is the recommendation of the OSCE[57].

By researching the attitudes of police officers, it has been concluded that most respondents have a positive attitude towards the strategic approach in the work of the criminal police[58]. It can also be concluded that most police officers tie the word "intelligence" to closed sources of information while open sources are completely neglected, which can lead to unreliable information on the criminal environment[59]. Based on this research, it can be concluded that it is necessary first and foremost to provide training and professional upgrading for police officers[60] in the field of ILP in order for the model to be adequately implemented.

Every piece of information collected by a field police officer or a local community policeman must be assessed and stored in a database, analyzed by a professional analyst who will produce the appropriate product in order to predict certain security risks. Ultimately, the manager, based on the analytical product, makes decisions on organization of police affairs and adequate direction of human, material, technical and financial resources. Based on these data collected, the Police Directorate, in accordance with European standards and good practice of international police organizations, issues a **Strategic assessment** that can include: 1) assessment of identified risks, threats and damage to citizens' safety in a given period; 2) assessment of the effectiveness of measures and actions undertaken in the previous period; 3) priorities and guidelines for the policing; and 4) analysis of the required capacities at the level of the Police Directorate and regional police departments.

Based on the Strategic Assessment and the collected data, the regional police departments adopt an **Operational Assessment** that can include: 1) an assessment of the security in the territory for which the regional police department has been established, with identified risks, threats and consequences for the safety of citizens; 2) predicting the development of the security; 3) assessment of the effectiveness of measures and actions undertaken in the previous period; and 4) proposal of priorities with recommendations on measures and actions. Based on the Strategic Assessment, the Police Directorate adopts the **Strategic Plan**, and on the basis of the Operational Assessment, the regional police departments issue the **Operational Plan**. Strategic and operational plans contain defined priorities, activities, performance indicators,

56 Ratcliffe J.H., (2003). *Op. cit.* p. 3.
57 More info in: Downes M, (2004). *Police reform in Serbia – towards the creation of a modern and responsible police service.* OESC, Mission in Serbia and Montenegro, p. 42. First of all, this refers to all analytical units that are outside the Police Directorate.
58 More info in: Simonovic, B., (2011). *Research of the attitudes of the criminal investigation police officers MIA Serbia on strategic approach to crime combating*, Bezbednost (53)1:5–27.
59 More info in: Sebek, V., (2015). *Sources of information in criminal intelligence*, Bezbednost (57)3:49–70.
60 *Ibid.*

bearers, resources and deadlines, as well as a mechanism for reporting, monitoring and evaluating the results achieved. In addition, the operational plan should also contain operational objectives with the methodology of their implementation.

In addition to Strategic and Operational Assessments and Strategic and Operational Plan, analytical products should identify both the target's profile and the profile of the problem. **The profile of the target** or the profile of a security-sensitive person should include the assessment of a particular person as a carrier of criminal activity (usually organized by a criminal group) with identified risks, threats and damage to citizens' safety, proposal of activities, bearers, resources and deadlines with methodology of realization of activities directed at a person who is a criminal activity. **The profile of the problem** should include an assessment of a security problem in a particular territory that requires resolution of the identified risks, threats and consequences for citizens' safety, proposal of activities, bearers, resources and deadlines with the methodology of realization of activities directed at a specific problem.

Based on the adopted plans, managers could plan to use human, material, technical and financial resources to carry out planned tasks at the daily, monthly and annual levels. Human, material and technical resources through the daily/weekly schedule of work would be used at the time and place where it is estimated that occurrences and events of interest for the service can occur and where this is already planned for the purpose of proactive action. Managers direct the activity of police officers to solve specific problems of citizens and the local community. The operational work of the police officers would be aimed at collecting information about a particular incriminated phenomenon, event, person or organized criminal group. This would result in significant savings in financial resources which would not be wasted unnecessarily with the possibility of daily, monthly, quarterly and annual monitoring of the use of all resources.

The most important part of the establishment of the ILP, is training. The staff already in the MoI and candidates who are still trained for policing, both police officers in the patrol, as well as the leaders of the strategic level, must pass through training. The most important role in training is certainly the Academy of Criminalistic and Police Studies, Basic Police Training Centre and the education system, professional upgrading and training in the MoI. The introduction of the ILP into the practice of the Serbian police, according to the authors, will not require much effort for several reasons: 1) the Serbian police is organized as a centralized state administration body led by the Police Directorate, which is a process of management and decision-making according to the ILP model, and in many ways it makes it easier; 2) certain segments of the ILP, in particular the process of planning, management and decision-making, are already being implemented in the practice of the Serbian police; 3) changes in the organizational structure of the MoI, the normative framework and the databases in order to establish the ILP are minimal; 4) a system of training and professional upgrading in the Serbian police can meet the needs of the ILP for its full implementation.

The introduction of the ILP should not neglect the model of community policing. On the contrary, these two models together with problem-oriented policing should be a "guide" for the entire police organization in Serbia. It is necessary to ensure that all models of policing get their role in the work of the police in Serbia and to ensure the necessary level of planning, direction and coordination in the implementation of all models of policing.

LITERATURE

1. ACPO, Centrex, (2007). *Practice Advice: Introduction to Intelligence-Led Policing.*
2. Andonov O., Stankovic Pejanovic V., (2014). *Criminal intelligence: Theoretical and practical approach in modern police activity,* Vojno delo (66)3:147–159.
3. Bell P., Congram M., (2013). *Intelligence-Led Policing as A Strategic Planning Resource in the Fight against Transnational Organized Crime*, International Journal of Business and Commerce (2)12:15–28.
4. Brnetic D., Kralj T., (2009). *Support by the police to parties in the proceedings and other parties according to the new criminal procedure act with an overview of the experiences of police actions related to victims and witnesses*, Croatian annual of criminal law and practice (16)2:475–519.
5. Butorac, K., (2011). *Geography of Crime-Criminological and Criminalistics Discourses*. Police and Security (20)3:363–379.
6. Cacan, A., (2010). *Geographic profiling as a criminal investigative methodology in criminal investigation of serial crimes*. Criminal Justice Issues (10)3-4:155–173.
7. Cavkov, M. *et al,* (2014). *Criminal intelligence manual*, DCAF Institute, Ljubljana.
8. Clarke P., (2016). *Intelligence-led Policing in Counter-Terrorism: A Perspective from the United Kingdom*, in ed. Wither, J.K, Mullins S. Combating Transnational Terrorism, Procon, Sofia, pp. 149–162.
9. Constitution of Republic of Serbia, "Official Gazette of Republic of Serbia", No. 98/06.
10. Criminal procedure Code, "Official Gazette of Republic of Serbia", No. 72/11, 101/11, 121/12, 32/13, 45/13 and 55/14.
11. Djurdjevic, Z., Radovic, N. (2015a). *The EU's strategic directions for countering crime and their significance for the Republic of Serbia*. Serbian Political Thought, 22(4): 275–291.
12. Djurdjevic, Z., Radovic, N. (2015b). *Kriminalisticka operativa*, ACPS, Belgrade.
13. Downes, M. (2004). *Police reform in Serbia – towards the creation of a modern and responsible police service.* OESC, Mission in Serbia and Montenegro.
14. European Convention for the Protection of Human Rights on Fundamental Freedoms, "Official Journal of Serbia and Montenegro – International agreements", No. 9/2003 & 5/2005.
15. Fatic A., (2011). *Criminal intelligence and traditions of civil and human rights,* in ed. Social Aspects of Organized Crime, Institute for International Politics and Economy, pp. 11–22.
16. Fuentes J.R., (2006). *New Jersey State Police Practical Guide to Intelligence-led Policing*, Center for Policing Terrorism at the Manhattan Institute.
17. Goldstein, H. (1990). *Excellence in problem-oriented policing*, McGraw-Hill, New York.
18. Goldstein, H. (1979). *Improving policing: A problem-oriented approach*, Crime & Delinquency, (2)25:236–258.
19. Harcourt B.E., Ludwig J., (2006). *Broken Windows: New Evidence from New York City and a Five-City Social Experiment*, The University of Chicago Law Review (73)93:2–47.
20. Henry, V. E. (2006). *Managing crime and quality of life using CompStat: Specific issues in implementation and practice,* Resource material series, No. 68, 129th International Senior Seminar Visiting Experts' Papers, 117–132.
21. Ivanovic A.R., (2014). *Criminal intelligence in the function of protecting national security*, Perjanik, (12)31:54–80.

22. James A., (2011). *The Influence of Intelligence-Led Policing Models on Investigative Policy and Practice in Mainstream Policing 1993-2007,* Department of Social Policy of the London School of Economics and Political Science, London.
23. Klisaric M., Kostadinovic N., (2016). *Intelligence Led Policing-manual*, MoI RS, Belgrade.
24. Korac, D., (2010). *Intelligence cycle in intelligence agency*, Criminal Justice Issues (10)1-2:79–97.
25. Laverty, I., MacLaren, P. (2002). *Geographic profiling: A new tool for crime analysts*. Crime mapping news, (3)4:5–8.
26. Lestanin, B, Nikac, Z, (2016). *Comment of Police Law*, Poslovni biro, Belgrade.
27. Mandatory instruction on the operational work of the police, an internal act of MoI.
28. Manojlovic, D., Jovic, V., (2004). *National crime intelligence service,* Bezbednost (46)3:419–430.
29. Manojlovic D., (2005) *Crime intelligence work*, Bezbednost (47)1:108–119.
30. Markovic, J., Christopher, S., (2002). *Criminal mapping and policing in democratic societies*, Bezbednost (44)4:64–652.
31. Nikac, Z. (2009), *Community policing,* ACPS, Belgrade.
32. Nikac, Z. (2015). *International police cooperation*, ACPS, Belgrade.
33. Peterson M.B., (1997). *The Role of Analysis in Intelligence-led Policing,* In "International Perspectives on Policing in the 21st Century", IALEIA, Lawrenceville, New Jersey.
34. Police Directorate, Strategic Assessment of Public Security, 2017, Belgrade.
35. Law on Police, "Official Gazette of Republic of Serbia", No. 101/05, 63/09 – Decision of the Constitutional Court, 92/11 and 64/15.
36. Law on Police, "Official Gazette of Republic of Serbia", No. 6/16.
37. Ratcliffe, J. H. (2007). *Integrated intelligence and crime analysis: enhanced information management for law enforcement leaders*. Washington: Police Foundation.
38. Ratcliffe J.H., (2003). *Intelligence-led policing*, Australian Institute of Criminology.
39. Ratcliffe J.H., (2008). *Pocket guide to intelligence led policing*, Willan Publishing: Cullompton, Devon.
40. Sebek, V. (2015). *Sources of information in criminal intelligence*, Bezbednost (57)3:49–70.
41. Simonovic, B., (2011). *Research of the attitudes of the criminal investigation police officers MIA Serbia on strategic approach to crime combating*, Bezbednost (53)1:5–27.
42. Spelman, W., Eck, J.E. (1987). *Problem-oriented policing*, US Department of Justice, National Institute of Justice.
43. The Law on Free Access to Information of Public Importance, "Official Gazette of Republic of Serbia", No. 120/2004, 54/2007, 104/2009 & 36/2010.
44. The Law on Organization and Jurisdiction of State Authorities in the Suppression of Organized Crime and Corruption and Other Particularly Serious Crimes, "Official Gazette of Republic of Serbia", No. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 – other law, 45/2005, 61/2005, 72/2009, 72/2011 – other law, 101/2011 – other law & 32/201.
45. The Law on Personal Data Protection, "Official Gazette of Republic of Serbia", No. 97/2008, 104/2009 – other law, 68/2012 – decision of CC & 107/2012.
46. The Law on the Basis of Regulation of Security Services of the Republic of Serbia, "Official Gazette of Republic of Serbia", No. 116/2007 & 72/2012.
47. The Law on Secrecy of Data, "Official Gazette of Republic of Serbia", No. 104/2009.

48. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, (2009). *Navigating Your Agency's Path to Intelligence-Led Policing*, Washington, DC.
49. Vojinovic, M., (2004). *Community policing*, Bezbednost (46)3:432–452.
50. Wade, C.L. (2010). *The California Law Enforcement Community's Intelligence-Led Policing Capacity*, Naval Postgraduate School, Monterey, California.
51. Wilson, J.Q., Kelling, G.L. (1982). *Broken windows: The police and neighborhood safety,* The Atlantic Monthly (3)249:29–38.

# INTERPRETATION OF CRIMINAL TATTO SYMBOLS IN PRISON FACILITIES

**Lt. Col. Barbora Vegrichtová, Ph.D.,MBA**
Police Academy of the Czech Republic in Prague

**Abstract:** The article discusses the importance of tattoo in the criminal environment and prison subculture. Special attention is paid to the function of tattoos, especially in the area of identification and communication. Frequently used symbols have a considerable explanatory value. They reflect the criminal past of the wearer, expressing religious or ideological beliefs, indicate a process of radicalisation, membership in a criminal group or gang. With the help of analysis of the selected tattoo symbols it is possible to collect valuable information about the personality profile of a particular individual.Information about inmate's criminal past, special skills, personal characteristics and preferences can be principal in the penitentiary procedures and measures. The styles and forms of tattoos are variable and pose a unique way of secret communication, namely in prison environment. Many tattoo's motifs are spread and shared by the criminals on the international level. With few exceptions, Russian, Asian or street gang's tattoos can be found in correctional facilities all over the word, in most cases with the same meaning and importance. Criminal tattoos interpretation is useful especially in the police and security practice. Complex information about criminal signs and symbols, includingthat of criminal tattoos, have to be disseminated among the members of law enforcement authorities in order to improve their knowledges about criminal scene. Empirical research and content analysis of criminal tattoo symbols is crucial in the identification procedures of potential risky person in the criminal and prison subculture but also his affiliation in the extremist organisation, street gangs and socio-pathological communities. The information in the paper are exemplified by authentic photos from the author's archive.

**Keywords: c**ommunication, criminal subculture, identification, meaning, tattoo

## INTRODUCTION

Criminal environment represents a specific hidden culture which has at disposal its own codes, language, and symbols, which are as a rule strictly guarded and kept in secrecy. Varied symbolic rituals, initiation processes, ceremonies, and tests, which are accompanied with the accession of a new member to a criminal organisation, form an integral part of this world. Organised crime syndicates, street and prison gangs, outlaw motorcycle clubs and other social pathological groups developed and adopted their own rituals and terminology. Some authors and experts in this field even call this system the criminal subculture codes.

Codes and symbols used in criminal groups and subcultures pose a specific phenomenon enhancing internal relation among members. Symbols help to strengthen collective identity in a very intensive way. Impressive criminal symbols can stir up human emotions, both positive and negative. Internal cohesiveness in criminal community is more than important in a group motivated by shared ideological, political or religious beliefs. Widespread use of symbols is therefore an essential attribute of different extremist and even terrorist organisation.

Gang members communicate using various methods. Besides the common communication in words these groups employ widely varied alternative ways of communication and information conveying. Graffiti, sign language, movement and clothing styling, hairdo variations, postures, gestures, and tattoos express affiliation with a certain group and the social status within the formation.[1]

A symbol represents a summary, apt expression of little known fact that is hard to capture in another way. It is of complex nature. On the one hand, it offers its content to the human reason; on the other hand, it cannot be perceptible by the reason. Therefore, it addresses both thoughts and emotions. Its liveliness, as one of its most important traits, is based on the symbol experience intensity.[2]

Symbols are used almost on a daily level especially in prison facilities all over the world and many symbols are of international importance. It necessary to highlight the fact, that criminal symbols are used as secret communication under the specific prison conditions. Hidden meaning of particular symbols could mask different tactics, messages and information, understood only by the inmates. Thus, criminal symbols can provide a wealth of information, but only if competent employees know the real meaning.The following text describes conceptual and theoretical background of research project and the crucial particular findings of empirical research, which has been realised by the author in the Czech correctional facilities.[3]

## CONCEPTUAL AND THEORETICAL BACKGROUND

In every research project it is inevitable to define the essential methodological methods and empirical background. The base of the project was in the continuous empirical research in the correctional facilities in the Czech Republic. It is indispensable to mention that simply getting access to a prison can be difficult for researchers. Prisoners are regarded as a vulnerable population for research study purposes. This study couldnot be realised without help of the employees of Prison Services of the Czech Republic.

The population of the Czech Republic is over 10 million and at the beginning of this year the number of prisoners was about 19,000, out of that 2,190 of pre-trial detainees. There are 41 persons in forensic detention facilities and roughly 1,600 prisoners are foreign nationals.

There are in total 35 prisons in the Czech Republic and each prison has its own governor. Approximately 11,000 employees work within the Prison Services of the Czech Republic. The central management is operated by the Prison Service General Directorate under the Ministry of Justice.

There are four basic types of prisons in the Czech Republic. They can be classified as follows: minimum, medium, high and maximum security.

The minimum security prisons hold convicts who are sentenced for the least severe offences. In the high and maximum security prisons there are convicts who are sentenced for the most severe offences.

There are more than 9,000 convicts in the high security prisons. In the maximum security prisons there are roughly 1,100 convicts. There are 50 convicts sentenced to life imprisonment, 47 male convicts and 3 female convicts.[4]

1 VALENTINE, B. (2000). *Gangs and their tattoos. Identifying Gangbangers on the Street and in Prison.* Boulder, Colorado: Paladin Press. pg. 7.
2 BECKER, U. (2007). *Slovníksymbolů.* Praha: Portál. pg. 287.
3 It has to be highlighted, research study is still ongoing.
4 For more information: www.vscr.cz

All research subjects (incarcerated persons) were informed of the potential risks and benefits of their participation, and they received enough understandable information to make a voluntary decision. Informed consent and voluntary participation are fundamental ingredients of ethical research. The inmates in the Czech prisons were interviewed by the author and during these procedures the tattoosymbols were documented. The information gathered from respondents were marked in the questionnaire prepared in advance. All dates were compared, analysed and the final findings were interpreted with regard to content analysis of relevant tattoo symbols, tattoo application methods, tattoo purpose and importance and other causalities.

Concerning the expected outcomes, the ambition of the research team is innovation of information system used by the Czech criminal police and investigation service related to the databases of criminal tattoo symbols. Research team have been developing electronic encyclopaedia of criminal tattoo symbols logically categorizing relevant symbols in specific groups accompanied with adequate description and risk assessment.

## SIGNIFICANT RESEARCH FINDINGS

Symbols in the form of tattoos related to the criminal environment, in other words to organised criminal groups and gangs, express several basic facts and deliver a numerous functions in the criminal environment. The following list of functions of the criminal tattoos is by far not exhaustive:

- Affiliation to a Certain Group
- Power Ambitions
- Collective Identity of a Group
- Demonstration of Strength and Means of Intimidation
- Hateful Motif and Ideological Conviction
- Power Ambitions
- Indicator of Radicalisation Process
- Means of Communication

In the environment of the US prisons there are also tattoos of pure purpose based on opportunism and calculus of the wearer. On this fact D. K. Hall says: "Certain tattoos arouse fear and respect and provide their wearer with a look of a "rough boy". In some cases convicts acquire them just for these reasons, even though they undergo a significant security hazard by doing so. A well-chosen tattoo of, for instance, a member of a motorcycle gang may make life in the prison cell easier and more secure. On the other hand, an inmate caught with a tattoo acquired by fraud may be physically punished or even killed."[5]

The selection of tattoo motifs and their design preferred in the criminal environment or by persons in the sentence of imprisonment may change over time and is affected by numerous factors. For instance, the members of extremist movements, street gangs or outlaw motorcycle gangs are extremely prone to using symbols. They usually adopt many symbols to represent their organisation, ideological point of view or a gang. Using symbols, including specific tattoo motifs work as part of propaganda and intimidation of potential victims, political opponents, rivals or law enforcement representatives.

Prominent criminal tattoos indicating affiliation to a certain gang are very impressive and spectacular. For this reason members place their tattoos mostly on hands and faces. Curtis

5 HALL, D.K. (1997). *Prison tattoos.* USA: St. Martin's Griffin. Pg. 210.

Allgier is an iconic person of the underworld inseparable namely from neo-Nazi structures and their supporters. He has his face all covered in tattoos which are exclusively of hate and racist nature. In 2012 Allgier murdered an employee of the prison guard escorting him while trying to escape. He was sentenced to death penalty for this felony yet he appealed against the judgement. At present the Utah Supreme Court resorted to an uttermost measure and dismissed Allgier's right to attorney following Allgier repeatedly intimidated and menaced his attorneys with violence.[6]

Representatives of police and government in general are frequently addressees of the hate symbols in the form of tattoos, signs, or gestures. One of the most popular tattoos among incarcerated persons in the Czech prisons is the so called ACAB sign. The ACAB acronym is an anti-police slogan meaning the phrase "*All Cops Are Bastards*".The "ACAB" tattoo can be found in the representativesof various non-conform subcultures and usually groups of delinquents, quite often of contradictory characters and compositions. Yet these groups are clearly linked together by their hate to police and employees of government security forces in general. Wearers of the tattoo can be identified among neo-Nazis, anarchists and extremists in general, football hooligans, members of motorcycle gangs, addicts, gamblers, habitual criminals, persons perpetrating various felonies, and other persons whose activities are mostly of illegal character.

Current terrorist organisations do not avoid symbolism, either hidden or open. The Islamic State and its devoted adherents use in their attacks or in propaganda a flag with symbols of Islam which arouse respect and fear.

There is so-called shahada, an Islamic statement of faith "There is no God but God and Mohammed is God's messenger" in white on the black backdrop in the flag. The second part of the shahada on the IS flag is depicted in the form of so-called Prophet Seal. Muhammad and the first caliphs are believed to sign official documents by this round emblem. "The power of the flag comes from the fact that the word 'Allah' is on it. The word itself is seen as sacred by Muslims," explained Hayder al Khoei, an expert on Middle East, for Time magazine.


*Anti-police acronym "ACAB" – All cops are bastards*

6 ROBINSON, W. (2015). White supremacist cop killer with tattoos all over his face loses right to an attorney after continuously threatening them and saying they do not have the honor of being in his 'Aryan GOD presence'. *Daily Mail Online*. Retrieved April 24, 2015 from http://www.dailymail.co.uk/news/article-2924453/White-supremacist-cop-killer-tattoos-face-loses-right-attorney-continuously-threatening-saying-not-honor-Aryan-GOD-presence.html

Selected tattoo symbols and motifs are widely spread in the criminal environment and prison subculture. Prison inmates create a specific and closed community with unique codes, values and behavioural norms. Unformal convict code of correctional facilities represents internal system of unwritten rules, whose betrayal attracts different types of sanctions and punishments. A part ofprisonization process is undertaken by "newcomers", i.e. the inmates who first enter the prison, reflects a long process of adoption to prison conditions. Survival in prisons is directly connected with appropriate understanding of internal rules and codes. Application of specific tattoo motifs can signify an acceptance of convict code or even identification with criminal community and a criminal way of life (criminal lifestyle).This term means a way of thinking and behaving whereby criminals are career criminals. It is a way of being, whereby criminals engage in recidivistic behaviour because of their way of viewing the world and themselves. Many researches worldwide came to identical findings, that having numerous tattoos is more consequential on recidivism[7] namely in a group of older inmates.

Overall, it seems there may be a connection between criminals who obtain prisontattoos, i.e. either tattoos that were made in prison or that are of prison images, andidentification with criminality as a subculture or way of life. The concept of a careercriminal stems from empirical research showing that the majority of crimes arecommitted by a minority of criminals, i.e. a percentage of criminals are repeat offendersthereby making criminality their career of choice. This subgroup of offenders isessentially identifying with a criminal lifestyle and a criminal culture. Since theseindividuals are criminals for life, recidivism is connected to this theory. Statistics showthere are a greater percentage of repeat offenders who have tattoos as compared to thegeneral public, although the type of tattoos was unspecified.[8]

Tattoos made in prisons could be very specific technically, from the esthetical and coloured point of view and in terms of symbol and motifs scale. Prison tattoos may serve rebellious function, in many cases represent a masculine statement,and symbolizeresistance to conformity and traditional norms and a defiance against the legal system.The criminal and prison tattoos may indicate inmate's emotional and physical endurance, some tattoos are an integral part of initiation rites of young delinquents formally joining a criminal family. The first symbols of recidivist criminals are usually tattooed in the youth detention centres or in children's home.

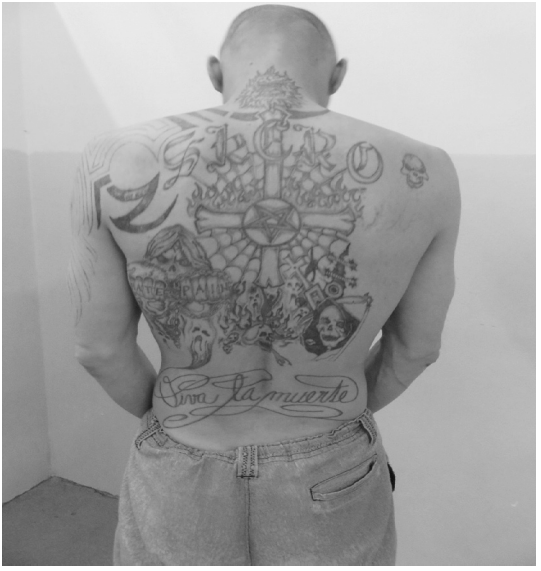
*The first tattoo has its origin usually in youth detention centres – small cross represents affiliation in a gang*

7 When criminals return to prison repeatedly; criminals who continually commit crimes and get arrested and sentenced for this behavior.

8 ROZYCKI, A. (2007). *Prison Tattoos as a Reflection of the Criminal Lifestyle and Predictor of Recidivism* Texas: Graduate Faculty of Texas Tech University, Electronic Theses, Treatises and Dissertations. pg. 5.

Tattoos simultaneously symbolize a group-organizational association and the hierarchical status of an individual. Prisoners use tattoos to represent their strength and status, to mark their belonging to a certain group, to create a unifying symbol, and to define their status and position within their group.[9]

Motifs of deaths, defeatism, negativistic opinions and approaches, defiance to the conventional society are heavily spread in the correctional facilities. Especially those symbols that are religious, biblical, or mystical in nature are frequently shared by prison community and are accompanied by the symbols of Satanism, occultism, paganism and other controversial faiths, beliefs or anti-social themed tattoos. Anti-social tattooshave images or themes that convey hostile messages against individuals, ethnic minorities, specific groups or subcultures within society, or society in general. These tattoo symbols are depicting aggressive, vulgar, morbid, or demonic images, or dire circumstances (e.g., images related to addiction), or depict images or themes of societal rules violations.




*Satanist and hateful tattoo symbols of an inmate located in one of the most guarded and safest prisons in the Czech Republic.*

The incarcerated persons usually choose the tattoo symbols representing and depicting criminal and prison images and themes (prison bars, spider web, prison inmate's number, spider web, barbed wire, etc.) Some symbols represent the indicator of affiliation in a criminal group or a gang. During the realised empirical research there were many different criminal tattoo categories identified. Particular tattoo symbols system were revealed and registered by the following entities:[10]

- African criminal groups
- Anarchists
- Asian gangs
- Drug addicts and drug dealers

9 SHOHAM, E. *Prison Tattoos. A study of rusian Inmates in Israel.* Switzerland: Springer International Publishing, 2015. pg. 49.
10 In alphabetical order.

- Football hooligans
- Gangs (prison/street gangs)
- Neo-Nazis
- Outlaw motorcycle gangs
- Radicalised persons
- Russian criminal group
- Satanists.

Every wearer of a tattoo or symbols of other categories must be assessed completely and in an individual approach at the same time. The interpreting of tattooed symbols can bring valuable information on the wearer personality solely if adequate level of objectivity and pragmatic assessment are applied. It must be emphasised that the tattooed symbols are just one of a lot of circumstantial evidence, which, if combined with other findings, may create a more complete profile of a given individual. Pieces of information can give a puzzle of summary information, processing of the pieces gives knowledge that is conditioned to practice and experience of the processing person.

## SUMMARY

It is of the utmost importance for the work and performance of duty of members of security forces, who virtually on a daily basis move in the criminal environment or are in contacts with its representatives, to have as much as possible information on such persons. Information on the way and about what they think, how they behave in communication processes, which determine and form their responses, is very essential. Such information represents useful tool, which may be used for operations in the criminal environment, especially when choosing suitable procedures and tactics for treatment of and dealing with these persons.

Higher awareness and sharing information in the field of criminal tattoos interpretation is a helpful mechanism especially for actors participating in combating different forms of criminality and other related socio-pathological behaviour. Target audience of the research findings namely are:

- Police Forces (Law Enforcement)
- Intelligence Services
- Prison Service
- Customs Administration
- Fire Rescue Service
- Emergency Medical Service
- Lecturers od Police Schools
- Staff of Ministry of Interior
- Armed Forces
- Refugee Facilities Administration, etc.

Qualified "reading" and interpreting of meanings of the criminal tattoos' symbols is a useful skill and practical tool, particularly in the field of the work of police and other actors collaborating in combating criminality and undesirable social phenomena.

The author's interest is to provide the information found to the employees of security forces by means of a suitable way within pedagogic activities and lecturing, extraordinary

education, and life-long education courses with the objective of making their activities more efficient and ensuring their personal security. At the same time increased awareness on these issues may affect as a prevention tool ina conflict situation or hazardous event in their professional as well as personal life.

## REFERENCES

1. BECKER, U. (2007). *Slovníksymbolů.* Praha: Portál. ISBN 978-80-7367-284-3.
2. GIBSON, C. (2010). *Symboly a jejichvýznamy.* Praha: Slovart. ISBN 978-80-7391-370-0.
3. GOLDBERG, L. (2001). Gang Tattoos: Signs of Belonging and the Transience Stigma. *linagoldberg.com*. Retrieved April 24, 2015 from http://www.linagoldberg.com/gangtattoos/
4. HALL, D.K. (1997). *Prison tattoos.* USA: St. Martin´s Griffin. ISBN 978-0-312-15195-0.
5. LUNDE, P. (2012). *Tajemstvíkódů.* Praha: NakladatelstvíSvojtka& Co. ISBN 978-80-256-0978-1.
6. PRUSHER, I. (2014). What the ISIS Flag Says About the Militant Group. *Time*. Retreived February 1, 2015 from http://time.com/3311665/isis-flag-iraq-syria/
7. ROBINSON, W. (2015). White supremacist cop killer with tattoos all over his face loses right to an attorney after continuously threatening them and saying they do not have the honor of being in his 'Aryan GOD presence'. *Daily Mail Online*. Retrieved April 24, 2015 from http://www.dailymail.co.uk/news/article-2924453/White-supremacist-cop-killer-tattoos-face-loses-right-attorney-continuously-threatening-saying-not-honor-Aryan-GOD-presence.html
8. ROZYCKI, A. (2007). *Prison Tattoos as a Reflection of the Criminal Lifestyle and Predictor of Recidivism* Texas: Graduate Faculty of Texas Tech University, Electronic Theses, Treatises and Dissertations.
9. SHOHAM, E. *Prison Tattoos. A study of Russian Inmates in Israel.* Switzerland: Springer International Publishing, 2015.ISBN 978-3-319-15870-9.
10. VALENTINE, B. (2000). *Gangs and their tattoos. Identifying Gangbangers on the Street and in Prison.* Boulder, Colorado: Paladin Press. ISBN 978-1-58160-099-5.
11. VEGRICHTOVÁ, B. (2013). *Extremismus a společnost*. Plzeň: Vydavatelství a nakladatelstvíAlešČeněk. ISBN 978-80-7380-427-5.
12. WATERS, K. (2012). *The Tattooed Inmate and Recidivism. Florida:* The Florida State University. Electronic Theses, Treatises and Dissertations. Paper 5262.

# SUBJECTS IN TAX LAW RELATIONS IN THE REPUBLIC OF SERBIA

**Mirko Kulić**
University Bussiness Academy
**Goran Milošević**
University of Novi Sad, Faculty of Law
g.milosevic@pf.uns.ac.rs
**Cvjetana Cvjetković**
University of Novi Sad, Faculty of Law

**Abstract:** Tax procedure represents the activity of taxation authorities and the taxation debtor, which is necessary in each tax legal relation, to determine the existence of tax obligations and estimated, both objective and subjective elements legal description of the tax facts. Activity subjects, participants in the tax procedure, leads to their mutual relations tax law. Under the tax legal relation involves the relationship of public law in which enters the body in charge of conducting the tax proceedings and a natural or legal person in relation to the resolution of tax issues. This means that the parties in the tax relationship are the body responsible for the conduct of tax procedure, on the one hand, and natural or legal person, on the other hand. Starting from the role of participants in the tax procedure, they can be divided into: main, that required participants; Special participants (public prosecutor) and possible participants (witnesses, experts and interpreters).

**Keywords:** tax procedure, the tax authority, tax debtor, the tax legal relation

## INTRODUCTION

The tax procedure is a set of formalized actions, aimed at providing information, legal facts and evidence in order to resolve a tax matter. It includes the process of collecting data on the basis of accounting documents, cadastre, tax returns and other sources, data processing, determining the base and later responsibilities, then the collection and control of public revenue. Although this is a very living matter, whose regulation in Serbia has still been enlarging, during the tax procedure must always be a harmonious relationship between the tax administration on the one hand, and taxpayers on the other side.

The tax procedure is the activity of the tax authorities and the taxpayer, which is essential in any tax legal relation, to assess how objective and subjective elements of the tax legal description of the facts are with the aim of resolving specific tax matter. The tax liability has to be individualized, both in terms of its very existence, and in terms of the tax debtor and scope of benefits.[1] How it occurs at the moment when it actually happens to a particular event (when a person realizes income, etc.), which can be subsumed under the legal description of the tax facts, it becomes necessary to concretize the requirements of public-legal bodies, as well as tax liability.

1 G. Milošević, *Utvrđivanje javnih prihoda*, S.Palanka, 2002, str. 41.

Tax treatment includes several interrelated and conditioned actions: determination, collection and control of public revenue. Establishing public revenues should be understood as an activity which consists in taking the statutory action, establishing of tax liability and imposing taxation elements. Following the procedure of determining the public revenue collection procedure follows the public resources, and then the control procedure which is performed in a manner and according to the procedure prescribed by the law. Tax procedure initiated by the competent tax authority, ex officio, and exceptionally at the request of customers. Tax procedure is initiated when the tax authority taken any action for the purpose of the procedure. If the tax authority at the request of the party determines that there are no conditions for initiating tax proceedings, in accordance with the law, will bring about this conclusion.

## DEFINITION AND CHARACTERISTICS OF TAX-LEGAL RELATIONS

1. The activity of subjects, participants in the tax procedure, there is tax-legal their mutual relations. The tax-legal relation involves the relationship of public law in which enters the body in charge of conducting the tax proceedings and a natural or legal person in connection with the resolution of a tax matter. Accordingly, the parties in the tax compared to the body responsible for the conduct of tax procedure, on the one hand and the natural or legal person, on the other hand. The content consists of the tax-relations rights and obligations in the tax procedure mentioned parties governing:[2]

- the obligation to pay taxes, duties securing tax liability and obligation to pay secondary tax duties by a natural or legal person and the right of tax authorities to demand the fulfillment of these obligations;

- obligation of an individual or legal entity, in accordance with the law, establishes the tax, after deduction, collect taxes on behalf of the taxpayer, the later required by accounting, submit tax return to the tax authority of the requested documents and data, payments was not carried out on the way other than prescribed, allow inspection of its operations official of the tax authority and other statutory obligations of acts, omissions or suffering, in order to timely and proper payment of taxes, and the right of tax authorities to request the fulfillment of these obligations.

Taxation relationship has certain characteristics. Its legal properties and characteristics are:[3]subjects, the way of design, conditions of formation, rise and establishment of dispute settlement.

a) Entities tax legal relations are the competent authorities to conduct tax procedure and physical or legal persons. Thus, one side of this relationship must always be the authority responsible for the conduct of tax procedure.

b) Taxation ratio is not based on an agreement of entities to enter it, but on the basis of the unilateral stronger will the authority responsible for keeping a tax procedure, as a mandatory participant in all the tax legal relation. Strengthens the will of the tax authorities in this respect is manifested, and in making the tax administrative act at the request of an individual or legal entity, given that the tax authority in accordance with tax regulations independently

2 Član 10. stav 1. Zakona o poreskom postupku i poreskoj administraciji, ("Službeni glasnik RS", br. 80/2002, 84/2002 - ispr., 23/2003 - ispr., 70/2003, 55/2004, 61/2005, 85/2005 – dr.zakon, 62/2006 - dr.zakon, 63/2006 - ispr. dr.zakon, 61/2007, 20/2009, 72/2009 - dr.zakon, 53/2010, 101/2011, 2/2012 - ispr., 93/2012, 47/2013, 108/2013, 68/2014, 105/2014, 91/2015 – autentično tumačenje, 112/2015, 15/2016 i 108/2016) – u daljem tekstu ZPPPA.

3 G.Milošević, M.Kulić, Poresko pravo, Novi Sad, 2015, str. 151

decide whether the requirements taken into account, and if you take into account - in which scope will set the requirements to admit.

v) Formation of the tax-relations based on the act of the body responsible for maintaining a tax procedure does not depend on its discretion. The tax authority is required to base the tax legal relation *when performances of a particular facts* and conditions laid down regulations.

g) Taxation relationship is based *upon resolution of a tax matter*.

d) Disputes arising from the tax relations are decided in administrative-procedure, i.e. in an administrative dispute.

2. Taxation ratio has two components: 1) a material (material), and 2) process[4].

Property (material) component of the tax-legal relationship is also called *property tax relations*. This component consists of the rights and obligations of property nature, such as: the obligation to pay taxes, duties securing tax liability and obligation to pay secondary tax duties by a natural or legal person and the right of tax authorities to demand the fulfillment of these obligations. The subject of tax property relations is exactly where their rights and obligations directed, and it is the *obligation of giving*.

Processing component of the of tax property relationship represents the ratio of whose content make the rights and duties of the process nature. The rights and obligations are determined and based on standards that are used to resolve a tax matter. The subject of tax property relations is exactly where their rights and obligations directed. These are obligations of acts, omissions or suffering, which include: obligation of an individual or legal entity in accordance with the law determines taxes, i.e. after deduction to collect taxes on behalf of the taxpayer to keep proper accounts to file tax returns and to submit to the tax authority of the requested documents and information, the obligation not to perform payments in a manner other than specified to allow a review of its operations official of the tax authority and other statutory obligations of acts, omissions or suffering with the aim of timely and correct property taxes, and the right of tax authorities to request the fulfillment of these obligations.

Although the tax compared to the distinction of two components (and process material), this relationship represents a single unit. The uniqueness of the tax-legal relationship stems from the fact that all its institutions turn to one goal - to the payment of taxes.[5]

## DEFINITION AND CLASSIFICATION OF SUBJECTS IN THE TAX COMPARISON

The tax procedure, there are certain operators which share the task required to accomplish this operation, i.e. enlightenment and salvation tax matter. These entities are holders of certain rights and obligations of the fund, whose implementation achieves the task of tax procedure. Their activity is manifested in the form of various process actions.

Fund rights and obligations of individual participants in the tax procedure is not the same, and that is the reason their position in the tax procedure is different as well as their contribution to the solution of the tax stuff. In fact, there are entities who are holders of the basic activities in the tax procedure and without which the tax procedure cannot run or later have its course.

However, in addition to the basic activities of the holders of such activities, the tax procedure, there are other less important activities, to a greater or lesser extent contribute to the

4 G.Milošević, M. Kulić, navedeno delo, str.151.
5 D.Popović, Nauka o porezima i poresko pravo, Beograd, 1997, str. 20-21.

achievement of the basic objective of the task and the tax procedure. Holders of these activities are the operators whose role is secondary. These entities by participating in the tax procedure to help and contribute, first of all, determining the true facts in a tax matter. Starting from the participants' role in the tax procedure, they can be divided into:[6](1) main, or participants in the required tax procedure; (2) the specific participants, and 3) potential participants.

The principal or mandatory participants are holders of the basic activities in the tax procedure. As participants in the required tax procedure appear to be: (a) a tax authority, which is empowered to take tax procedure, and (b) a tax debtor - as a party on the occasion of the water tax procedure. Tax procedure is authorized to lead the Tax Administration and the competent authorities of local governments. There are times when you contribute to determine the organization for mandatory social insurance. When importing goods, value added tax and excise duty in the customs procedure calculated and collected by the Customs Administration. In addition to tax debtors involved in tax proceedings and their representatives, or proxies.

As a participant in the special tax procedure the attorney may appear because he his participation in the procedure that does not protect and does not exercise their rights or interests, but rather represents the overall interests. Thus, e.g., the public prosecutor may request the repetition of the tax procedure. As potential participants in the tax procedure may include: (1) witness; (2) and experts (3) is interpreted.

## THE COMPETENT AUTHORITIES FOR THE CONDUCT OF TAX PROCEDURE

According to the tax regulations, taxation procedure is authorized to water: 1) Tax Administration; 2) the competent authority of the local government, and 3) organizations for compulsory social insurance.

**Tax Administration**

The Tax Administration is an administrative body within the ministry in charge of finance.[7] Administrative authorities within the ministries are established for the performance of certain administrative tasks within the purview of ministries, when required by the nature and character of the work, or when these jobs require special organizational service, rationality and a certain extent of independence in the performance of duties. Tax Administration performs state administration relating to the conduct of the first instance tax procedure, the conduct of a single register of taxpayers and tax accounting, disclosure of tax crimes and offenses and their perpetrators, apply for recalculation of misdemeanor proceedings, as well as other duties specified by law.

Tax Administration performs state administration relating to the conduct[8] of the first instance tax procedure, the conduct of a single register of taxpayers and tax accounting, disclosure of tax crimes and offenses and their perpetrators, apply for recalculation of misdemeanor proceedings, as well as other duties specified by law.[9] Tax Administration independently per-

6 G.Milošević, M. Kulić, navedeno delo,str. 150.
7 Tax Administration headed by a Director. Directors appointed by the Government, at the proposal of the Minister of Finance. Director of the Tax Administration provides coordination of work and uniform application of tax regulations on the entire territory of Serbia, which is realized by the Minister acts (regulations, orders, directives, instructions mandatory) and immediate release of internal documents for operation (instructions, orders, instructions, etc.).
8 After the appeals against the first instance decision issued in tax proceedings, solves the appellate authority - the ministry responsible for finance.
9 Član 11. stav 1. ZPPPA.

forms activities within its jurisdiction in the entire territory of the Republic of Serbia and is organized so as to provide a functional unity in the implementation of tax legislation.

In order to ensure uniform application of regulations within the competence of the ministry responsible for finance acts (explanations, opinions, advice, instructions, etc.) On the implementation of these regulations by the Minister for Finance or a person authorized by him, are binding for the Treatment of Tax administration.[10]

Within its competence, the Tax Administration:[11]

- register taxpayers by assigning tax identification number and the unique register of taxpayers;

- keep registers in the exchange office operations in accordance with the regulations governing foreign exchange operations, as well as in the field of games of chance in accordance with the regulations governing games of chance;

- determination of tax is performed in accordance with the law;

- perform tax control in accordance with the law;

- perform regular and enforced collection of taxes and secondary tax duties;

- revealed tax crimes and their perpetrators and in this regard shall take measures prescribed by law;

- issue misdemeanor orders or competent misdemeanor court submits requests for initiating criminal proceedings for tax offenses, misdemeanors prescribed by the law governing the cash register, infringements in the area of the exchange office operations and other activities according to the law regulating foreign exchange operations, as well as violations of the games of happiness;

- ensure the implementation of international agreements on avoidance of double taxation;

- develop and maintain the unique tax information system;

- maintain tax accounting;

- planned and implemented training for employees;

- supervise the implementation of laws and other regulations by its organizational units and executed by the control measures undertaken in accordance with the law regulating the general administrative procedure;

- performs internal control of behavior and tax officials and the employees in connection with the work and in cases where it is determined unlawful conduct or behavior initiated and conducted by appropriate procedures in order to determine responsibilities;

- perform an internal audit of all organizational units of the Tax Administration in accordance with the law and international standards of internal audit in the public sector;

- provides technical assistance to taxpayers in application of tax regulations for taxes that identifies, controls and costs, in accordance with the code of conduct for employees of the Tax Administration;

- provides a release of the paper;

- issue and revoke authorization for exchange operations;

- organizing training and issue certificates for exchange operations;

10 Član 11.stav 3. ZPPPA.
11 Član 160, stav 1 ZPPPA.

- controls the planetary gear and foreign exchange operations, in accordance with the regulations governing foreign exchange operations, as well as control of foreign trade and prevention of money laundering and financing of terrorism, in accordance with the law;

- performs state administration in the field of gambling, in accordance with the regulations;

- Perform other duties in accordance with law;

- perform other tasks on the basis of contracts concluded for a fee, in accordance with the law.

To carry out the responsibilities of the Tax Administration shall be established an organizational unit. Method of education, number, structure, network and scope of organizational units shall be determined by an act of the Minister of Finance, at the proposal of the Director of Tax Administration. Certain operations of the Tax Administration may be performed outside the seat of the organizational unit, which is decided by the Tax Administration. To perform operations on the detection and reporting of tax crimes and their perpetrators shall establish the Tax Police, as a separate organizational unit of the Tax Administration. Tax police plan, organize and execute the tasks in accordance with the law. Tax police by chief inspector of the Tax Police who, on the proposal of the minister appointed by the Government.[12]

**The competent authority of local governments**

Budget funds local government units shall be provided from the source and shared revenues, transfers, income in respect of borrowing and other revenues and income established by law.[13] ULG belonging to the original revenue generated on its territory, as follows:[14]

property taxes, excluding taxes on transfer of absolute rights and taxes on inheritance and gifts;

- local administrative fees;

- local utility taxes;

- local taxes;

- fees for use of public goods, in accordance with the law;

- concession fees;

- other charges in accordance with law;

- revenues from fines imposed in misdemeanor proceedings for misdemeanors prescribed by an act of the assembly of the local government, and seized assets in this process;

- income from leasing or the use of real estate and movable property owned by the Republic of Serbia, used by local governments or authorities and organizations of the local government unit and indirect beneficiaries of its budget;

- income from leasing or the use of real estate and movable property owned by local governments;

12 Tax Police inspector shall have an official badge and identification card of authorized official. Tax police inspector in performing must have an official badge and identification card. Act of the official identity card Tax Police inspectors, tax inspectors and tax executors, as well as the official badge of tax police inspector by the Minister for Finance. Tax Police inspector must have protective clothing with labels Tax Police whose appearance and cases in which the benefits prescribed by the Minister.

13 Član 5. Zakona o finansiranju lokalne samouprave ("Sl Glasnik RS", br. 62/2006, 47/2011, 93/2012, 99/2013 – usklađeni din. iznos, 125/2014 - usklađeni din. iznos, 95/2015 - usklađeni din. Iznos, 83/2016, 91/2016 - usklađeni din. iznos и 104/2016 – dr.zakon).

14 Član 6. Zakona o finansiranju lokalne samouprave ("S: Glasnik RS", br. 62/2006, 47/2011, 93/2012, 99/2013 – usklađeni din.iznos, 125/2014 - usklađeni din.iznos, 95/2015 - usklađeni din. iznos, 83/2016, 91/2016 - usklađeni din.iznos, i 104/2016 – dr ).

- Revenues from sale of services users of the budget of the local government which is contracted to provide natural and legal persons;
- interest income on funds from the budget of the local government;
- income from donations to the local authority;
- revenues on the basis of voluntary.

The competent local government authority in the determination, control and billing of taxes and tax administration, as well as the code of the request for initiation of offense procedure for tax violations, treated in accordance with the tax procedures and tax administration. This law applies to original public revenues of local governments that these units are determined, collected and controlled by the public law relationship, as well as the secondary tax duties on these grounds, in proceedings in which returns tax administrative acts, including acts in administrative proceedings, for which the prescribed application of this law.[15]

**The organization for mandatory social insurance**

The organization of mandatory social insurance contributions determines obligation for persons who were involved in compulsory social insurance. A person included in the mandatory insurance is a natural person to its request included in compulsory social insurance in accordance with the law. In addition, the organization for mandatory social security lays down the obligation to pay contributions and when determined by the status of the insured, because the insurance application was not filed on time, or for other reasons, in accordance with the law.[16]

## ROLE OF CUSTOMS ADMINISTRATION IN THE METHOD OF DETERMINING THE BILLING AND VALUE ADDED TAX EXCISE AND AT IMPORTATION

Customs Administration, and Tax Administration, a body within the ministry is responsible for finance. Its main task is the implementation of customs regulations. However, it is in some cases tax regulations authorized to impose and collect the tax. Thus, the Law on Value Added Tax stipulates that for the calculation and payment of value added tax on importation of goods by the customs authority competent to conduct the customs procedure, unless the law provides otherwise.[17]

In addition, the Law on Excise is determined that the excise tax on import of excise goods is calculated by competent customs autory.[18]

---

15 Član 2a ZPPPA.

16 Članovi 61-63. Zakona o doprinosima za obavezno socijalno osiguranje («Sl.Glasnik RS», br. 84/2004, 61/2005, 62/2006, 5/2009, 52/2011, 101/2011, 7/2012 – usklađeni din.izn., 8/2013 - usklađeni din.izn., 47/2013, 108/2013, 6/2014 - usklađeni din.izn., 57/2014, 68/2014 – dr.zakon, 5/2015 - usklađeni din. izn., 112/2015, 5/2016 - usklađeni din.izn., и 7/2017 - usklađeni din.izn.)

17 Član 59. Zakona o porezu na dodatu vrednost ("Sl.Glasnik RS", бр. 84/2004, 86/2004 - испр., 61/2005, 61/2007, 93/2012, 108/2013, 6/2014 - usklađeni din.izn., 68/2014 - др. закон, 142/2014, 5/2015 - usklađeni din.izn., 83/2015, 5/2016 - usklađeni din.izn., 108/2016 и 7/2017 - usklađeni din.izn.) – у даљем тексту ПДВ.

18 Član 21a. stav 2. Zakona o akcizama ("Sl.Glasnik RS ", бр. 22/2001, 73/2001, 80/2002, 43/2003, 72/2003, 43/2004, 55/2004, 135/2004, 46/2005, 101/2005 - dr.zakon, 61/2007, 5/2009, 31/2009, 101/2010, 43/2011, 101/2011, 6/2012 - usklađeni din.izn., 43/2012 - odluka, 76/2012 - odluka, 93/2012, 119/2012, 8/2013 - usklađeni din.izn., 47/2013, 4/2014 - usklađeni din.izn., 68/2014 - dr.zakon, 142/2014, 4/2015 - usklađeni din.izn., 5/2015 - usklađeni din.izn., 55/2015, 103/2015, 5/2016 - usklađeni din.izn., 108/2016 и 7/2017 - usklađeni din.izn.)

# TAXPAYERS AND OTHER TAX DEBTORS

Versus the authority responsible for keeping a tax procedure, as the other side in the tax compared, there is a tax debtor. The tax debtor is a natural or legal person who is required to perform a specific action from the tax legal relations. Viewed from a process aspect, the tax debtor party is in the tax procedure, it is a natural or legal person on whose request or upon whom the tax procedure originated. In this capacity, the tax debtor is the holder of certain rights and obligations. These rights and obligations may be non property and property rights (procedural) nature.

In order for a natural or legal person may be a tax debtor, it must have the ability Taxation, as a special form of legal capacity. This ability to have those natural and legal persons who are eligible to assume the rights and obligations established by the regulations.[19]

a) Taxation ability to have all individuals, regardless of gender, age, mental state, physical health and other characteristics. For individuals there is no difference between the tax legal and civil capacity. This ability of individuals are acquired by birth. In some cases, the tax legal capacity may have conceived a child. Thus, in the event that the tax debtor dies before he can determine tax obligations, the obligations exceed its successors, and therefore the child who was born after his father's death. Tax legal capacity of a natural person ceases his death or declaration of the deceased.

b) A legal entity is the holder of certain rights and obligations. Legal sphere of a legal entity separate from the legal sphere of its founders and participants. In other words, the legal entity is a separate legal entity in relation to its founders, who have their own legal personality. Taking into consideration this rule there are some exceptions. Thus, for the obligations of certain types of legal entities (limited partnerships, cooperatives, limited partnerships, etc.) do not correspond to only those persons of their property but also the participants of its assets. And with the joint stock partnerships and responsibility can be transferred to the property of the founders, when they process their deliberate harm the interests of the company's creditors. In this case, it can be applied institute legal personality punching.

Tax debtors include: (1) a taxpayer; (2) a tax guarantor; (3) a tax payer; (4) the tax intermediary and (5) other tax debtors.[20]

**Tax payer**

The taxpayer is a tax debtor who is obliged to pay the tax or secondary tax duties. With regard to the legal obligation of the taxpayer to pay the tax, he is considered a major tax debtor. The taxpayer also referred to as a tax entity.[21] However, this is not an active subject, but a passive entity. Tourist tax entity is the state that has the right to impose and collect taxes. To avoid the use of active and passive tax subject, adopted the term taxpayer for passive tax subject. Taxpayers may participate in the tax legal relationship through their proxy or legal representative.[22]

Tax representative is a natural or legal person - resident of the Republic in which the granted power of attorney in the name and for the account of the taxpayer carries out tasks related to the taxpayer's tax liabilities (receiving tax documents, submit tax returns, pay taxes, etc.).[23]

19 G.Milošević, M. Kulić, *navedeno delo*, str. 160.
20 Član 12 ZPPPA.
21 The tax laws and literature expresses the taxpayer and the tax debtor are often used interchangeably.
22 A.Perić, *Finansijska teorija i politika,* Beograd, 1971, str. 184.
23 A non-resident of the Republic who has no permanent establishment in the Republic, or who gains income or property in the territory of the Republic of van operations of its permanent establishment shall, within ten days from the date of earning income, or acquisition of property subject to taxation in

Legal representatives of individuals (the parents of a minor, a guardian incapacitated ward, etc.), Legal entities (natural person who is registered as such in the prescribed register), as well as foremen and entrepreneurs temporary guardian legacy, fulfilling tax obligations of the persons they represent. If the taxpayer is an individual who is not competent, but has no legal representative, the tax authority shall appoint a representative ex officio shall immediately inform the guardianship authority. In addition, the tax authority, ex officio, of the order of tax advisers[24] or lawyer asks MPs[25].

- taxpayer whose seat is not in place at the address given in the application for registration or evidencing a VAT, which is governed by the regulations on Value Added Tax;
- a non-resident who has not informed the tax authority of his tax representative;
- unknown owner of the property subject to the tax procedure;
- taxpayer who obviously avoiding to participate in the tax procedure, if his participation is mandatory.

**Tax guarantor**

A tax guarantor is a person who is responsible for paying the taxpayer's tax debt in the event that the taxpayer does not pay the debt on time. Responsibility for the tax liability of another person may occur on a legal or on an optional basis.

The statutory tax guarantee may result from the tax laws that have character, but can be arranged and tax laws.

Cases regulation of liability for the tax liability of another person can be found in the *Law on Companies*. So in this law stipulates that the partners of a partnership are jointly and severally liable with all its assets for the liabilities of the company.[26]

For the obligations of the limited partnership jointly and severally liable general partner and limited partner is liable to the limited amount of their unpaid or not fed stake role.[27] There should also be the responsibility related to the so-called. *piercing the corporate veil*. The limited partner, member of a limited liability company and a shareholder, as well as the legal representative of that person if it is incapable of operating a natural person who abuses the rule of limited liability for the liabilities of the company.[28] Entrepreneur for all liabilities incurred in connection with the performance of its activities liable with all its assets and the assets that enters and assets acquired in connection with the performance of activities. This responsibility does not stop entrepreneur's deletion from the register.[29] When the status changes - the acquiring company becomes jointly and severally liable with the company narrators of his obligations which are not transferred to the acquiring company but only to the extent of the difference value of assets of the company transferee that he was transferred and liabilities of the transferor which is assumed unless a specific creditor differently agreed. Limited partners, members of limited liability companies and joint stock company jointly and severally liable for the obligations of the company in liquidation even after the deletion from the register of economic subjects, up to the amount received from liquidation.[30] Limited partners, members of limited liability companies and joint stock company jointly and severally liable for the ob-

the Republic inform the tax authority at the seat of the person who is its tax representative.
24 The tax adviser is a person who performs tax consulting taxpayer in the tax procedure.
25 Conclusion on the appointment of members ex officio is delivered to the agent and on the notice board of the tax authority.
26 Član 93. stav 1. zakona o privrednim društvima («S.Glasnik RS», br. 36/2011, 99/2011, 83/2014 – dr.zakon i 5/2015)
27 Član 125. Zakona o privrednim društvima.
28 Član 18. stav 1. Zakona o privrednim društvima.
29 Član 85. Zakona o privrednim društvima.
30 Član 505. stav 1. tačka 2. Zakona o privrednim društvima.

ligations of the company in liquidation even after the deletion from the register of economic subjects, up to the amount received from liquidation.[31]

Control member of a limited liability company and controlling shareholder of the joint stock company jointly and severally liable for the obligations of the company and after the deletion of the company from the register.[32]

The *tax laws* of Serbia envisage several cases bail. Thus, the Law on Personal Income Tax Law stipulates that the payment of withholding tax payer jointly and severally guaranteed income, and that the payment of tax on income from self-employment guarantee subsidiary of its assets all adult members of the household taxpayers who at the time when the liability consists of household taxpayers.[33] The Law on Property Taxes stipulates that the person to whom it is transferred to the absolute right or donor, subsidiary guarantees for the payment of tax on transfer of absolute rights, i.e. to pay gift tax.[34]

The Law on Property Taxes provided the guarantee on an optional basis. It is stipulated that the person to whom it is transferred to the absolute right or the donor, who is contracted to pay tax on transfer of absolute rights and gift tax, guaranteed jointly and severally to pay this tax.[35]

**The tax payer**

The tax payer is the payer of income to the taxpayer who is required to calculate and pay the prescribed withholding tax on that income, in the name and for the account of the taxpayer, to the appropriate account. It may be that the employer pays earnings, the bank that pays interest, a joint stock company paying the dividends and the like. The tax payer guarantees for the payment of taxes that are calculated after deduction.

**Tax broker**

Tax broker is a person who is liable to the account of the taxpayer (taxpayer or the tax payer) on the basis of their orders for the transfer of funds to the suspension and withholding payment of the tax, on its own behalf and on behalf of the taxpayer or the tax payer, as appropriate payment account.

**Other tax debtors**

In other tax debtors include natural and legal persons required to perform an action from the tax legal relations, and not the taxpayer, tax payer, tax representative or tax guarantor.[36]

## INSTEAD OF A CONCLUSION

Tax procedure represents the activity of taxation authorities and the taxation debtor, which is necessary in each tax legal relation, to determine the existence of tax obligations and estimated, both objective and subjective elements legal description of the tax facts. Essentially

31 Član 545. stav 2. Zakon o privrednim društvima.
32 Član 548. stav 4. Zakona o privrednim društvima.
33 Član 548. stav 4. Zakona o privrednim društvima
34 Član 157. st. 1. i 2. Zakona ("Sl.Glasnik RS", br. 24/2001, 80/2002, 80/2002 - dr. zakon, 135/2004, 62/2006, 65/2006 - isp., 31/2009, 44/2009, 18/2010, 50/2011, 91/2011 - odluka US, 7/2012 – usklađeni din. izn., 93/2012, 114/2012 – odluka US, 8/2013 - usklađeni din. izn., 47/2013, 48/2013 - isp., 108/2013, 6/2014 - usklađeni din. izn, 57/2014, 68/2014 – dr.zakon, 5/2015 - usklađeni din. izn., 112/2015, 5/2016 - usklađeni din. izn. i 7/2017 - usklađeni din. izn.)
35 Član 42. stav 1. Zakona o porezima na imovinu ("Sl.Glasnik RS"br. 26/2001, "Sl.Glasnik RS" бр. 42/2002 – odluka SUS i ("Sl.Glasnik RS" br. 80/2002, 80/2002 – dr.zakon, 135/2004, 61/2007, 5/2009, 101/2010, 24/2011, 78/2011, 57/2012 – odluka US 47/2013 i 68/2014 – dr.zakon)
36 Član 42. stav 2. Zakona o porezima na imovinu.

the tax procedure involves several interconnected and conditioned actions: determination, collection and control of public revenue. In Serbia, the control of taxpayers, assessment and collection of public revenues by the tax administration. Billing and identification of customs duties carried out by the Customs Administration. Certain forms of public revenues, in accordance with tax regulations are the responsibility of local authorities. The organization of mandatory social insurance contributions determines obligation for persons who were involved in compulsory social insurance.

In addition to the tax legal relation of the tax authority involved and the tax debtor. Tax debtor party is in the tax procedure, or a natural or legal person, by whose request originated, or who is subject to tax procedure, i.e. it is the face which is due to a specific action from the tax relations. The tax debtors include: taxpayer, tax guarantor, the tax payer, the tax intermediary and other tax debtors.

## LITERATURE

1. Милошевић Г., Утврђивање јавних прихода, С. Паланка, 2002.
2. Милошевић Г., Кулић М.,, Пореско право, Нови Сад, 2015.
3. Перић А., Финансијска теорија и политика, Београд, 1971
4. Поповић Д., Наука о порезима и пореско право, Београд, 1997.
5. Закон о пореском поступку и пореској администрацији, ("Службени гласник РС", бр. 80/2002, 84/2002 - испр., 23/2003 - испр., 70/2003, 55/2004, 61/2005, 85/2005 –др. закон, 62/2006 - др. закон, 63/2006 - испр. др. закон, 61/2007, 20/2009, 72/2009 - др. закон, 53/2010, 101/2011, 2/2012 - испр., 93/2012, 47/2013, 108/2013, 68/2014, 105/2014, 91/2015 –аутентично тумачење, 112/2015, 15/2016 і 108/2016).
6. Закон о финансирању локалне самоуправе ("Сл. гласник РС", бр. 62/2006, 47/2011, 93/2012, 99/2013 - усклађени дин. изн., 125/2014 - усклађени дин. изн., 95/2015 - усклађени дин. изн., 83/2016, 91/2016 - усклађени дин. изн. и 104/2016 - др. закон).
7. Закон о доприносима за обавезно социјално осигурање ("Сл. гласник РС", бр. 84/2004, 61/2005, 62/2006, 5/2009, 52/2011, 101/2011, 7/2012 - усклађени дин. изн., 8/2013 - усклађени дин. изн., 47/2013, 108/2013, 6/2014 - усклађени дин. изн., 57/2014, 68/2014 - др. закон, 5/2015 - усклађени дин. изн., 112/2015, 5/2016 - усклађени дин. изн. и 7/2017 - усклађени дин. изн.).
8. Закон о порезу на додату вредност ("Сл. гласник РС", бр. 84/2004, 86/2004 - испр., 61/2005, 61/2007, 93/2012, 108/2013, 6/2014 - усклађени дин. изн., 68/2014 - др. закон, 142/2014, 5/2015 - усклађени дин. изн., 83/2015, 5/2016 - усклађени дин. изн., 108/2016 и 7/2017 - усклађени дин. изн.) – у даљем тексту ПДВ.
9. Закон о акцизама ("Сл. гласник РС", бр. 22/2001, 73/2001, 80/2002, 43/2003, 72/2003, 43/2004, 55/2004, 135/2004, 46/2005, 101/2005 - др. закон, 61/2007, 5/2009, 31/2009, 101/2010, 43/2011, 101/2011, 6/2012 - усклађени дин. изн., 43/2012 - одлука, 76/2012 - одлука, 93/2012, 119/2012, 8/2013 - усклађени дин. изн., 47/2013, 4/2014 - усклађени дин. изн., 68/2014 - др. закон, 142/2014, 4/2015 - усклађени дин. изн., 5/2015 - усклађени дин. изн., 55/2015, 103/2015, 5/2016 - усклађени дин. изн., 108/2016 и 7/2017 - усклађени дин. изн.).
10. Закон о привредним друштвима ("Сл. гласник РС", бр. 36/2011, 99/2011, 83/2014 - др. закон и 5/2015).

11. Закон о порезу на доходак грађана ("Сл. гласник РС", бр. 24/2001, 80/2002, 80/2002 - др. закон, 135/2004, 62/2006, 65/2006 - испр., 31/2009, 44/2009, 18/2010, 50/2011, 91/2011 - одлука УС, 7/2012 - усклађени дин. изн., 93/2012, 114/2012 - одлука УС, 8/2013 - усклађени дин. изн., 47/2013, 48/2013 - испр., 108/2013, 6/2014 - усклађени дин. изн., 57/2014, 68/2014 - др. закон, 5/2015 - усклађени дин. изн., 112/2015, 5/2016 - усклађени дин. изн. и 7/2017 - усклађени дин. изн.).
12. Закон о порезима на имовину ("Сл. гласник РС", бр. 26/2001, "Сл. лист СРЈ", бр. 42/2002 - одлука СУС и "Сл. гласник РС", бр. 80/2002, 80/2002 - др. закон, 135/2004, 61/2007, 5/2009, 101/2010, 24/2011, 78/2011, 57/2012 - одлука УС, 47/2013 и 68/2014 - др. закон).

# APPLICATION OF GEOINFORMATION TECHNOLOGIES AND GEOGRAPHIC METHODS IN ASSESSING THE VULNERABILITY OF POTENTIAL TERRORIST TARGETS IN THE LOCAL COMMUNITY

**Slobodan Miladinovic, PhD**

*Academy of Criminalisticand Police Studies, Belgrade*

Abstract: Basic security holder in the local community is the police or police administration. It needs to recognize and analyze security problems in the city and approach certain risks opting for the most efficient way. One form of threat to security is terrorism.In the context of countering contemporary forms of terrorism, so far, the police have mainly focused on seeking answers where and when there are opportunities for terrorist attacks in order to find preventive solutions to neutralize these attacks. By applying extensive experience, police officers have recognized the connection between the dynamics of terrorist activity and geographical space.Linking occurrences with a specific location is an effective means of recording, compiling, analyzing and reporting a large amount of data on terror and other security phenomena. The paper presents spatial identification of the aims of terrorist attacks and the determination of priorities in their protection by separation and mapping of characteristic areas.The aim of this technique is not to predict which individual target is most vulnerable or when a specific target is to be attacked, but to map the result of risk analysis in a particular geospatial area, based on the assessment of the vulnerability of potentially endangered targets in the local community.The focus of protection is strategy rather than tactics. Geographic method uses valuation techniques and cartographic visualization of relationships and characteristics of geographical objects, which could be a potential target for terrorists such as the building of local government, schools, commercial buildings, railways, transit city roads, parks, tourist facilities, etc. The paper will show a case study of the city of Smederevo with several types of geospatial entities that could be potential targets of terrorists.

**Keywords:** geographic method, geographic objects, terrorism, GIS.

## INTRODUCTION

Nowadays terrorism is a global problem and one of the biggest threats to modern security. The main feature of today's form of terrorism is its unexpectedness. Time and manner of attack are unpredictable, and goals often unclear, which makes it difficult to effectively prevent terrorist attacks[1]. The causes of terrorism may be different: nationalism, great social and economic differences within states, ethnic problems, poverty, and so on. Ideologically, modern terrorism is rich with teachings of religious fundamentalists and is characterized by misuse of religious concepts[2].

1 M. Mladenovic*Terrorist attack as the cause of emergencies,* Proceedings Crisis and emergency management –Theory and Practice, Belgrade, 2015, p 75.

2 M. Šipkar*Police cooperation with the local community for the purpose of preventing the criminal offense of Terrorism* Police Security Zagreb, 2015, year 24, number 3, pp. 292–298.

In order to anticipate and prevent a terrorist attack in any way, one has to take into account the wide range of terrorist opportunities and to make a detailed plan of prevention and response. The basic task of all security actors is to protect the vital values of a society, which includes the protection of human life and health, the protection of natural and material assets and the protection of the state and society infrastructure. These are in fact all activities that endanger these values, impair the normal functioning of services and businesses and pose a threat to the stability of local, national and global development. Terrorists always choose the most vulnerable targets for their targets, such as innocent people, and always tend to cause fear among the people, thus exerting pressure on the authorities of the specific country.Terrorists also strive for media spectacularity, which is why they often choose places where there is a high concentration of people for their target. The most vulnerable objects from the aspect of terrorist attacks can be determined on the basis of several criteria: number of people, accessibility, criticality from the aspect of everyday life, economic significance, symbolic value.On the basis of these criteria, most objects that are most vulnerable to potential terrorist attacks can be identified. Among these facilities are: transport infrastructure, waterways, airports, railways, subway stations, government institutions, recreation centers, historical buildings, military facilities, computer systems, nuclear facilities, etc.[3]Although terrorism is a risk with major consequences, due to less probability of occurrence, the risk of a terrorist attack is often ignored, which is a wrong approach.

Effective functioning of the security system depends on the quality and timely decision making. The basic prerequisite for making a quality decision is the availability of reliable information about the problem that is the subject of decision making. The development of information and communication technology provides a large amount of information needed for decision making.Police daily encounters a large number of collected data to be reviewed, systematized, classified, processed and analyzed. The Geographic Information System (GIS) can greatly assist the police in making decisions in the execution of strategic, tactical and operational security tasks.Over the past two decades, the development of GIS as one of the information technologies, has greatly contributed to the resolution of numerous geospatial problems. Today conventional GIS is complemented by the so-called Geospatial analysis (extensions) in which a combination of data from different sources creates an interactive environment that allows individuals from different occupations to simultaneously input a variety of data.Such geospatial data allow the extraction of a large number of information whose structure, scope and dynamics are viewed by analysts from the aspect of endangering certain objects and areas of security events. By entering these data in the map, there is an opportunity to predict and direct police forces to preventive and proactive activities because almost everything the police do is related to the location or address.

The paper deals with the possibility of applying GIS to map areas in a local community that is estimated to be exposed to a greater or lesser potential threat of terrorist attacks. Ron Clark and Graeme Newman (2006), experts in the field of situational crime prevention, in the "Outsmarting the Terrorists" section, provide concrete ways in which local police can use activities and experiences in the analysis of terrorism and mapping the places of execution of terrorist acts, that is, understanding terrorism, risk assessment and prevention.This paper uses the criteria developed by Clark and Newman (2006) to assess the vulnerability of the target, along with the current possibilities of mapping the crime scene within local communities based on target vulnerability to terrorism.A case study of the city of Smederevo was applied in order to assist competent police officers and security analysts in improving anti-terrorist efforts at the local level. In general, this technique can use GIS, geographic data, local experiences for vulnerable targets for the purpose of creating a thematic map with segregated areas

3 M. Mladenović, p.77.

in a particular community that potentially represent high and low risk areas for terrorism. What's important is that this technique can be implemented by a local police analyst with geographic data and software[4]. The aim of this technique is not to predict which individual target is most vulnerable or when a specific target will be attacked but to present the results of a risk analysis of a particular area that contains multiple objectives of a particular community, which means focusing on strategy, not on tactics.In the case study, the author did not use a map in the GIS environment because a police administration in Smederevo does not have such software. A digital orthophoto map was used, the Republic Geodetic Authority. The intention is for police officers to get acquainted with one of the modern techniques which isused in countering terrorism in developed countries.The separation of surfaces is based on their importance for the city of Smederevo in public, economic and cultural terms. The author presented the vulnerability assessment on the basis of the available data and personal knowledge of the listed entities. Such a model can be applied to larger urban environments such as local units that have city status.

## ASSESSMENT OF VULNERABILITY AND EVALUATION OF POTENTIAL TERRORIST TARGETS

If one wants to prevent terrorist attacks, one needs to understand the motives and way of acting of terrorists, that is, their way of selecting, preparing, organizing and carrying out attacks, as well as the activities that they carry out after the terrorist act is executed. In order to do this, one needs to "think as a terrorist", which means, one needs to know their method of planning and the tactics of acting in the conduct of a terrorist attack.It is necessary to do this separately for each type of attack, because differences in terms of specificity must be taken into account. Security experts cannot be guided by the fact that terrorists are merciless fanatics that are hard to stop, nor that they are all extremely intelligent people who plan every detail.Terrorists cannot achieve all planned goals at every opportunity; they often have to do what is feasible with regard to the opportunities and resources available to them at a specific time and place. They continuously measure the balance between achieving one or more of their goals against possibilities and available resources.Terrorists can take advantage of the benefits of various technologies and systems. They also work on ideological, professional, moral, voluntary, psychophysical, and other forms of training and improvement. When deciding what types of terrorist attacks will be planned, a terrorist must take into account three main elements[5]. The first element is the decision on the scope of the mission. Which of the objectives will be fulfilled? The second is the complexity of the mission. Will the complexity of the set goal require a lot of training, money, members, and so on? The third element is the decision on the type of goal, whether they are certain individuals or objects that people inhabit.Planning the way to goals and choosing goals become crucial to the implementation of a terrorist act. In addition, terrorists must create a way to choose goals and ways that will not become predictable. Assessing potential targets and protecting them even in cases where terrorist acts cannot be stopped, influences their effects to become extremely mild.For example, setting up a vehicle as a barrier around the US embassies forced terrorists to leave the cars they used during the bombing[6]. Protecting potential targets, directs terrorists to move to a less attractive location with less impressive results. By protecting potential targets, Israel

4 Boba, R., *Crime Analysis and Crime Mapping*. Thousand Oaks, CA: Sage Publications, Inc., 2008,p. 144.
5 Clarke, R. V. and Newman, G. Clarke, R. V. and Newman, G. *Outsmarting the Terrorists*. Portsmouth, NH: Greenwood Publishing Group, 2006,p. 19.
6 Clarke, R. V. and Newman, G., p.26.

and Northern Ireland have built different barriers that have made it difficult for terrorists to choose the goals that are available and plan the way to the goal[7]. There are numerous examples of concrete attacks that will be neutralized in the near future by the introduction of protective prevention, such as abductions of regular-line aircraft that were largely eliminated during the 1980s by a series of security measures introduced by state and air transport companies[8].

Clarke and Newman[9]analyze four basic elements of terrorist attacks (aim, tool, weapons and security conditions).The mentioned authors believe that the separated elements of terrorist attacks should be understood in order to understand the risk and develop a prevention program. Namely, the authors argue that local security authorities "must identify vulnerable goals, analyze their specific weaknesses, set priorities for protection and provide protection that corresponds to the level of identified risk".The mentioned authors believe that the separated elements of terrorist attacks should be understood in order to understand the risk and develop a prevention program. Namely, the authors argue that local security authorities "must identify vulnerable goals, analyze their specific weaknesses, set priorities for protection and provide protection that corresponds to the level of identified risk".Analysis of terrorist attacks and mapping of endangered targets can help to neutralize almost all elements of terrorist attacks. However, the work focuses on one of the stated goals, assessing the weaknesses of the chosen objectives, applying and using data available to most security services.The synthesis of the technique used by GIS, geographic data, local police experience and the criteria defined by Clarke and Newman (2006) determine vulnerable targets in the form of marked areas on the map of local communities pointing to high and low areas of risk for terrorism. In mapping targets, security analysts and local police should assess why certain targets are more attractive to terrorists than others, and it is necessary to put themselves in the role of terrorists in order to understand their decisions. In order to facilitate making decisions for the police, Clarke and Newman[10]have established a way to evaluate potential terrorist targets in any community. The authors have developed the following criteria for goals such as: exposed, significant, primal, legitimate, destructive, settled, close and easily accessible.

The above criteria are general and can be applied in different environments from large cities to rural communities. Geographic objects that are considered vulnerable and can be a potential target of terrorist attacks by Ronczkowski[11]are: nuclear power plants, airports, railways, city transport lines, amusement parks, shopping centers, landmarks, research laboratories, dams, refineries, ports, government buildings, highways, rivers, residential zones with high population density and main urban infrastructure.

The application of this technique involves reliance on two components. The first component is the selection of an area considered to be endangered, based on the location of the target or type of target. Instead of looking at each target individually, as it is for tactical analysis, the assessment is targeted at all targets in a predetermined area. Endangered goals and their weaknesses are analyzed together, based on which, the area of priority protection and strategic prevention activities in certain parts of the local community is determined. GIS software allows analysts to select a particular area through several different methods.

- *Intersection method:* allows analysts to choose the area based on whether at any moment of the threat, the area is crossed or there is a crossing of an individual target or target type in that area.

7 Clarke, R. V. and Newman, G. p.27.
8 Clarke, R. V. and Newman, G. p.29.
9 Clarke, R. V. and Newman, G. p.4.
10 Boba, R.p.144.
11 Ronczkowski, R. *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis,and Investigations.* Boca Raton, FL: CRC press2004, p. 72.

- *Distance method:* directs the security service to select the area of vulnerability based on the proximity of a target or a specific target type.

- *Complete method:* it helps analysts map the selected area based on whether the target is completely within the boundaries of the area.

- *The method of presence of any part:* determines the area when any part of the aimed target is in the area, which is useful when the target is larger than the area.

The second component of the technique is to assign the results to the selected area based on the degree of vulnerability of specific targets or the type of target. A scheme of damage that can occur in each area is created, which gives the categorization of the selected area based on the nature of the objectives of the area.Each of the eight aforementioned criteria for evaluating goals can be assigned a score of 1, which means that each target can be scored according to which value it has on the scale from 0 to 8.Scores of target targets or target types should depend on the assessment of analysts and their experience in the field of terrorism and the vulnerability of targets. Analysis can be more complicated, giving weight to each of the components from the damage caused to the schemes, instead of giving equal importance.For example, if a target is considered significant, a value of 2 can be assigned, while easily accessible or accessible targets can have a value of 1. Since many goals are easy, this criterion is less important.The numerical values of the objectives are determined by experts with experience in this field. The results of combining two components, techniques and types of targets are presented as layers in GIS. The scoring of the individual layer is separated, and the overlapping of the layers gives the accumulated value for each area, in order to score separately, but also to summarize for each area.The cumulative rate for each area based on the score will be topically shaded and will vary in relation to other areas. Thematic classification and gradation will depend on the needs of analysis, the nature of the data and should be determined by analysts. The result will be the thematic shading of the area. Darker shading involves greater risk. This technique and its components are shown in the next simulated case study.

## ESTIMATION OF VULNERABILITY OF POTENTIAL TARGETS IN SMEDEREVO

The strategic and geographic traffic position of Smederevo makes it, to a certain extent, a potential target of terrorist attacks. Smederevo is a regional center located at the point of connecting two European corridors, Danube and Moravia (land corridor X and river corridor VII). In Smederevo is the northernmost port which can host the Black Sea ships. Downstream of the city there is Kovinbridge, the last link with the left bank of the Danube to the Djerdap gorge.Smederevo is a true northern origin of the Moravian – Vardar valley and the route along its route. The city has realistic opportunities to establish the function of alternatives and intermediaries between the eastern Panonian (Banat) and the Western Carpathian region on one side and the Pomoravlje Corridor that connects the south (Skopje, Thessaloniki, Athens) and the south-eastern Balkans (Sofia, Istanbul) on the other side. Therefore, it is possible to find it on the path of modern migrant currents, or the main axis of their movement. The transit city of Smederevo on the Danube is also endangered by potential terrorist attacks. The significance of this great European river, developed international traffic on it, the direction of the flow, the heterogeneity of the regions and the countries through which it flows (the center of the European Union in the Northwest and the wider Black Sea coastal zones in the southeast) are pointing to caution.


*Figure 1 Geographic objects in Smederevo that can be potential targets of terrorists*

Extract of digital orthophoto map 1:25 000, Republic Geodetic Authority, Belgrade

Figure 1 shows the digital orthophoto map of Smederevo with several types of geographic characteristics and objects that could be potential targets of terrorists. Due to its simplicity, we have selected the Danube coast, the railway line, the industrial zone, the fortress, the police and the municipal administration, the zones of parks and schools.Analysis of objectives and specific geographical object on the basis of which areaswill be extracted and evaluated will depend on the available data and estimates. What follows are maps that show different ways of selecting predefined fields within the GIS and the results obtained in accordance with the criterion of potential damage.Each component of the specified criterion is evaluated as 1, and the result is estimated based on the general characteristics of the target and its significance. In practice, the assessment is based on location and specific nature of the target in the selected community.


*Figure 2. The Danube coast, the railway zone and the industrial zone*

Figure 2 shows the Danube function with the selected zones through which it flows, or "cuts" it. The result for these zones is 4, and it is based on the fact that rivers are generally exposed, legitimate, close (in this case) and easily accessible, but not necessarily of vital importance, important, destructive or inhabited. The Danube coast in Smederevo is divided into an area in the narrower city area consisting of an old dock, a marina, a zone of a fortress, a zone from a fortress to a rowing club and a zone from a rowing club to an old ironworks and an industrial zone. In the narrower city area, the coastline extends to a length of 2300 meters. The port is registered for international traffic and is located in the very center of the city. A vulnerable target is also a marina next to a fortress that is unregulated, neglected and undeveloped. Potential targets in the Danube coast can be a road bridge and a main gas pipeline across the Danube, which are not covered by this map. Considering that the Smederevo fortress, railway station, rowing club and promenade rest on the Danube, we have increased the score to 6, because in addition to the mentioned characteristics for rivers, the specificity for Smederevo is that this target is vital for the city, the residential part is close and easily accessible.

The current conception of the railway infrastructure established for decades, has the primary aim of satisfying the needs of business entities that are located directly in the urban fabric. This was the main task of the railway and is still valid today, although the economic circumstances and transport requirements have changed considerably.The Smederevo train station is between the fortress and the city with the function of passenger and freight traffic, with 9 electrified tracks. Industrial tracks of the port and tracks that connect Old Steelworks are connected through the station to the main railway network.The method of choice is different from that used at the river. The railroad is partly parallel with the Danube and physically

separates the coast from the city. This means that the coastal zone vulnerabilities will partially overlap with the railway zone. The railway and the railway station physically separate the Smederevo fortress from the city, and there may also be overlaps. Here the distance method, intersection method and complete method are expressed.The score of the tracks is generally 6 because they are exposed, vital, legitimate, destructive, close and easily accessible.It extends on area of 5,100 m along the right bank of the Danube from Kovinbridge to the former flow of the Jezava River. According to the position and content, several subzones can be distinguished. Existing industrial zone where there is the largest number of industrial enterprises is 101.3 ha[12]. Subzone "Šalinac road" of an area of 15 ha with prepared infrastructure for small and medium enterprises. The foreign investor started the production of cables for cars PKC here. The second sub-zone is located along the main road of the industrial zone along the Danube bank.In this subzone the objects of communal activities, separation and transshipment-overloading activities are included. There is a terminal, a decant, business buildings and reservoirs of NIS, a complex of commercial buildings, a new industrial port, a main gas pipeline across the Danube, Pancevo–Smederevo, with a projected capacity of 150 million $m^3$ and the bridge on the Danube.The area of this sub-zone is about 36 ha. The proximity of the Danube and the main road M 14, which connects the Morava valley with Banat, are elements which influence that this zone with its content is represented as a potential target of terrorists. The criteria it meets are exposure, easy access, vital, but not locationally near and not populated. In some segments, it can be overlapped with the Danube coast. The score of the zone is 4.

Figure 3 refers to the Smederevo fortress, the municipality building and the Police Administration as a potential target of a terrorist attack. City of Smederevo is located along the route of the Roman border (Limes) and Constantinople road, which during its history significantly determined its importance and role in the historical events. In the beginning of the fifteenth century, in the time of the despot ĐurađBranković, Smederevo gained a special significance when it became the last capital of the Serbian medieval state and the seat of church and business life. At that time, the Smederevo fortress was built, whose walls still stand today and testify to the turbulent past of the city, but also to the importance of Smederevo, which even then exceeded the local and regional dimension.Smederevo became the center where the influences of the East and West intertwined. The fortress is located on the right bank of the Danube. The interior space occupies 11 ha. It was modeled after the Constantinople fortress. It consists of the fortified palace (Mali grad, built 1428–1430) and the fortified town (Veliki grad, built in 1430–1439), which as a whole is connected to the palace.With its 25 massive towers, over 20 m high, connected ramparts, with a total length of 1.5 km and a thickness greater than 2 m, is one of the largest fortresses in Europe. Since it represents the tourist potential of international importance, it is visited by many tourists throughout the year. A significant number of cultural and entertainment programs are organized there.The significance of the fort, cultural value, position and number of visits may be motives for terrorist attacks. The attractiveness of the fortress as a terrorist target is higher at the time of the tourist event "Smederevskajesen" (Smederevo'sAutumn), when the most important programs in the fortress take place. Then the number of participants and visitors reaches several tens of thousands a day.The fortress is located between the Danube coast and the railway line, which we have identified as being vulnerable zones. Each of the aforementioned methods managed in the allocation of vulnerable zones may refer to the zone in which the fortress is. If we apply the criteria for evaluating the fortress as a potential target for terrorist attacks, the conclusion is that they are all represented, which means that the score is 8.

12 General Urban Plan of Smederevo, 2011 pp. 78–80.

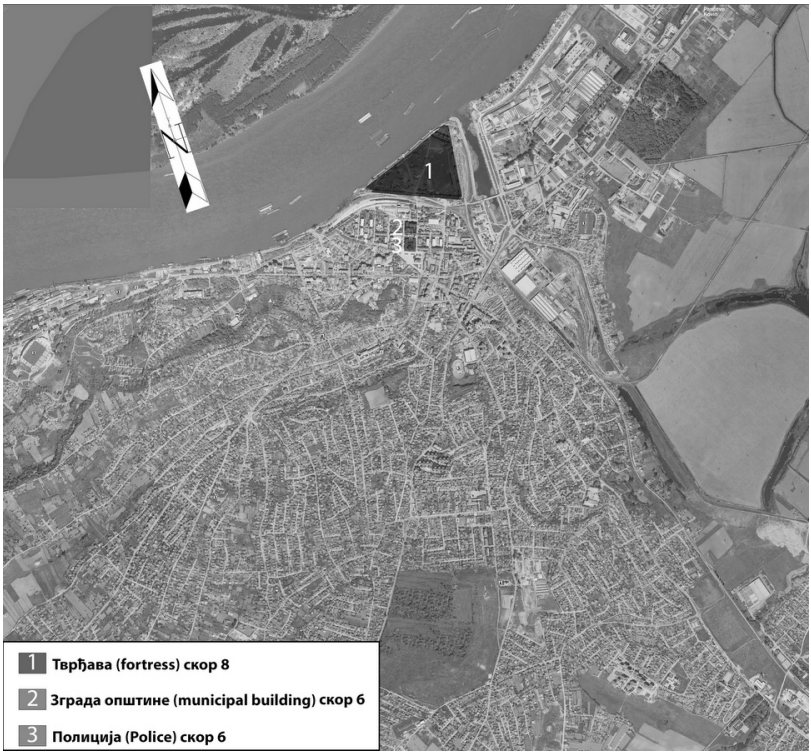



*Figure 3. The location of the fortress, the Municipality building and the Police Administration in Smederevo*

Municipal administration and police are very important institutions of the city, so they can represent potential targets. The spatial centralization of these public services is in a relatively small area of the city core, where the largest number of central activities is grouped. Like with other municipalities in Serbia, Smederevo is distinguished by the urbo-centric model of the organization of the administrative service, more precisely there are police and courts in one building. This zone is in intersection and overlaps with the zone of city central parks, railway tracks, fortresses and in the immediate vicinity of the Danube coast. This zone is exposed, significant, legitimate, destructive, inhabited and close. The value of target can be expressed by score 6.


*Figure 4. Locations of primary and secondary schools and parks in Smederevo*

In the urban area there are 7 primary schools attended by more than 6500 pupils, music school and 4 secondary schools, with over 4500 pupils[13]. The result of schools is 8, because schools generally have all the characteristics of the scheme; exposed, significant, primal, legitimate, destructive, settled, close and easily accessible. The analysis within a particular community can vary with the result that characterizes the vulnerability of each school.

Figure 4 lists the zones of certain characteristics, such as parks. They are marked as polygons representing the surface of the park. In Smederevo park areas are divided into the park areas of the Danube coast (Rowing Club and the Danube Park), recreational park surfaces:Aquarium, Pioneer Park, Majdan– Journalism Park, Park on Carina and Trade Park and green areas of the Central City Zone: "Park of the Combat Union", "Park of Three Heroes", "Park June 5th", "Waiting Room Park". The use of an area instead of a point can be used for locations that cover a large surface at that moment, and it is not necessary to present characteristics individually. The core assigned to these areas and which can cover any part of the park is 4, as parks are generally exposed, legitimate, close and easily accessible.The results may, however, vary depending on the season and the specific dates when the park can become filled with people, for example at the time of the economic and tourist event "SmederevoʾsAutumn".

13 General urban plan of Smederevo, p. 87.

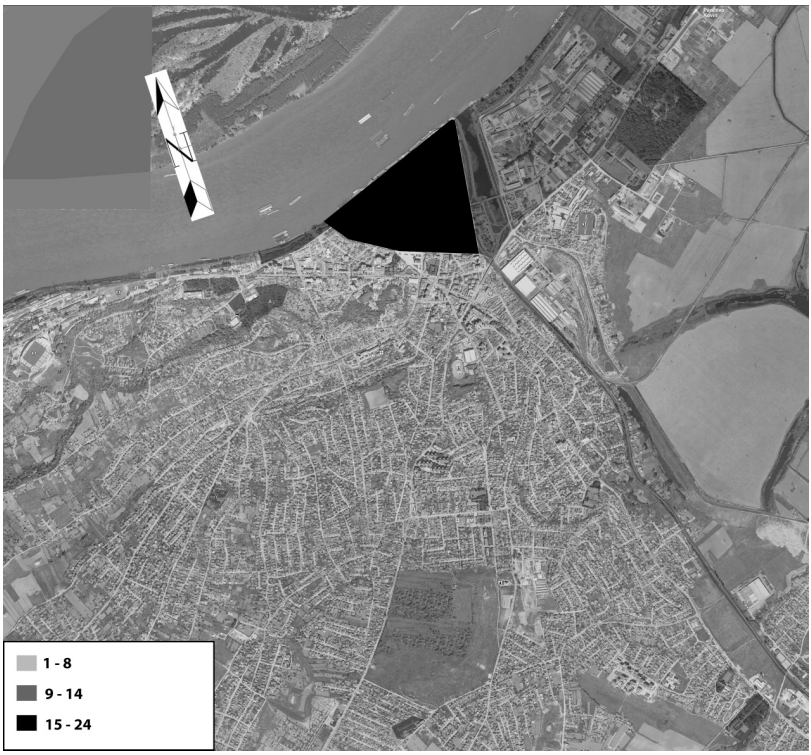



*Figure 5. Collective results of potential target vulnerability in Smederevo*

Figure 5 illustrates a summary of the results of the previous analysis. By overlapping maps of the individual targets, a map of collective values is obtained where the degree of vulnerability of the selected zones in Smederevo is based on the intensity of shading. From the attached map, it is noticeable that the most endangered areas are the Danube coastline from the fort to the rowing club, the fortress zone, the railway station, the city square (municipalities and the police) and the park area around the city square. Scores of potential vulnerabilities range from 15 to 24. In the second place is the Danube coast, which relies on the industrial zone, due to the importance of the facilities that are located here, such as NIS plants, gas pipeline and bridge over the Danube. The score ranges from 9 to 14. The other targets that we have selected have a score of potential vulnerability from 1 to 8.The map can be used to determine the priorities of strategic efforts in the prevention and use of resources within the community. Maps illustrate the geographical method by which the analysis of terrorism in the local community and assess of the vulnerability of targets for potential terrorist attacks can be carried out. There is great help from the police, as well as the city administration, with determining priorities, in time and with efficient response. The size and actual part of the given geographical unit will be based on the knowledge of the competent and specific location (topographic characteristics, proximity, etc.).

## CONCLUSION

If terrorism is a global problem, it means that no state or local community within it is exempted from possible terrorist activities. Terrorists target and plan for local communities that are easily accessible by applying tactics that match their goals.The paper presents one of the methods that can contribute to the successful work of the police in the local community. It should be emphasized that the use of mapping techniques in this way has not been empirically tested, so decision-making should be based on these results, together with other factors. Then many of the decisions to be made are subjective, which requires a team of people with experience in the field of geospatial analysis and terrorism. Team approach is essential for an effective assessment. Finally, this method does not determine where the potential center of the event is, but the possibility where there is a likelihood of a terrorist attack and provides a way for the police to establish a priority in determining possible targets, as well as educating citizens about the most vulnerable areas of their communities.The presented methodology can represent another form of vocational education and training of police officers important to analyze and solve problems related to the prevention of terrorist activities. This method should not be regarded as static and used on a single map for a certain moment and consider it sufficient. As stated above, events can be measured throughout the year, such as "Smederevo'sAutumn", "Nusic's Days" and other events, not just for certain periods.Targets and their vulnerabilities are constantly changing, which makes it necessary to constantly update the analyses. However, the ease of this technique and the use of available software, data, and analytical skills can make it easy to repeat the task.

## REFERENCES

1. Boba, R.*A crime mapping technique for assessing vulnerable targets for terrorism in local communities,*Crime Mapping Case Studies: Practice and Research,John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,West Sussex PO19 8SQ, England, 2008, pp. 143–151.
2. Clarke, R. V. and Newman, G. *Outsmarting the Terrorists*. Portsmouth, NH: Greenwood Publishing Group, 2006.pp. 4–29.
3. Directorate for Urbanism and Construction Land Smederevo General Urban Plan of Smederevo, Smederevo, 2011, pp. 76–87.
4. Mladenović M. Terrorist Attacks as a Cause of Emergency Situations, Proceedings of Crisis Management and Emergency Management – Theory and Practice, Belgrade, 2015 pp. 74–79.
5. Mensur, Š. Cooperation with the local community police for the purpose of preventing the criminal offense of Terrorism, Police Security, No. 3, 2015, pp. 292–298, Zagreb.
6. Orthophoto Plans of the Cities of Serbia, Republic Geodetic Authority, 2012, Belgrade.
7. Ronczkowski, R.*Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis,and Investigations*. Boca Raton FL: CRC press, 2004, p. 72.

# THE CONTRIBUTION OF THE EUROPEAN COURT OF AUDITORS IN THE FIGHT AGAINST THE FINANCIAL CRIME[1]

**Marko Dimitrijević, PhD**[2]
Faculty of Law, University of Niš

**Abstract:** The subject of analysis in this paper is the role of the European Court of Auditors (ECA) in combating financial crimes, primarily in the area of public funds managing. In this regard, in the first part of the paper, it points to the functions of the ECA, which are relevant to the harmonisation of the financial administrations of the Union and to ensuring the transparency of the entire budgetary system. The focus is on audit types of the audit process and methodology through which the Court exercises its jurisdiction and contributes to the development of a harmonised financial management, proper execution of administrative activities and exchange information with other public law institutions. As the Court does not have the possibility of making a legally bound decision in the case of financial fraud, in practice that can be resolved by close cooperation with the European Anti-Fraud Office (OLAF), which provides a significant contribution to general prevention against the financial crime. The budgetary spending control of the ECA has been completed with other forms of control, primarily control is exercised by the Department of Commission for the internal control of the national administration, according the fact that the funds from the EU budget are transferred to the national bodies, where there is a maneuver room for committing the various abuses. Establishment of credible macroeconomic dialogue beetwen ECA and other communitarian institutions, according to the author, is a prerequisite for efficient management of public funds and curtailment of real opportunity to exercise the financial crimes.

**Key words:** European Court of Auditors, financial crimes, OLAF, sound financial management, public funds.

## INTRODUCTION

Harmonisation of national budgetary policies in the European Union represents a major challenge for the European legislator, because the Member States do not want to limit the components of their fiscal and financial sovereignty. Namely, the concept of single budget represents since the establishment of the European Economic Unions (EMU) the question that Member States approached with caution because they do not want to delegate their subjective budgetary law, as well as the authorisation of the establishment, implementation, collection and control of paying taxes. Precisely for this reason, the formation and functioning of the European Court of Auditors (ECA) in practice was accompanied by numerous repercussions in terms of defining its jurisdiction, the legal nature of the decisions, status and relations with other communitarian institutions. However, the reason for its creation we recognise the

1 The paper is a part of the research done within the project "Protection of Human and Minority Rights in the European Legal Area", D172046 financially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia.
2 markod1985@prafak.ni.ac.rs.

absence of financial legitimacy which in the EU in the global economic and financial crisis is becoming particularly acute and strengthening the fight against financial crime.

Taking into account the concept of democratic legitimacy, by which the power of all the state and political institutions derives from the citizens and their returns, there is the difference between so-called *input* legitimacy or the legitimacy of the procedure and *output* legitimacy, or the legitimacy of the results.[3] The legitimacy of the proceedings exists when subjects make decisions on the basis of powers delegated by the citizens, while the legitimacy of the results assessed in relation to the fact whether the elected mandatories achieved their expectations and needs. According to this theoretical setting, the Court of auditors enjoy the legitimacy of the proceedings, which arising from the work of delegation of financial sovereignty.

## THE EUROPEAN COURT OF AUDITORS AS A KEEPER OF THE FINANCIAL CONSISTENCY

The formation of the ECA in monetary and financial law of the Union confirmed the need for establishing the *financial consistency* in conceiving the agenda of monetary and fiscal policy at the supranational level. With the formation of the EMU, financial consistency becomes an imperative in implementing of the national economic policies, where the discretionary powers of national operators are limited by supranational norms. This confirms the substantial value of financial compliance in the broadest sense (especially in terms of crisis) and reinforces the reputation of supranational bodies in charge of implementing it (primarily judicial authorities, which ensure the much needed legitimacy and transparency of the process). The European Court of Auditors performs the function of an external auditor and, as such, it carries out *three* types of audit: *financial audit, compliance audit, and review of the effectiveness of business operations.*[4] When performing financial audits, the Court assesses the accuracy, reliability and integrity of the submitted reports. It is important to determine whether reports reflect the actual financial situation, cash flows from previous years and performance results according to applicable financial reporting standards. At this point, we have to recall *modus operandi*, by means of which some States became EU members. The disputable activities were directly connected with the financial audit which was carried out in an adequate way; thus, owing to the methods of "creative auditing", some countries became members of the Union and later the EMU. In this sense, the term "*creative auditing*" implies the actions of the Member States of the European Monetary Union which are neither lawful nor unlawful in terms of their legal nature.[5] In practice, this involves taking advantage of *legal gaps*, which are inevitable both in the national and communitarian law due to the inability of lawmakers to predict all socio-economic relations which need to be regulated by the legal norm.

When performing *compliance audits*, the Court assesses whether the Union revenue and expenditure transactions are accurately calculated and whether they comply with the applicable normative framework. In case of the *review of the efficiency of business operations*, the Court analyzes the value of invested financial resources, and identifies its expense ratio. In the process of reviewing the effectiveness of business operations, special attention is given to the study of programs, operations, management systems and procedures of all bodies that manage the Union funds, in order to be assessing the efficiency of using funds. Although this

3 Scheller, H K.(2006), *The European Central Bank: History, Role and Functions,* European Central Bank, p. 127

4 European Court of Auditor, *Auditing the Public Finances of the European Union*, Office for Official Publication of European Communities, Luxembourg, 2010, pp.10-12.

5 Prokopijević, M. (2007), *European Monetary Union*, pp.79-82.

form of review covers a wide range of topics, it particularly focuses on the areas of economic growth and employment; reviews on these issues are published in separate thematic reports. Another subject matter of analysis in the process of auditing the efficiency of business operations is the assessment of various aspects of public interventions, including invested *resources* (i.e. financial resources, human resources, financial and regulatory-organizational resources), *output products* (performance results), *results* (the immediate effects of the program for direct beneficiaries), and *effects* (understood in terms of long-term changes in the society resulting from the action of the EU as a supranational organization). The question of the viability of invested resources and recovery of their opportunity costs is always a topical issue in the finances of the Union, especially in the circumstances of recession and crisis. The importance of this type of auditing implies the need for constant training and professional development of the judicial staff, introducing and developing new audit methodologies that increase the rate of the return of the invested Union funds (although the audit itself is carried out in line with the international auditing standards and code of ethics). In performing these audits, the Court uses different *manuals* that contain detailed technical instructions governing the activities.[6] Regardless of the differences in the forms and types of audit, each of them has to be based on common grounds which imply the use of a solid methodology based on professional standards and the adoption of best practices and principles that reflect the degree of quality required for changes in the mode of management of public finances.[7]

## POSITION OF OLAF IN ANTIFRAUD POLICY

Pursuant to the provisions of EU primary law, the Union and the Member States have the unambiguous joint responsibility in fighting and combating financial fraud. European Commission pursuant to art. 218 (2) of the EU can establish a special office to combat financial fraud whose authorisations are finally determined by Council Regulations (Council Regulation 2185/96 and Council Regulation 1073/99) on the conditions of starting and conducting investigations. OLAF in performing the investigation enjoys wide powers which are often in conflict with the principle of functional and institutional independence of the Communitarian institutions.[8] In order to protect financial stability, the European Parliament, the Commission and the European Council have signed the Agreement on the establishment of inter-institutional cooperation with OLAF. However, we must note that any communitarian institutions retained for themselves the powers to determine a specific conditions for the performance of technical cooperation with OLAF, which is especially important for independent work of the European Central Bank and the European Investment Bank. Interestingly, the perception of the European Central Bank, which does not recognise the competence of OLAF over its businesses, because OLAF internal organ of the Commission is formed according to the rules of procedures between themselves organisational units of the Commission and the European Central Bank as a supreme monetary institution in the European monetary law certainly does not have that status.

6 *European Court of Auditor Manuals* (2008), pp. 10-11.
7 Reed, J. (2015), How to Increase the Impact of Environmental Performance Audits?, *International Journal of Government Auditing* 41(2), pp.17-18. The Court of Auditors has initiated the establishment of the so-called *Contact Committee*, which should ensure the development of an integrated auditing framework in the EU by introducing mandatory standards for conducting audits in the public sector, and shape new functions, tasks and role of external auditors in the new institutional framework of the EMU. See: Laffan, B., Lindner, J. (2005), "The Budget", in Wallace H. and Wallace W. (eds) *Policy Making in the European Union*, Oxford University Press, pp. 210-222.
8 Duzler, B. (2001), *OLAF or the Question of Applicability of Secondary Community Law on ECB*, European Integration online Paper (EIOP), Vol. 5, pp. 2-3.

OLAF has the authority to initiate the investigation and performance in the field of financial activities and the imposition of a financial penalty. The origin of this body originates from the department of the General Directorate of the European Commission for a coordinated fight against the financial fraud (Unity for coordinating anti-fraud fight UCLAF), which was established in 1988. In terms of globalised financial flows it has become clear that national courts of auditors and supreme audit institutions cannot rely solely on the work of national authorities in the fight against the financial crime which receives the trans-national character. Over the years, UCLAF received the exporting powers to initiate an investigation on its own initiative in all circumstances where there are indications of some form of financial crime irrespective of the needs of national court of auditors which is primarily motivated by the need to preserve financial stability in addition to monetary stability becoming more and more characteristics of a pure public good because it can be provided only the competent national authorities which act in a way *de lege artis.* Competence of OLAF refers to the initiation of the investigation in cases related to illegal spending a single budget of the EU, acts of corruption and serious abuse of authority at the expense of financial interests of the Union.[9] In performing its jurisdiction this authority may cooperate with the Commission, but it is primarily in their work subordinate to the Commissioner responsible for issues of the Customs Union, tax and auditing. *Ratio legis* of its functioning is a protection of the financial interests of the Union by combating corruption and financial crime, safeguarding the reputation of the Union through the use of disciplinary measures to the members of the body that do not respect the rules of the profession and does not take into account the communitarian interests as well as providing support to the Commission in detecting and timely prevention of fraud actions.

Cooperation with the European Court of auditors with OLAF has been significantly promoted by giving specific recommendations for combating financial crime which in one consistent way has shaped a cooperation of these bodies with clear antifraud tools and instruments. On that occasion, the Court took the view that it is necessary to make certain changes in the work of OLAF so as to increase the number of persons involved in the investigations in order to shorten their duration, increase efficiency in the context of planning and supervision of investigations themselves, consolidating antifraud legislation, as well as the need to adopt special reports on the effectiveness of the work of OLAF.[10] It enjoys administrative, operational and financial independence in the performance of the aforementioned tasks. In exercising its authority it can carry out internal and external investigations. Subjects of an internal investigation may be all the communitarian authorities while performing external investigations OLAF operates as an extension of auditors in all matters concerning the EU budget and can then cooperate with the competent authorities of the Member States. By performing these tasks, valuable coordination mechanisms are established that contribute to the exchange of information, dissemination of good practices and learning from their own mistakes that is creating optimal instruments in the fight against financial crime. At the same time, realized and criminological support element of the situation when the competent authorities in the Member States in criminal proceedings can count on technical, logistical and operational support of this supranational authority.

9 *Commission Decisions of 28 April 1999 establishing Anti-fraid Office* (*OLAF*), (notified under document number SEC(1999) 802), *Official Journal L 136, 31/05/1999 P. 0020 – 0022.*
10 European Court of Auditors, *Special Report No. 2/2011 concering the management of the European anti-Fraud Office*, p.6.

## COOPERATION OF THE EUROPEAN COURT OF AUDITORS AND OLAF IN FIGHTING FINANCIAL CRIME

The main disadvantage in designing policies to fight financial fraud in the EU concerns the insufficient level of cooperation between Member States, lack of coordination of activities of competent authorities, which in the final stage can lead to occurrence of discontinuity of court proceedings, to the existence of legal gaps in national and European legislation, as well as the different solutions of Criminal Code for the form of punishment, which implies the imposition of inadequate criminal sanctions.[11] It is for this reason there is a realistic and logical need to establish a new normative framework of antifraud policy that will establish a normative and economic efficiency of the police work, public prosecutors and all competent of judicial authorities as the primary subjects of such policies at the national level, but also authoritative supranational agencies such as OLAF, EUROPOL and EUROJUST.

As the financial fraud in the conditions of the global economic and financial crisis are receiving the special dimension, the European Commission in early 2012 adopted a report which makes a distinction between financial frauds, suspected frauds and other financial irregularities which cannot be treated as frauds.[12] Under frauds, it is meant any use or presentation of false, incomplete or incorrect documents and report caused by the effect of the reduction of budgetary revenues, as well as the disclosure of information or misuse of a legally obtained benefit with the same end effect. The cases of suspected scam boil down to any irregularities that may initiate a separate administrative or judicial proceedings, while other irregularities relate to causing inadvertent errors in billing and collection of taxes, customs duties, as well as cases of accidental fulfilling these duties. The most prevalent forms of financial crime that directly or indirectly affects the EU budget includes commitments in the field of import duties, namely the falsification of documents relating to the origin, description, value and quantity of the product, value on added tax and various forms of informal economy.

The European Commission in early 2011 has adopted a strategy which it prevent budgetary losses by applying preventive and corrective measures in the form of early identification of irregularities, the investigation and return of illegally spent budgetary funds. The role of the European Court of Auditors in the implementation of this strategy is set as a *conditio sine qua non* for solving cases in pronouncing a final verdict on committed fraud, the recognition of the evidence collected in other Member States, and which concerning the illegal spending of budgetary funds to reduce rates of financial crime.[13] The European Court of Auditors publishes the annual accounts of the expenditure of funds from the common budget of 2007 financial year. These acts include a statement of assurance in terms of ways to keep business books and European expenditures (i.e. whether the transaction granted in accordance with the rules).[14] Recently, the Court in this act found that the financial fraud make up 0.2% of current spending and the largest number of cases was processed and detected by OLAF. The Court also was of the view that the medium term budgeting represents the optimal mechanism to reduce errors in the use, management and in spending of funds, as well as a requirement to increase

11 Strabyla-Chudzio, K.(2016), The Effectivenes of EU Financial Interests Protection-the Case of Traditional Own Recources, *Journal of International Scientific Publication, Economy and Business*, Vol. 10, pp. 390-395.
12 *Proposal for a Directive of the European Parliament and the Council on the fight against fraud to the Unions financial interests by means of criminal law*, COM (2012), 363 final, European Commission, Brussels.
13 European Commission, *Anti-fraud Strategy*, Communication from the Commission to the European parliament, the European Council, The Council, the Economic and Social Committee and the Committee of the regions and the Court of Auditors, COM(2011) 376 final, Brussels.
14 *European Court of Auditors Annual report Q&A* (2015).

the efficiency of public expenditure, which indirectly contributes in reducing the opportunity to commit financial fraud.

A significant step in concretising the cooperation between the Court of Auditors and OLAF made by the decision of the Court on the concrete forms of cooperation in the field of access to information to OLAF which comes in carrying out investigations.[15] This decision applies to all cases in which there is a reasonable suspicion that are violated the financial interests of the Community, where none communitarian institutions cannot enjoy immunity (including the Court of Auditors itself). In circumstances where there is a suspicion that the communitarian financial interests are violated, each Member State, without delay about that, must inform OLAF in the form of standard written submission. Similarly, if the Court of Auditors on potential financial irregularities to be informed in an anonymous report, it shall timely inform OLAF to take appropriate investigative actions. In exchange of information, it should be taken into account the respect for the principle of confidentiality of data from the application, and communication with other communitarian bodies in a way that does not jeopardize the investigations.

In circumstances where OLAF requesting information or access to documents on which the Court carried out the investigation, all information shall be promptly submitted to the Director of OLAF and the competent authority of the relevant Member State involved in financial investigation, by which is established a functional cooperation in leading the fight against financial crime at a higher level . When the initiation of an investigation is initiated by a third party *ex privato*, and concerning the violation of the financial interests of the poor management of public finances, incompetence, corruption or other illegal activities the Court also promptly inform the Director of OLAF and the competent national authorities. Certainly, the Court can continue to audit the way *de lege artis* after informing OLAF and the initiation of the investigation, provided that it does not prejudice the course and outcome of the investigation. We note that in this way the Court has confirmed the position of OLAF as the main financial prosecutor of the Union in all cases of serious non-performance or roughly violation of duty of Communitarian bodies in the broadest sense in the sphere of budgetary interests.

The next step in the importance of cooperation with OLAF, the Court of Auditors has made the decision on the concretisation of the terms and conditions for the conduct of internal investigations.[16] On that occasion it explicitly determined that the Director of OLAF shall inform the Court of Auditors on initiating internal investigations by sending written notification to the Secretary General of the Court on the conditions under which the investigations will be conducted and specifying the identity of the responsible persons who will realize it. All officers of the Court shall cooperate in carrying out investigations and are obliged to provide the necessary information and to answer the questions about what the Secretary General must receive a written note. If there is a legal interest to a third party to be involved in the investigation and informed about the results, it may be allowed, as a rule, only after the conclusion of the investigation or earlier if not undermine its flow, but only about the facts that are relevant to that part. In circumstances where there is a need to preserve absolute confidentiality, the court may postpone the submission of such information by concluding a separate agreement of behalf of the court, signed by the Secretary General. Similarly, if the competent police and judicial authority shall request the immunity from prosecution of individual officers in cases of financial crime, such a request must be submitted to the Director of OLAF to review and giving opinion of justification.

15 *Decision No 97-2004 of the Court of Auditors laying down arrangements for cooperation with the European Anti-Fraud Office in respect of access by latter to audit information.*
16 *Decision No 98-2004 of the Court of Auditors concering the terms and conditions for internal investigations in relation to the prevention of fraud, corruption and any other illegal activity detrimental to the Communities financial interests, p. 4.*

Terms of performing cooperation between the Court of Auditors and OLAF in practice are later amended by Decision of the Court on the application of certain rules for the implementation of cooperation in the legal traffic.[17] At the same time, is determined a clear commitments of the judges of the Court of Auditors that on the existence of financial scam notify the court president or the oldest judge if there is doubt that the president himself actor of illegal financial activities. The European Court of Auditors is, in our opinion, by the adoption of such decisions has given the greatest contribution in the fight against crime financial defining the direction, the course, the terms and conditions of cooperation with OLAF on a broad basis, where the legitimacy of the prosecution cannot enjoy not only the staff of the court which as far as possible contributes to establishing the principle of material truth in the procedures in the true sense of the word. This is only the Court confirmed its position as the authoritative guardian of the financial consistency in the European Monetary Union in a credible way that gives hope for the revitalisation of deteriorated financial legitimacy in terms of the crisis and its preservation raises a legal imperative in the future.

## CONCLUSION

The European Court of Auditors performs the role of ex post guards of fiscal or financial discipline in the Economic Monetary Union. Stable public finance imply a reduction of opportunities for the exercise of financial crime, where the European Court of Auditors with its internal acts (by decisions, opinions, reports and recommendations) seeks to contribute in the creation of optimal antifraud policy. As the Court does not enjoy the possibility of imposing legally-binding decisions in this sphere, it is in practice replaces by the cooperation with OLAF which in the past few years from the outbreak of the debt crisis significantly improved and placed on a solid basis. In this sense, with the analysis of a large number of contractual arrangements on the concretisation of inter-institutional cooperation with other bodies we can recognise the effort which the court as the primary external auditor is investing in order to protect the budgetary interests of the Union. Also, we may note that the European Court of Auditor constantly evolving its role and competence *ratione materiae* in the fighting against the financial crime, which is indirect in the initial years of its operation has received equally important role and position of OLAF, and their activities in this field cannot be seen separately since they condition their mutual success. We believe that in the fight against financial crime the role of European Court of Auditors is inevitable because there is a need that by derogation of standards of primary and secondary law court receives the possibility of pronouncing verdicts, which will in conjunction with the work of other bodies involved in the macroeconomic dialogue will achieve a much needed general prevention.

## REFERENCES

1. Commission Decisions of 28 April 1999 establishing Anti-fraid Office (OLAF), (notified under document number SEC(1999) 802), *Official Journal L 136 , 31/05/1999 P. 0020 – 0022.*
2. Decision No 97-2004 of the Court of Auditors laying down arrangements for cooperation with the European Anti-Fraud Office in respect of access by latter to audit information.

17 *Decision No 99-2004 concering the rules of arrangements for cooperation with by Members of the Court in internal investigations in relation of fraud, corruption and any other illegal activity detrimental to the Communities financial interests, p.2-4.*

3. Decision No 98-2004 of the Court of Auditors concering the terms and conditions for internal investigations in relation to the prevention of fraud, corruption an any other illegal activity detrimental to the Communities financial interests.

4. Decision No 99-2004 concering the rules of arrangements for cooperation with by Members of the Court in internal investigations in relation of fraud, corruption an any other illegal activity detrimental to the Communities financial interests.

5. Duzler, B. (2001), *OLAF or the Question of Applicability of Secondary Community Law on ECB*, European Integration online Paper (EIOP) Vol. 5 (2001),1-6.

6. European Court of Auditor Manuals (2008).

7. European Court of Auditor (2010), *Auditing the Public Finances of the European Union*, Luxembourg: Office for Official Publication of European Communities.

8. European Court of Auditors, *Special Report No. 2/2011 concering the management of the European anti-Fraud Office*.

9. European Commission (2011), *Anti-fraud Strategy*, Communication from the Commission to the European parliament, the European Council, The Council, the Economic and Social Committee and the Committee of the regions and the Court of Auditors, COM(2011) 376 final, Brussels.

10. European Court of Auditors Annual report Q&A (2015).

11. Laffan, B., Lindner, J. (2005), "The Budget", in Wallace H. and Wallace W. (eds), *Policy Making in the European Union*, Oxford University Press, 210-222.

12. Proposal for a Directive of the European Parliament and the Council on the fight against fraud to the Unions financial interests by means of criminal law, COM (2012), 363 final, European Commission, Brussels.

13. Prokopijević, M. (2007), *European Monetary Union*, Belgrade: Construction Book.

14. Reed, J. (2014), How to Increase the Impact of Environmental Performance Audits?, *International Journal of Government Auditing* 41(2), 17-23.

15. Scheller, H. K. (2006), *The European Central Bank: History Role and Functions,* Second Revised Edition, European Central Bank.

16. Strabryla-Chudzio, K. (2016), „The Effectivenes of EU Financial Interests Protection-the Case of Traditional Own Recources", *Journal of International Scientific Publication, Economy and Business*, Vol. 10, 390-400.

# TAX FRAUD AND PLEA BARGAINING

**Suzana Dimić, PhD**
**Mirjana Đukić, LLM**
University of Priština, Kosovska Mitrovica, Faculty of Law

**Abstract**: Taxation because of economic strength causes a negative reaction from the taxpayer. Though as old as taxes, the problem of non-fulfillment of tax obligations is present in modern countries because of multiple causes. Especially because of frequent detrimental financial effects consisting of the fact that the Treasury is deprived of the amount of tax that could be collected if all citizens were tax liable. The behavior of taxpayers is often unlawful in case of tax evasion. The worst form of the violation of tax legislation is tax fraud qualified as a criminal offence.

Special attention has recently been paid to the voluntary payment of taxes. Preventive efforts to create a climate in which paying taxes could be popularized influence the positive attitude of taxpayers in accepting and fulfilling their tax obligations. Additionally, an important factor in combating tax crime is adequate penal policy.

Implementation of the agreement on the admission of the offense in the domain of tax fraud involves the detection and punishment of tax evaders. The purpose of the repressive measures of penal policy is not only to punish these persons, but also to achieve a psychological effect on other taxpayers. Agreement on the admission of the offense gives the public prosecutor and the defendant the opportunity to negotiate for a particular influence on sanctioning tax evaders facing the dilemma of the kind of message sent to other taxpayers with respect to the proper execution of tax liabilities.

**Key words:** tax evasion, tax fraud, plea bargaining, criminal policy

## INTRODUCTION

Taxation, due to the reduction of economic power, causes a negative reaction among taxpayers. Although they have an indirect benefit, because it is inconceivable for a state to function without paying taxes, taxing process is followed by various modes of resistance among taxpayers. Thus, the Treasury remains deprived of the amount of revenue that would be collected if they complied with tax liability. Hence, the reduction of the so-called "tax gap" which represents the difference between the revenue that would be collected if all the taxes were paid in accordance with tax laws and the taxes actually paid, is a priority task of the tax policy of modern states. Identifying the factors influencing the choice whether the taxpayer should or should not pay tax is important for finding ways to reduce tax evasion. Very often the evasion to pay taxes takes the form of illegal tax evasion, which consists of an unlawful conduct of a taxpayer. The most severe form of a direct violation of tax regulations is the tax evasion (tax fraud), qualified as an offense.

One of the hallmarks of modern criminal procedural legislation, which has not bypassed our country, is the parallel existence of common, ordinary forms of criminal procedure which represent the regulation and distribution of a simpler form of treatment in criminal matters basing its justification on a heterogeneous structure of crimes and their perpetrators. Today we can safely conclude that simplified procedural forms of criminal cases are one of the important instruments of criminal procedure.

Since 2006, when the institute of plea of the offense (then the plea agreement) was introduced into our law, it has undergone some changes which have been subjected to criticism in the scientific and professional community, primarily because it was not in accordance with certain principles of criminal procedure and the purpose of punishment (special and general prevention). Certain elements of the agreement (the possibility of the agreement on the occasion of any criminal offence regardless how serious it might be, as well as the measurement of the sentence) arise the questions of the realization of the purpose of punishment, the principle of truth and fair-trial procedure. As one of the benefits for the confession, the defendant receives a more lenient punishment. In this way, especially in case of serious offenses, it does not provide the possibility of educational influence on others in order not to commit criminal offenses, and the perpetrator, as a party to the agreement is motivated to continue his criminal career. In an effort to end the procedure as soon as possible, the fairness of the proceedings is left out.

## TAX FRAUD - THE MOST SEVERE FORM OF TAX EVASION

In our previous legislation, there were some wanderings in terms of regulating the offense of tax evasion. The question of whether the offense should be put in criminal or tax law has been now resolved by its regulation of Article 229 of the Criminal Code.[1] The object of criminal protection of this criminal act is tax liability.[2] The act of committing tax evasion is determined in terms of determining the payment of taxes and other duties, and it may consist of: 1) providing false data on legally acquired income, on items or other facts which affect the determination of these obligations; 2) the failure to legally report the acquired income, that is, objects or other facts which affect the determination of these obligations and 3) withholding data in other ways. For this criminal act to exist, it is necessary that at the time of the offense an intention for complete or partial tax evasion is present (exists).

Unlawful conduct of the taxpayers which is qualified as a criminal tax offense is socially dangerous behavior. Breach of fiscal rules directly or indirectly threaten the fiscal interests of the state.[3] That is why the preventive and repressive measures taken in one country for combating tax evasion as the primary tax offence are of great importance. In modern countries special attention is paid to preventive measures which affect the attitude of taxpayers towards the exercise of their tax obligations. The subjective causes of tax evasion related to the personality of the taxpayer include tax awareness, tax mentality, a sense of belonging to a particular community, the level of education, the perception of fairness of the tax system.[4] Loyalty to the tax may be affected by the tax mentality of the people. Creating the resistance of taxpayers towards their obligations may occur due to the negative public perceptions expressed by certain social norms (for example, in some areas the tax evaders are considered heroes).[5]Changing the concept of the relationship between tax authorities and

1 Кривични законик Р Србије, "Сл. гласник РС" бр.85/2005, 88/2005-испр., 107/2005-испр., 72/2009, 111/2009, 121/2011, 104/2013, 108/2014. In addition to tax evasion, the Criminal Code regulates non-payment of withholding tax and smuggling, classifying them into crimes against the economy. On the other hand, some tax offenses remained in the Law on Tax Procedure and Tax Administration(Закон о пореском поступку и пореској администрацији Републике Србије ("Сл. гласник РС", бр. 80/02, 84/02 - испр., 70/03, 55/04, 61/05, 85/05 - др. закон, 62/06 - др. закон, 61/07, 20/09, 72/09 - др. закон, 53/10, 101/1, 2/12 - испр., 93/12) ,), such as, for example, wrongfully disclosed amounts for tax refunds and tax credits, prohibited excisable products.

2 Поповић, Д., *Коментар Закона о пореском поступку и пореској администрацији*, Cekos in, Београд, 2003, p.246

3 Анђелковић, М., Димитријевић, М., *Пореско право Србије*, Ниш, 2009, p.326

4 Анђелковић, М., *Деформације пореског односа,* Правни живот бр. 10/1997, p. 230.

5 Анђелковић, М., *Моделирање понашања пореских обвезника у савременој теорији,,* Међународна

taxpayers helps in creating a positive attitude of taxpayers in acceptance and fulfillment of tax obligations. Abandoning the traditional relationship which meant acting of tax authority from the position of state power, the concept of service-oriented work is created in order to facilitate the fulfillment of obligations of taxpayers. From preventive reasons, the relationship with the conflicting interests of its subjects grew into a relationship in which there is greater communication, cooperation and understanding.[6] Due to modernization of the attitude towards taxpayers, tax authorities affect the mind and strengthen tax morality. They strive to achieve that by greater involvement of the taxpayers in the assessment and collection of taxes. Such changes are referred to as cooperation of taxpayer in the tax procedure.[7]

Numerous objective factors affect the tax evasion. From general economic developments in the country, through the economic power of the taxpayer, for the taxation procedure covers the part of the income earned, all the way to the factors that are on the side of the design of the tax system and individual tax forms. When designing individual tax forms, the behavior of taxpayers may be affected by the type and amount of the tax rate, since as a rule, progressive rates result in higher tax burden. When designing the tax system as a whole, the creators of tax policy should take into account the amount of the total tax burden. Taxpayers feel the tax liability as certain interference of state into their privacy, tapping into their income and (or) property, so that with the increase of the tax burden tax resistance increases, too.[8] If one takes into account that the share of tax revenues in GDP is about 33.4%, and the data are commonly used as an indicator of the overall tax burden, we can see that the tax burden in Serbia is great.[9] This situation, among other things, is the result of high public spending inherited from the socialist period. In Serbia, as in other socialist countries, the role of the state in meeting public needs was great, and the fiscal burden even then was not in accordance with real economic opportunities. The rigidity of inherited significant public spending remains one of the most serious disturbances of economic development in our country. [10] As one of the factors affecting the formation of unfavorable sentiment towards the payment of taxes is frequent changes of tax regulations. Inconsistency and frequent wanderings in tax regulations have been present in Serbia in the previous period. The level of tax penalties and their consistent implementation affect the compliance with the tax liability. By prescribing and imposing penalties tax evaders are punished, and also general prevention is achieved. Detection and punishment for tax crimes should be a warning to all other taxpayers to properly fulfill their tax obligations.

A fine and a prison sentence depending on the form of the criminal offense of tax evasion are regulated in our criminal law. As a basic form, which includes unpaid taxes amounting 150 000 dinars, a fine and a prison sentence of 6 months to 5 years are prescribed. For the first more severe form of tax evasion, in which the amount of unpaid tax exceeds RSD 1 500 000 a fine and a prison sentence of 1 to 8 years is prescribed. While for the other severe form, in which unpaid tax exceeds the amount of 7 500 000 dinars, in addition to the fine, a prison sentence of 2 to 10 years is imposed.

Adequate penal policy has a major role in combating the criminal offense of tax evasion. According to some authors, its tightening would contribute to combating tax evasion. The

научна конференција "Правни систем и друштвена криза", Правни факултет Универзитета у Приштини са привременим седиштем у Косовској Митровици, 2011, p.483.

6 Анђелковић, М., *Редифинисање пореских односа*, Заштита људских и мањинских права, Тематски зборник Правног факултета у Нишу, 2015, p. 58.

7 Димитријевић, М., *Значај кооперативности пореских обвезника у савременом пореском систему,* Зборник радова "Право Републике Србије и право ЕУ - стање и перспективе", p. 419.

8 Jelčić, B. *et al*, *Financijsko pravo i financijska znanost,*Narodne novine, Zagreb,2002, p. 190.

9 Countries such as Denmark (49,6%), Belgium (47,8%), have great tax revenue in GDB, but these are the countries with strong social role of the state.

10 Раичевић, Б., *Јавне финансије,* Економски факултет, Београд, 2008, p.33.

behavior of the taxpayer depends on the relationship between the expected benefits of unpaid taxes and any expenses which can occur in the event of being discovered and punished.[11] In that case, a kind of punitive policies should be led aiming at imposing fines which significantly exceed the amount of the unpaid tax. In terms of imposing prison sentences it should be added that the current criminal legislation gives the possibility of setting house arrest as an alternative to imprisonment. If the offender was sentenced to imprisonment up to 1 year, the court may at the same time determine that it would be served in the premises where he lived if given the personality of the offender, his previous life, the degree of culpability and other circumstances, we may expect that the purpose of punishment would be achieved.[12] This means that for the primary and the more severe form of the offense, the court may order the tax evaders house arrest.

## GENERAL CHARACTERISTICS OF THE PLEA BARGAINING

The USA represent the cradle of the agreement, where it is known as plea bargaining, which literally means barging, guessing. One cannot say with certainty what specifically led to its appearance, so there are several points of view in theory. According to some authors, one of the causes of the emergence and development of this institute could be structural changes in the trial (specifically, when the court lost a dominant role in criminal proceedings).[13] The Industrial Revolution (1900-1940) also contributed to its development, when the courts were looking for a way out in simpler procedures which were affected by a number of processes between manufacturers and consumers. It can be said that this institute experienced a boom as a result of draconian penalties provided for in the American criminal law. Since there was a huge difference between the minimum and the maximum fine imposed, surely the sentence imposed by the prosecutor offering the defendant the conclusion of an agreement, was far more favorable and attractive than the one that could have been imposed if the regular criminal procedure had been carried out.[14]

The plea bargain in our country can be concluded under following conditions[15] 1) the process for one or more criminal offences is led against the defendant, for which the sentence of 12 years is provided by law; 2) the defendant pleads guilty of the crime or crimes for which he was charged; 3) it was concluded in writing; 4) the agreement was submitted to the judge for the previous process-if concluded by the time of indictment confirmation-or to the President of the Council –if concluded after the confirmation of indictment. In terms of the type and severity of the crime or criminal offenses as a subject of the agreement, the Code does not contain a precise provision which would stipulate that the agreement is going to be concluded precisely for any criminal offense, regardless of how serious it is, as well as for those for which the punishment of imprisonment for the period of over twelve years is prescribed. Since there are no legal limits that would relate to the nature and gravity of the offense, we can logically conclude that the agreement can be concluded for all criminal offenses for which the overall

11 Милошевић, Г., *Економски аспект евазије пореза,* Економски хоризонти, 2006, 8, (1-2), p.76.
12 Article 45, paragraph.5 Criminal Code of Serbia..
13 M. Haller, *Plea Bargaining: The Nineteenth Century Context*, Law & Society Review, vol. 13, no. 2, 1979, 274-275.
14 M. Damaska, *Negotiated Justice in International Criminal Courts*, World Plea Bargaining-Consensual Procedures and the Avoidance of the Full Criminal Trial, Carolina Academic Press, 2010, 81-103.
15 Article 313. Code of Criminal Procedure (Законик о кривичном поступку („Службени гласник РС", бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014).

criminal proceedings is normally led.[16] Mandatory elements of the agreement are[17]:1) description of a crime that was the subject matter; 2) confession that the defendant has committed a criminal offense referred to in item 1 of this paragraph; 3) the agreement on the nature, extent, or range of punishment or other criminal sanctions; 4) the agreement on the costs of the criminal proceedings, forfeiture of the offense, on the property claim if it is presented; 5) the waiver of the parties and counsel of the right to appeal against the decision by which the court has fully accepted the agreement, except in cases foreseen by Article 319 of the Code Optional elements include:[18] 1) the declaration of the public prosecutor of the cancellation of the prosecution of offenses which are not covered by the agreement; 2) a statement of the defendant that accepts the obligations of Article 283, paragraph 1, provided that the nature of the obligation is such that permits beginning of its execution before submitting the agreement to court; 3) the agreement in terms of assets derived from crime to be confiscated from the accused.

According to the latest legal provisions, the agreement may be concluded between the public prosecutor and the defendant all the way from the order to conduct an investigation till the statements of the accused on the charges at trial.[19] In relation to the former legal solution according to which there was a possibility of concluding an agreement only for criminal offenses for which a prison sentence of up to 12 years was prescribed, fundamental change is reflected in the fact that this type of agreement is now possible to conclude on the occasion of any criminal offense, therefore, even if the prescribed prison sentence exceeds 12 years, where the legislator finds justification in the fact that the former regime was contrary to the nature and objectives of the institute. Surely this kind of legal solution agitated scientific community because it actually provides that the agreement may be reached in respect of any type of crime, regardless of its severity, for example with the defendant who is charged with multiple murder, child rape and other serious crimes. From the text of the new Criminal Code of the Republic of Serbia, the provision that the agreed penalty may not be below the minimum prescribed for the offense for which the defendant pleads guilty is deleted, opening the possibility that for the serious crimes the mildest punishment can be arranged.[20]

A key element of the agreement is the confession of the defendant that he had committed the crime he is charged with. In essence, it is a formal process to a specific action in which the defendant agrees with the allegations of the public prosecutor regarding the legal and factual issues that are the subject of proceedings. There is no doubt that the aim of introducing this institution in our and other legal systems is to solve the issue of the existence of the offense and the guilt of an individual charged with it without any proof, which is justified by savings in the budget and other public resources. The confession of the offense cannot be regarded as the truth established by the agreement, bearing in mind that the law does not oblige the parties in the agreement to use it to truthfully describe the features of a confessed criminal offense. The prosecutor in the agreement states the facts for which he finds a doubt they are true,

16 This means that the agreement can be applied for minor offenses, for which summary criminal proceedings are instituted. The provisions on the summary criminal proceedings shall apply to all criminal offenses punishable by up to eight years in prison, and if those provisions are not particularly prescribed, the other provisions of the Code shall be applied, which would be in accordance with applicable provisions of the agreements between the public prosecutor and the defendant since in relation to them there are no prescribed deviations (Ђурђић, В., *Споразум о признању кривичног дела – форма за изрицање правде или за решавање спорова*, Зборник радова са научне конференције: Људска права између идеала и изазова садашњости, Правни факултетУниверзитета у Приштини, КосовскаМитровица, 2016, р.371-372).

17Article 314.Paragraph 1.Code of Criminal Procedure.

18Article 314.Paragraph 2.Code of Criminal Procedure.

19Article 313.Criminal Procedure Code.

20 Ђурђић, *Перспектива новог модела кривичног поступка Србије,* Журнал за криминалистику и право, Београд, 20.2, 2015, р.86.

where the defendant confirming them is under no obligation to tell the truth. The defendant simply can realize his interest in the agreement so as to confirm the recognition of the facts that are not true if in turn he can realize certain benefits (cancellation of the public prosecutor from prosecution for other crimes, a less severe penalty). The truth is certainly the goal of the criminal proceedings, but it may not be such a value that must be attained at all costs. However, it is necessary to border the path to reaching it by the application of procedural and legal resources available to the participants of the process with respect of all rights that are guaranteed to them by numerous national and international documents.[21] The other extreme would be a notion of truth as an absolute value, which would mean non-compliance with the rules of evidence and the prohibition, which would ultimately pave the way to torture, drug analysis and other illegal means to obtain evidence.[22] Abandoning the mixed model and introducing the adversarial criminal proceedings, the very way of establishing the truth has changed. In the former mixed model, the court activity in determining the facts that did not allow the parties to interfere with the judge when establishing the facts, determined the truth as material. On the other hand, in the adversarial model, the dominant role of the parties in the process of proving, in which the court is just a passive arbitrator, determines the truth as formal. So we are not talking about the truth in the material and formal sense (different kinds of truth), but "different paths to discover the truth in court proceedings".[23]As a result of the accusatory and contradictory elements (inherent in the adversarial procedure), the truth is ignored and becomes subordinated to the interests of efficiency of the process (the principle of truth being replaced by the principle of process economy). Within the agreement on the admission of the offense, the truth represents the facts on which both parties (plaintiff and defendant) agree.[24]

The essence of the principle of immediacy is a direct determination of facts based on the source of information, so that there are no intermediaries between the criminal court and the source of information, and the court reaches a decision according to the facts it determined itself.[25] In the Article 419 of the Criminal Code of the Republic of Serbia, it is stipulated that the court shall reach a verdict solely based on the evidence presented at trial. It is clear that the proceedings conducted on the occasion of the agreement on the admission of the offense considerably deviate from the principle of immediacy. The hearing at which the court decides on the agreement primarily takes place not only to determine that the defendant knowingly and voluntarily entered into an agreement but also that he is fully aware of the legal consequences of such confession.[26] Due to lacking of proof, the court has no direct access to sources of information, but it learns about the evidence from the agreement. Finally, when deciding on the agreement, it only ascertains whether the evidence is inconsistent with the confession or not.[27]

It is traditionally considered that the main tasks of a judge in criminal proceedings is to establish the facts properly and declare sentence correctly on the basis of these facts, where he plays an important role in the policy of repressing crime.[28] However, the type of adversarial criminal proceedings in recent years has called into question both judicial functions. Firstly, correct or complete and true fact-finding by the Court in this model of criminal procedure

21 Шкулић, М., *Однос начела истине и поједностављених форми кривичног поступка*, Поједностављене форме поступања у кривичним стварима – регионална кривичнопроцесна законодавства и искуства у примени, Мисија ОЕБС, Београд, 2013, p. 69.
22 *Ibid,* p.69-70
23 Кнежевић,С., *Основна начела кривичног процесног права*, СКЦ, Ниш, 2012 p.93.
24 *Ibid*, p.101
25 *Ibid*, p.184
26 *Илић*, Г.П. *et al*, *Коментар Законика о кривичном поступку*, Службени гласник, Београд, 2013, p.725
27 Criminal Procedure Code, Article 419, paragraph 2 of the same Article anticipates that the Court is obliged to draw a conclusion about the existence of a certain fact based on conscientious assessment of each piece of evidence individually and in relation to the other pieces of evidence.
28 Срзентић*et al*, *Кривично право Југославије,* Савремена администрација, Београд, 1997, p.404

has been replaced by passivity of the judge regarding evidence, who as an impartial arbitrator does not determine facts or present evidence past the initiative of the parties. Here we have in mind the ordinary criminal procedure in which the parties were allowed more freedom in terms of impact on the fact to be determined in the process. On the other hand, the plea bargain as a form of simplified procedural form, first the confession of the accused, then his agreement with the prosecutor regarding the facts stated in the description of the offense, eliminate the need to prove them. In addition to the defendant's confession, existence of any other evidence which was not in opposition with it would be enough; instead of requiring the existence of evidence to support the given confession.[29]The hearing at which the decision on the agreement is made is held in closed session. The right of the accused (defendant) to a public trial is proclaimed by the international and national documents. The principle of the public has the rank of constitutional principle. Both the RS Constitution Article 142, paragraph 3 provides that the Court hearing is public, but it may be restricted only in accordance with the Constitution.[30] Since this is a special type of procedure which does not necessarily result in acceptance of the agreement in this respect, it requires a certain vigilance to protect the rights and interests of the defendant. In case of refusal or rejection of the agreement, the procedure returns to step preceding its closing. In view of the confession, the public would create a negative image of the defendant, which would further aggravate an opportunity for the charges in the contradictory procedure.[31]

Sentencing means determining the type and length of sentence to be imposed on the perpetrator of a crime. A system of relatively defined penalties has been adopted in our country, as well as in most modern laws where the legislator determines the type of punishment and its minimum and maximum amount for each criminal offense, thus providing limits within which the court will move when pronouncing the sentence in the particular case. According to Article 54 of the Criminal Code of the Republic of Serbia it is stipulated that the court would sentence the offender within the limits prescribed by law for this act, bearing in mind the purpose of punishment and taking into account all the circumstances which influence the sentence to be longer or shorter (mitigating and aggravating circumstances), in particular: the degree of culpability, the motives to commit the offense, the degree of danger or injury to the protected good, the circumstances under which the offense was committed, the past conduct of the perpetrator, his personal situation and his conduct after the offense, especially his attitude towards the victim, and other circumstances describing his personality.[32]Since the type of punishment or other criminal sanctions are "negotiated" by the agreement and its refinement by the court, it can be said that the provisions of this Article shall be hardly applicable to the plea bargain when it comes to judicial sentencing since no evidence is presented upon which a court would specify the sentence. Primarily, we can speak about prosecutorial sentencing, where the plaintiff is in better position in relation to the judge to get an insight (through informal conversations with the defendant) into his personality, the circumstances under which the offense was committed and others.

29 Шкулић, М.,*op.cit,* p.223
30 Article 315, paragraph 3, Criminal Procedure Code.
31 Илић, Г.П.,. *et al,op. cit.*, p. 726.
32 Article 54, paragraph 1 of the Criminal Procedure Code.

## CONCLUSION

Within the plea bargaining, first the confession of the accused, then his agreement with the prosecutor regarding the facts stated in the description of the offense eliminate the need to prove them. This certainly contributes to efficiency, as this significantly shortens the procedure, reduces costs and contributes to relieving the courts. Tax offences are specific of the process of proving, which is very complex and time-consuming, and judges are required, in addition to the role of financial experts, to have certain knowledge in this field. Viewed from a financial point of view, the state will hereby quickly get to the revenue generated by the payment of fines. Indeed, according to the amount in most cases in practice, they are far below the amount that would be collected if tax evaders paid tax on time. But in a situation where the payment of taxes is omitted (not paid), simplified form of criminal procedure allows faster collection of fines.

Significant objections can be made to the implementation of the plea bargaining in the field of tax evasion.

Surely, the state in this way quickly comes to revenue from the collection of fines, but it can be assumed that these penalties are far below the amounts which the court would pronounce if it conducted a regular criminal proceedings. The plea bargaining is nothing else but a certain "bargain" of tax evaders with the public prosecutor. In assessing the current situation (taking into account the evidence available to it, the need to "solve the case", etc.) with the demonstration of good will of the perpetrator, the public prosecutor will go on accepting lower fines. In any case, the actions of the public prosecutor are limited by the criminal policy of the court; otherwise, the sense of negotiating of the tax evader who strives to get a more lenient punishment would be lost.

In addition to complaints, which may be made in respect of all criminal offenses, such as the realization of the principle of truth in fair criminal proceedings, the question of the realization of the purpose of punishment is of particular importance for the tax evasion. It is a very socially dangerous behavior, since it violates the fiscal interests of the state. Only the timely payment of taxes and other public revenue ensures continuity in the financing of public needs, and thus the regular functioning of the state. In addition, by taking measures that all taxpayers fulfill their tax obligations, the conditions for tax fairness are provided. Otherwise, the tax burden would be borne by a conscientious taxpayer, while tax evaders would be privileged. Therefore, to ensure fiscal discipline it is very important to strengthen tax morality through expressing social condemnation for non-compliance with tax laws. Provision of appropriate penalties should prevent taxpayers to commit crimes. The imposition of appropriate penalties should affect tax evaders not to make them in the future, and stop motivating them to continue their criminal career. In addition to the aforementioned, special prevention and general prevention are extremely important as regards tax crimes. Punishment of tax evaders should affect other taxpayers not to commit criminal offenses of tax evasion.

Instead of the traditional sentencing by the court, taking into account aggravating and mitigating circumstances within the limits of the punishment prescribed by law, the implementation of the plea bargaining involves prosecutorial sentencing. When arranging the sentence, the public prosecutor shall be guided by the circumstances that affect the sentence. Thus, e.g. he should take into account the past conduct of the perpetrator, or whether that person was convicted in the past, his conduct after the commission of the crime, or whether he paid tax afterwards. If the person is a repeat offender, that represents an aggravating circumstance and the public prosecutor in this situation does not go below the legal minimum. In practice in some courts in Serbia there are known cases of professional tax evaders, people

engaged in certain activities to commit tax crimes who establish companies that make a false VAT invoice.

Unlike judicial sentencing, which is within the limits prescribed by law, in the plea bargaining the public prosecutor according to the law is not bound by the statutory minimum. The provision that the agreed penalty may not be below the minimum prescribed for the offense the defendant had been charged with, was deleted from the original version that was in effect from the introduction of this institute. This means that the public prosecutor for the most severe form of tax evasion (where the amount of unpaid tax exceeds 7 500 000 dinars), for which a prison sentence of 2 to 8 years is prescribed, can negotiate a reduced sentence or even house arrest because it can be determined in cases of imprisonment up to 1 year. In fact, it comes to lowering the penalties far below the prescribed ones. This cannot have a positive effect not only on special but also on general prevention. In addition to the already existing bad tax morale and a low level of tax awareness in our country, this application of prescribed regressive measures can only contribute to a greater breach of tax regulations. This can be an incentive to tax evaders to continue their criminal activities. It may also have a negative psychological effect on other taxpayers, because it can lead to the effect of the so-called "looking up to" tax evaders who go unpunished or with very small fines.

A special segment of the problem of applying repressive measures is the fact that the public prosecutor is bound by the criminal policy of the court. When concluding a plea bargaining we can move only within the boundaries of criminal policy. This means that the public prosecutor will be limited regarding the maximum sentence because he can negotiate just as much as the court would prescribe for that crime. In fact, an upper limit for the public prosecutor is not the maximum penalty prescribed by law for tax evasion, but the one imposed by the court. Furthermore, a lower limit for the public prosecutor is not the minimum penalty prescribed by law for tax evasion because he can go in arranging the sentence below the prescribed minimum. This can mean only one thing that the current lenient penal policy for tax evasion can only be more lenient because the penalties can only go down. Lenient punishment of tax evaders is not desirable not only from the aspect of not special, but also from the point of general prevention. Hence, the legislator should, starting from the theoretical knowledge and practical experience of other countries and taking into account our circumstances, review the existing provisions governing its implementation. In this sense, a recommendation can be made to bring back the deleted provision to the legal text, which stipulates that the agreed penalty may not be below the minimum prescribed for the offense for which the plea bargain is signed.

## REFERENCES

1. Анђелковић, М., Димитријевић, М., *Пореско право Србије*, Ниш, 2009
2. Анђелковић, М., *Деформације пореског односа,* Правни живот бр. 10/1997
3. Анђелковић, М., *Моделирање понашања пореских обвезника у савременој теорији,* Међународна научна конференција "Правни систем и друштвена криза", Правни факултет Универзитета у Приштини са привременим седиштем у Косовској Митровици, 2011
4. Анђелковић, М., *Редифинисање пореских односа*, Заштита људских и мањинских права, Тематски зборник Правног факултета у Нишу, 2015,

5. Damaska, M., *Negotiated Justice in International Criminal Courts*, World Plea Bargaining-Consensual Procedures and the Avoidance of the Full Criminal Trial, Carolina Academic Press, 2010

6. Димитријевић, М., *Значај кооперативности пореских обвезника у савременом пореском систему,* Зборник радова "Право Републике Србије и право ЕУ - стање и перспективе"

7. Ђурђић, В., *Споразум о признању кривичног дела - форма за изрицање правде или за решавање спорова*, Зборник радова са научне конференције: Људска права између идеала и изазова садашњости, Правни факултет Универзитета у Приштини, Косовска Митровица, 2016

8. Ђурђић, *Перспектива новог модела кривичног поступка Србије,* Журнал за криминалистику и право, Београд, 20.2, 2015

9. Jelčić, B. *et al*, *Financijsko pravo i financijska znanost,* Narodne novine, Zagreb,2002

10. Милошевић, Г., *Економски аспект евазије пореза,* Економски хоризонти, 2006, 8, (1-2)

11. Кнежевић, С., *Основна начела кривичног процесног права*, СКЦ, Ниш, 2012

12. Илић, Г.П. *et al*, *Коментар Законика о кривичном поступку*, Службени гласник, Београд, 2013

13. Раичевић, Б., *Јавне финансије,* Економски факултет, Београд, 2008

14. Поповић, Д., *Коментар Закона о пореском поступку и пореској администрацији*, Cekos in, Београд, 2003

15. Haller, M., *Plea Bargaining: The Nineteenth Century Context*, Law & Society Review, vol. 13, no. 2, 1979

16. Срзентић *et al*, *Кривично право Југославије,* Савремена администрација, Београд, 1997

17. Шкулић, М., *Однос начела истине и поједностављених форми кривичног поступка*, Поједностављене форме поступања у кривичним стварима – регионална кривичнопроцесна законодавства и искуства у примени, Мисија ОЕБС, Београд, 2013

## LEGISLATION

1. Кривични законик Р Србије, "Сл. гласник РС" бр.85/2005, 88/2005-испр., 107/2005-испр., 72/2009, 111/2009, 121/2011, 104/2013, 108/2014.

2. Закон о пореском поступку и пореској администрацији Републике Србије ("Сл. гласник РС", бр. 80/02, 84/02 - испр., 70/03, 55/04, 61/05, 85/05 - др. закон, 62/06 - др. закон, 61/07, 20/09, 72/09 - др. закон, 53/10, 101/1, 2/12 - испр., 93/12)

3. Законик о кривичном поступку ("Службени гласник РС", бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014)

# ORGANIZATION OF THE POLICE SYSTEM IN BOSNIA AND HERZEGOVINA

**Dragomir Jovičić, PhD**
Facultyfor Security Studies, Banja Luka
**Gojko Šetka, PhD**
College of Internal Affairs, Banja Luka

**Abstract:** The police system in Bosnia and Herzegovina is a complex uncoordinated police system, which, as such, inevitably presupposes a conflict of jurisdiction and problems between police agencies that comprise it. The paper discusses the circumstances that gave rise to the formation of the police system and its design. It focuses on the way this police system is organized and explains its complex organizational structure. Besides the aforementioned, according to the specifics of the police system in Bosnia and Herzegovina, we analyze its functionality and efficiency, but also explain the problems that occur in its functionality and efficiency. This paper presents some specific practices that best reflect the real situation in the current system of the police in Bosnia and Herzegovina. The authors offer practical solutions that would lead to an increase in functionality and efficiency of the police system. As possible solutions to the current problems in the functioninf of the police system, we will give examples of organization and functioning of some of the modern police systems in the world, which could serve as an example for the organization of the police structure in Bosnia and Herzegovina.

**Keywords:** police system, organization, functionality, jurisdictional disputes.

## INTRODUCTION

Security is one of the priorities of every society since its inception, and its implementation is one of the basic functions of the state. State security function is realized by a larger number of subjects, however it is certain that one of the most important and most visible is police. It is clear that any authority to accomplish its business in an efficient manner must have an adequate organization. Therefore, every country organizes police structure to protect its constitutional order, its internal security, and enables the achievement of guaranteed rights and freedoms of its citizens."The organization itself is a dynamic category, and, accordingly, those involved in the organization constantly invent new rational solutions through which they can make a bigger impact with the least expenditure of funds and personnel."[1]Thus, each country tends to its police to be organized so that the most efficient and best way performs its responsibilities.

Organization of the police structures in a country may vary from country to country. Currently in the world there aren't two countries that have identical organization of the police. ''Matched organizational solutions virtually do not exist. Some of the solutions are centralized and the other predominantly decentralist.Regardless of the fact that there is no country with an identical organization ofpolice structures, we can say that in all countries same factors have

1 Jovicic, Dragomir, Origin and Development of the Ministry of Internal Affairs of the Republic of Srpska, Journal ''Safety, Police, Citizens", Ministry of Internal Affairs Republic of Srpska, no. 1/05, Banja Luka, 2005, p. 20.

the impact on the police organization."[2] First of all, we are referring to the following factors: the specific form of political organization of the state, territorial organization (division) of the state, the reasons of traditional nature (historical heritage), cultural heritage, economic and social status of the state, the state legal system, security system, etc. In addition to these factors, the police organization may be affected by the security situation in a country and its environment, problems in the area of crimes and misdemeanors, the new forms of threats to security and others.[3]

Given the complex state organization of Dayton Bosnia and Herzegovina, the current political relations in BiH, developments in the region in recent decades (the civil war in Bosnia-Herzegovina between its peoples and the dissolution of the former common state, and changing socio-political and economic systems), impact of the international factors (the imposition of certain legal solutions in the field of organization of the police system) Transition, which is a constant process in Bosnia and Herzegovina (primarily reflected in the frequent changes in regulations and the reorganization of state authority), contempt of the Constitution regarding the division of responsibilities in the area of police operations between the entities and joint bodies at the state level, it can be said that in BiH established police system is faced with a number of everyday problems. Such a police system often brings confusion in the conduct of police agencies which are existing in the system itself, therefore there is a lot of room for manipulation, political influence (political manipulation of the police), contributes to the inertness of the police structures, large financial allocations from the budget, and certainly have a negative impact on the security situation in Bosnia and Herzegovina.[4]

Starting from different theories in domestic and foreign literature we can find different classifications of the police systems. Classification of the police systems depends on various factors and the contribution of these different attitudes and practices of the police conduct and attitudes of scholars who work in this important area. For the purpose of this work the most interesting division of the police system is the complex coordinated and uncoordinated complex police systems. The division of the police system in the complex coordinated and uncoordinated complex police system is based on the manner in which is conducted the territorial division of the responsibilities between different police organizations."If territorial jurisdictionsare divided in that manner that for every part of the territory responsible there is only one of the police organizations, we also have a case of a complex coordinated police system; conversely, if for the same parts of the territory is competent more than one police organization, we have the case of complex uncoordinated police system."[5] So, the basic characteristics of complex uncoordinated police system are reflected in the concurrent jurisdiction of several separate police agencies for parts of the same territory.[6]Theoretically, the BiH police system can be defined as a complex uncoordinated police system which consists of several police organizations, some of which are simultaneously responsible for the same parts of the territory of Bosnia and Herzegovina. This practice creates problems and is one of the key factors that affects the functionality of the police agencies.

2 Miletic, Slobodan, Police Law, Police Academy, Belgrade, 2004, p. 108.
3 Setka, Gojko, BiH police system between their functionality and dysfunctionality, Conference Proceedings of the International Scientific Conference: Archibald Reiss Days, Police Academy, Belgrade, 2016, p. 193.
4 Setka, Gojko, Impact organization of police structures in BiH in the security situation, the Faculty of Security and Protection, Banja Luka, 2016, p. 29.
5 Milosavljevic, Bogoljub, Police Science, Police Academy, Belgrade, 1997, p. 360.
6 Jovicic, Dragomir, Setka, Gojko, Organization and competence of the police, Faculty of Security and Protection, Banja Luka, 2015, p.80.

# THE CONSTITUTION OF BOSNIA AND HERZEGOVINA AND FIELD OF INTERNAL AFFAIRS

The Constitution of Bosnia and Herzegovina, defines the organization of government and public authorities and thus naturally law enforcement agencies, but also it represents a part of the General Framework Agreement for Peace in Bosnia and Herzegovina. ''There is almost no examples in international law and international treaties and agreements that as part of, or annexes of the agreement, the parties ensure the constitution."[7] Agreeing with this statement, we need to point out that the Constitution is the only example in the world, which is a product of international law, namely the peace agreement and as part of it. Characteristic for the organization of the police agencies in Bosnia and Herzegovina is that it is based on the Constitution of Bosnia and Herzegovina stipulates that the entities responsible for internal affairs, and that they , without changing the constitutional provisions, formed police agency at the state level institutions involved in police affairs. These agencies are mostly formed under the laws imposed by the High Representative in Bosnia and Herzegovina. ''According to the Constitution of Bosnia and Herzegovina (art. 2), establishing the list of responsibilities of institutions of Bosnia and Herzegovina and the responsibility of the entities list. It is very important to point out that the constitution has embraced the solution in which the assumption is that the jurisdiction should be based in ordered to serve the particular entity.In Article 3, item 3a of the Constitution stipulates that all governmental functions and powers conferred by this Constitution are not expressly assigned to the institutions of Bosnia and Herzegovina, but it will belong to the entities."[8] So, as in the Constitution of Bosnia and Herzegovina, when you see what those competencies are enumerated that are located in the authority of the common Bosnia and Herzegovina institutions, does not include internal (not even the police work) activities, in general clause which is provided in the constitution It is absolutely clear that we can conclude that they are in the jurisdiction of the entities. So, contrary to the provisions of the Constitution of Bosnia and Herzegovina at the level of the common institutions of Bosnia and Herzegovina have established police organization. ''Characteristic of violations of the Constitution of Bosnia and Herzegovina in the field of transfer of jurisdiction of security from the entities to the level of Bosnia and Herzegovina institutions, as a result can, and does, jeopardize the security situation in Bosnia and Herzegovina and the disruption of the overall security of the implications of the political, economic, social relations, destruction of property, and other forms of instability. Perhaps one of the greatest negativities expressed is the 'passivity' the 'police authorities, which could be established, but is invisible in ordinary observation."[9]

So part of the police system which now operates in Bosnia and Herzegovina was established opposite to the provisions of Bosnia and Herzegovina. By saying this we mean the police agencies that have been established at the level of the common institutions of Bosnia and Herzegovina. We can say that this kind of awkwardness is unique compared to all regulated countries in the world, because in those countries the organization of the police system complies with the constitutional provisions. In practice, this anomaly is the real major problem in the functioning of the police structures in place and partnerships between law enforcement

7 Dmicic, Mile, Political and legal character of the Dayton Peace Agreement and the constitutional order of Bosnia and Herzegovina, the Journal Defendologija,Defendology Center for Security, Sociological and Criminological Research, no. 21-22, Banja Luka, 2008, p.12.
8 Jovicic, Dragomir, Organization and jurisdiction, Faculty of security and Protection, Banja Luka, 2011, p. 307.
9 Karan, Sinisa, The responsibilities of institutions of Bosnia and Herzegovina in the area of security, Journal ''Safety, Police, Citizens", Republic of Srpska Ministry of Internal Affairs, no. 1/08, Banja Luka, 2008, p. 104-105.

agencies, it produces a competitive relationship. Here we should also point out that those who support this way of the establishment and functioning of the police agencies to justify the fact that the laws underlying this Agency, after the imposition of the High Representative passed the adoption procedure in the Parliamentary Assembly of Bosnia and Herzegovina, and that it was voted for by representatives of all nations.Of course it is not in this fact, that we can seek support for the legality of these agencies, and therefore not for their operation, for the simple reason that they continue to infringe upon the Constitution of Bosnia and Herzegovina, since there has been no change in the Constitution, which would give a legal foundation for the existence of these agencies and, as things are at this moment, it is not realistic to happen, not only in the near future, but it seems that this will never be achieved by consent of the constituent nations.

## ORGANIZATION OF THE POLICE SYSTEM IN BOSNIA AND HERZEGOVINA

The establishment of the police system in Bosnia and Herzegovina characterizes many decisions that go against the functioning of the legal system. This claim is based on the decision on the establishment of police agencies at the level of the common institutions of Bosnia and Herzegovina, as we have already explained, contrary to established Provisions of Bosnia and Herzegovina and on the basis of the decisions of representative of the international community.

''Following the conclusion of the Dayton Peace Agreement in Bosnia and Herzegovina there were only entity police forces which are in accordance with the Constitution of Bosnia and Herzegovina. As the Dayton peace agreement provided for the establishment of international police forces IPTF who initially had a role to supervise the work, provide assistance and advice to local police agencies, and later in the sessions of the Peace Implementation Council, these responsibilities have been significantly expanded, and the IPTF accordingly, to these facts started to behave.This expansion of jurisdiction included the reorganization and restructuring of the police agencies, as the IPTF during its mandate was doing. ''[10]

It was in this period when the IPTF performed tasks entrusted to it by the international community police organizations,at the state level contrary to the Constitution of Bosnia and Herzegovina, were established. First of all, the State Border Service was established (2000), later renamed the Border Police of Bosnia and Herzegovina (2004), then they established the Information and Protection Agency (2002), which later changed its name to the Agency for investigation and protection and received police powers (2004). During this period they established the police of Brcko District.Prior to these agencies, they established the Office of Ineterpol, which is in contrast to the aforementioned Agencies in accordance with the division of responsibilities between the Bosnia and Herzegovina and the entities according to the constitution of the Bosnia and Herzegovina. In the last year the mandate of the UN mission, by the IPTF, an analysis of all police organizations and their accreditation, and certification of all members of the police organization was arranged. ''But it happened that after the end of the UN mission for the first time in the history of international organizations after this mission established a new mission, as we know, the EU mission, which largely ignored everything that and all the work that was done under the UN mission , at least when it comes

10 Jovicic, Dragomir, Impact of the police reform in the security situation in Bosnia and Herzegovina. In: Conference Proceedings: Safety and protection in the Republic of Srpska and Bosnia and Herzegovina - status and perspectives, Faculty of Security and Protection, Banja Luka, 2008, p. 112.

to law enforcement institutions."[11]This was the prelude to the new reforms which brought with them the establishment of the Ministry of Security of Bosnia and Herzegovina which are incorporated Bosnia and Herzegovina State Border Service, State Information and Protection Agency and the Office for Cooperation with Interpol office in Bosnia and Herzegovina. The effect of this mission required the new reform process.

Today in Bosnia and Herzegovina police structure is organized as follows: in the Republic of Srpska there is only one police organization - Police of the Republic of Srpska, in the Federation of Bosnia and Herzegovina there are: the cantonal level of police forces, that is ten cantonal Ministries of Internal affairs and entity-level Ministry of Internal Affairs of the Federation of Bosnia and Herzegovina, and in Brcko district police operations conducted by the police of Brcko district.At the level of the joint state institutions that were established and now exist within the Ministry of Security of Bosnia and Herzegovina there are following agencies: Border Police, State Investigation and Protection Agency, Directorate for Coordination of Police Bodies, Service for Foreign Affairs, the Agency for Education and Professional Training Agency for forensics and the Agency for police support. It should be noted and emphasized that this agency within the Ministry of Security functions as independent administrative organization. This implies that each agency is independent in its operational work, and that the functioning of such a "system" (referring to the BiH Ministry of Security) corresponds to the Minister of Security. Taking into account the complex organization of the Bosnia and Herzegovinapolice system and a complete environment in which the system exists (turbulent past in Bosnia and Herzegovina, the current problems in the sphere of social, political, economic and other relations) we can say that such police system is organized in such way that is much more closer to be very dysfunctional than rather to be functional.

We claim this partly because of the results of research[12], which showed that there is a negative perception and confidence of Bosnia and Herzegovina citizens in the police structure. Therefore it is determined by the negative impact of the organization itself of police structures in Bosnia and Herzegovinain the security situation, which is reflected in distrust of citizens towards the police structure in BiH, feeling of insecurity (vulnerability) of citizens of Bosnia and Herzegovina, a large number of offenses under unknown crime scenario (especially in the field of economic crime), a large number of rejected reports about the crime committed by the Prosecution Officers which are submitted by the police agencies in Bosnia and Herzegovina judicial authorities (according to official data Prosecution of Bosnia and Herzegovina in the last five years, the percentage of rejections of reports about crime is more than 30%), the perception of corruption levels in the police structures by the citizens of Bosnia and Herzegovina, the inefficiency of police work, lack of professionalism in the conduct of members of the police structures in Bosnia and Herzegovina, conflicts of jurisdiction between the police agencies that work in various jurisdiction on the territory of Bosnia and Herzegovina, the competitive relationship between the police agencies and so on. In any organization one of the most important issues is the question of the division of labor within the organization between the lower organizational parts of the organization, which is a larger organization, this issue is even more important. The police is the most numerous in the work of public authorities, which is to say that it is one of the major organizations and is taking into account

11 Jovicic, Dragomir, Impact of the police reform in the security situation in Bosnia and Herzegovina, Conference Proceedings: Safety and protection in the Republic of Srpska and Bosnia and Herzegovina - status and perspectives, Faculty of Security and Protection, Banja Luka, 2008, p. 112-113.
12 Primarily referring to research conducted by the Faculty of Security and Protection Banja Luka in 2013 titled: Public perception of the state of security and confidence in the safety of subjects; and research that was conducted in 2015 as part of a doctoral dissertation, PhD. Gojko Setka titled: Impact of organizations granting police structures in Bosnia and Herzegovina on the security situation.

the nature of the tasks that are the responsibility of policing is crucial to regulate the division of responsibilities between the different parts of the police system in Bosnia and Herzegovina.

It is completely founded the claim that the police model inBosnia and Herzegovinaso poorly organized that it can not be functional not even assuming that in Bosnia and Herzegovina there are no national, political or any problems, and we know what burdens the Dayton Bosnia and Herzegovina, then to everyone who understands the organization of the police, it is clear that as long as we do not change the concept of the organization and functioning of the police agencies, Bosnia and Herzegovina citizens will not have the quality service of this important state body. The best example of dysfunctional police organization is a terrorist act, in which two members of the Armed Forces were killed in Rajlovac, and it took half a day to MUP FBiH ( Ministry of internal affairs of Federation of Bosnia and Herzegovina) and Cantonal MUP Sarajevo to reach an agreement, as in this particular case it was unclear who would conduct the investigation. What kind of serious police work can be expected then if within the Federation of BIH two police agencies cannot agree on who will conduct the investigation. So, the solution is to change the concept of action and clearly determine who does what, when the agency is responsible for something and when and under what conditions it can include another.

As an example for overcoming the problems in the organization and functioning of the Bosnia and Herzegovina police system can serve examples of the organization of the police system of Germany and Switzerland. These systems, are a good example because these systems have different levels through which it is established an extremely efficient police system, and on the other hand the actual police authority is located in the lower territorial units, as provided in the Constitution ofBosnia and Herzegovina. The key thing that has to be taken out of the police system is a way of functioning and the relationship between law enforcement agencies in solving practical problems. This refers to situations where the police structure with a higher level of its tasks should be performed on the part of the territory that is under the jurisdiction of another territorial police structures (territorial police forces in Germany or the cantonal police in Switzerland). In these countries it is clearly established rule of law enforcement agencies from the federal level, must inform of their activities the competent local police agencies at a lower territorial level, and under their supervision perform their duties.

As an additional argument the need to recompose the way of action of the police in Bosnia and Herzegovina in accordance with positive European practices (in the first place we think of Germany) is also a fact that a similar mode of operation was in force before the war at the time of the existence of the former common state. Even though we were lived in a state of '' brotherhood and unity '', it was not possible for anyone from the police authority of a higher level to appear at the local level without the knowledge of the police from the local level, nor was it possible to undertake any kind of police measures and actions without the participation of the police officers from the local level. Therefore the right question to ask is why anyone thinks that this is possible in today's Bosnia and Herzegovina, after everything that has happened in the recent past? Thus, the decision to establish a more efficient, simpler and of course much cheaper police system is quite clear, as with this current system there is no way to put any ethnic group in Bosnia and Herzegovina in an unequal position, but to make this happen requires political will that is for now not quite possible.

## CONCLUSION

Generally, watching the police organization, as state authorities responsible for the realization of the security, it can be said that it has the biggest impact on the security situation with the prevention and repression of the crime. The efficiency of the police work in the prevention and repression of crime causes a variety of factors, including factors which play an important role with the organization of the process. We believe that a preventive and repressive activities of the police structures directly depend on the organization of the police personnel who manage the organization.Professional training of managers and workers, proper scheduling within the organization, respecting subordination and coordination in the police organization, inner police cooperation (both within the local community and at the international level), as well as all the factors previously listed (referring to the factors and problems affecting the organization of the police in Bosnia and Herzegovina). If there are problems in the prevention and repression of crime by the police structure, it can be concluded that the structure of a state police is not able to do everything to contribute to creating a favorable safety conditions. Unfortunately, now almost all key factors suggest that such an organized police system in Bosnia and Herzegovina does not have the ability to contribute to achieving full capacity of a favorable security situation.

There is no need to be an expert on police matters in order to to understand this fact to conclude that this inability of administration to exercise these important functions at the appropriate level in Bosnia and Herzegovinaat this pointstems from the unregulated relations between the various police agencies. In addition to the agencies,there are other problemsat the level of the common institutions of Bosnia and Herzegovina established in contradiction with the Constitution of Bosnia and Herzegovina. One of the more visible problems is the structure and position of the Ministry of Security. Specifically, the Minister of Security under the Council of Ministers is authorized to exercise political control over the work of police agencies within the Ministry, and it is clearly stated that there is no right to interfere in operational police work. Thus, someone who has no right to interfere in police work has the responsibility for the security situation, which of course is not sustainable.

All citizens regardless of all differences that exist between them (whether related to nation, religion, status, gender or any other feature) equally need security to be able to fulfil their needs and live without fear, enjoying a decent life in the twenty-first century. This basic social need of the citizens can be provided by a well-organized police service. Although a much broader elaboration is needed, this paper points out the way, taking into account best practices, as well as the specifics of Bosnia and Herzegovina, and point out to the need for establishing a police organization in Bosnia and Herzegovina that would be able to offer the necessary security to all its citizens.

## REFERENCES

1. Dmicic, Mile, political and legal character of the Dayton Peace Agreement and the constitutional order of Bosnia and Herzegovina, Journal ''Defendology", Defendology Center for Security, Sociological and Criminological Research, no. 21-22, Banja Luka, 2008,
2. Jovicic, Dragomir, Origin and Development of the Ministry of Internal Affairs of the Republic of Srpska, Journal ''Safety, Police, Citizens", Ministry of Internal Affairs Republic of Srpska, no. 1/05, Banja Luka, 2005,
3. Jovicic Dragomir, Setka Gojko, Organization and jurisdiction of the police, Faculty of Security and Protection, Banja Luka, 2015,

4. Jovicic Dragomir, Organization and jurisdiction of the police, Faculty of Security and Protection, Banja Luka, 2011,
5. Jovicic, Dragomir, Organization and jurisdiction of the police,Faculty of Security and Protection, Banja Luka, 2008,
6. Jovicic, Dragomir, Impact of the police reform in the security situation in Bosnia and Herzegovina,Conference Proceedings: Safety and protection in the Republic of Srpska and Bosnia and Herzegovina - status and perspectives, Faculty of Security and Protection, Banja Luka, 2008,
7. Jovicic, Dragomir, the Republic of Srpska police role in the implementation of the Dayton Peace Agreement, High School of Internal Affairs, Banja Luka, 2005,
8. Jovicic, Dragomir, Role of the Police of the Republic of Srpska the implementation of the peace agreement of Dayton Peace agreement, Faculty of Security and Protection, Banja Luka, 2007,
9. Karan, Sinisa, the responsibilities of institutions of Bosnia and Herzegovina in the area of security, Journal ''Safety, Police, Citizens", Ministry of Internal Affairs Republic of Srpska, no. 1/08, Banja Luka, 2008,
10. Miletic, Slobodan, Police Law, Police Academy, Belgrade, 2004,
11. Milosavljevic Bogoljub, Police Science, Police Academy, Belgrade, 1997,
12. Setka, Gojko, Impact on the organization of police structures in BiH in the security situation, Faculty of Security and Protection, Banja Luka, 2016,
13. Setka, Gojko, Vukovic, Mladen, Popovic, Predrag, Results of the police agencies and prosecutors' offices in Bosnia and Herzegovina as indicators of their expertise, Conference Proceedings scientific conference: Countering contemporary forms of crime - analysis of the situation, by European standards, measures promotion, Volume 3, The Academy of Criminalistic and Police Studies in Belgrade and the Hanns Seidel Foundation, Belgrade, 2015,
14. Setka, Gojko, Police system in Bosnia and Herzegovina between their functionality and dysfunctionality, Conference Proceedings of the International Scientific Conference: Archibald Reiss Days, Police Academy, Belgrade, 2016,
15. Setka, Gojko, Models police organizations and police system in B&H, Journal ''Safety, Police, Citizens", Ministry of Internal Affairs Republic of Srpska, no. 1-2 /16, Banja Luka, 2016,
16. Setka, Gojko, Llimitation policing system Bosnia and Herzegovina compared to nowdays security challenges, risks and threats, Proceedings of the Ninth International Scientific Congress: Days of safety on the topic: Contemporary security risks and threats and their influence on the security of the countries of the region, Faculty of Security and protection, Banja Luka, 2016.

# REPRESSIONOF CRIMINAL ACTS IN THE FIELD OF GREY ECONOMY IN THE REPUBLIC OF SERBIA[1]

**Dragan Cvetković, PhD**
*Police Directorate for the City of Belgrade, Criminal Police Directorate*
*cvetkovicdragan@mts.rs*
**Marija Mićović, PhD**
*Academy of Criminalistic and Police Studies, Belgrade*
*marija.blagojevic@kpa.edu.rs*
**Marta Tomić, PhD**
*Academy of Criminalistic and Police Studies, Belgrade*
*marta.tomic@kpa.edu.rs*

**Abstract:** Grey economy is undoubtedly one of the biggest problems of nowadays. In recent years, this phenomenon is increasingly being said of and written about as a negative social phenomenon that appears as a serious brake on both economic and general social development. Criminal offenses from the field of grey economy are a group of offences with a wide array of different manifestations that occur in almost all areas of economic activity. Grey economy is a phenomenon that has various consequences, both on the fiscal and socio-political plan, and the activities and behaviours that are aimed at not paying taxes often impair some social values, which must withdraw the corresponding reaction - whether at moral, whether in the legal field. It is one of the most widespread forms of financial indiscipline of legal entities in the Republic of Serbia, which is not only a problem of public finances, but also regarding respect for laws and ethical perceptions. The fight against tax evasion, as well as measures against grey economy, are the basic goals of the economic policy of all countries. The Republic of Serbia is making efforts to stall grey economy that reduces its budget revenue by one-third annually. In addition to determining the causes and manifestations of criminal offenses in the field of grey economy, we will analyse their participation in the mass of total or economic crime and the trends in the Republic of Serbia in the period from 2006 to 2015. The aim of the paper is to emphasize the significance of its suppression by analysing the causes and effects as well as the dynamics of this phenomenon.

**Key words:** grey economy, criminal acts, phenomenon, financial indiscipline, crime.

## INTRODUCTION

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.

To a greater or lesser extent grey economy is present in all countries, regardless of the type of society and the degree of socio-economic development.[2]Grey economy includes economic activities and generatesincome that circumvents or otherwise avoids regulations, taxation or monitoring by the competent authorities. From a statistical point of view, grey economy is classified as registered and unregistered, from a legal point of view to a legal and illegal one, from a fiscal angle to taxable, untaxable (but the tax authorities cover the entire income or part thereof) and the rest (for which there are clear tax regulations and which is done using gaps in legal regulations). A particularly big problem is black economy, whose conduct is related to criminal activities, which is also covered by this strategic document.[3]

Criminal offenses in the field of grey economy such as tax evasion, non-payment of tax on deduction, illicit trade, smuggling and unauthorized production destroy the principle of business and ethical norms, thereby destroying the economic, production and market environment of the state and at the same time challenging the realization of numerous state functions. They, as a possible consequence, have a total or partial avoidance of payment of taxes and other charges, making or submitting a forged document relevant for taxation, jeopardizing the collection of fiscal obligations and fiscal control, as well as unauthorized turnover of goods and services. This group of criminal offenses is extremely socially dangerous behaviour of individuals and groups, that is, legal entities, companies, institutions or other organizations that violate the regulations directly or indirectly endangering the financial interests of the whole community, primarily by causing great damage to the fiscal system and the public revenue system at all.

Grey economy, according to the MIMIC method, amounts up to 30% of the GDP in the Republic of Serbia, which makes us a country with an exceptionally high level of tax avoidance (the average in the countries of the region is around 22-33% of GDP, while the developed countries of Western Europe reach a figure of 15% GDP in the grey zone).[4] In order to reduce the participation of grey economy in the GDP of the Republic of Serbia, the Government of the Republic of Serbia adopted the National Program for Suppression of Grey Economy. It is about more efficient monitoring of grey economy flows, improvement of the functioning of the fiscal system, reduction of the administrative and para-fiscal burden for the economy and citizens and raising the citizens'awareness about the importance of combating grey economy.[5]

In order to examine the scope and dynamics of crimes in the field of grey economy and the characteristics of the criminal justice response to this phenomenon in Serbia, weneed to analyse the participation of this group of criminal offenses in total and economic crime and their dynamics in the period from 2006 to 2015. This period was selected as suitable because it is long enough to show certain tendencies in the dynamics of crime. In addition, it corresponds to the time since the beginning of the application of the Criminal Code, which was passed in 2005. These incriminated behaviours will be analysed based on the available statistical data, which, in addition to knowing the limitations and deficiencies in science, nevertheless represent an irreplaceable source of information on detected criminality.

## DEFINING GREY ECONOMY PHENOMENON

In exploring the grey economy phenomenon, it is of key importance to define the term. There are numerous and different definitions of the term "grey economy", and as synonyms

2 Socijalnoekonomskisavet RS (2010)*Efikasnosuzbijanjesiveekonomije*, Beograd: NIP Radničkaštampa, p.9.
3 *Nacionalni program zasuzbijanjesiveekonomije* "Službeniglasnik RS", broj 110 od 28. decembra 2015
4 *Nacionalni program zasuzbijanjesiveekonomije* "Službeniglasnik RS", broj 110 od 28. decembra 2015
5 http://www.srbija.gov.rs/

are often used: "informal economy", "concealed economy", "illegal economy", "unofficial economy", "irregular economy" and many others. Given that the term "grey economy" combines numerous economic activities, it is difficult to determine one official definition. For example, a distinction must be made between goods and services produced and consumed within home and illegal employment and social fraud, as well as criminal economic activities. Many scientific controversies and political discussions have been created due to several unsatisfactory definitions.[6] This is why it is necessary at the beginning to point out the most common definitions of grey economy among the leading researchers in this field.

According to the Economic Dictionary[7] informal economy is "part of the economy that characterizes irregular and illegal business. It can be viewed as a grey economy, or business that can be legalized by undertaking certain actions (for example, paying taxes), and a black economy that cannot be legalized (for example, drug trafficking). All countries are implementing measures to curb it in order to increase tax revenues."The definition of Canadian economist Adam Smith[8]is interesting, who definedgrey economy as "market based production or service provision, lawfully or illegally, but in such a way to avoid detection in official estimates of gross domestic product".

The group of authors, however, agree that grey economy is "a series of economic activities and the acquisition of income by avoiding official legal regulations, paying taxes and insight into business".[9]

It can be seen that grey economy implies undeclared income from legal income acquisition, whether it is monetary activity or commodity exchange, and these revenues would certainly be taxed to be reported to the competent tax authorities.

## BASIC CAUSES AND CONDITIONS OF GREY ECONOMY

The growth of grey economy is, of course, in some way a necessary companion of the transition process. An informal economy does not arise by chance and by itself but is already a reflection of the imperfection of the state apparatus and the inadequacy of the politics, especially economic ones. Factors that affect its formation, creation and development are very numerous and complex. The consequences of this phenomenon are: unfair competition caused by entities operating in the grey economy zone, which leads to the closure of business entities that comply with regulations or their transition to grey currents, layoffs and investment cuts; lower budget revenues that cause worse public services such as education, health care, security, rule of law, utility services, etc.; infringement of the rights of persons engaged in work, safety and health (absence of payment of contributions for pension and disability insurance, health insurance and unemployment insurance, insurance in case of work injury for students engaged through student cooperatives, endangered quality and health safety of products).

Based on the analyses carried out,10 the following basic causes of grey economy have been identified: low level of tax culture of citizens and state economy, mainly caused by mistrust in state institutions, non-transparent spending of resources, insufficient information

6 Nikolić, Đ., Čudan, A., & Đorđević, B. [2016]. *Carinski organi u funkciji suzbijanja sive ekonomije*. Nauka, bezbednost, policija, 21(2), pp. 159-180

7 *Ekonomski rečnik* (2006) EkonomskifakultetUniverzitetauBeogradu, Beograd,pp. 463.

8 Smith, P. (1994), 'Assessing the size of the underground economy: the Canadian statistical perspectives', Canadian Economic Observer, Catalogue no. 11–010, pp. 16–33

9 Dell'Anno, R. (2003), 'Estimatingtheshadoweconomy in Italy: a structuralequationapproach', WorkingPaper2003–7, Department ofEconomics, UniversityofAarhus; Fleming, M.H., J. Roman and G. Farrel (2000), 'Theshadoweconomy', JournalofInternationalAffairs, 53(2): pp.64–89

10 *Nacionalniprogramzasuzbijanjesiveekonomije* "SlužbeniglasnikRS", broj 110 od 28. decembra 2015

and corruption, complicated regulatory framework subject to frequent changes, inconsistent implementation of regulations, insufficient knowledge of regulations and weak capacity of public administration in implementing regulations; relatively high tax and non-tax burdens with additional administrative barriers and high administrative costs for business and retail; relatively high level of corruption and state tolerance towards grey economy (inspections, customs, judiciary, police), high unemployment and poverty.

The most important factors of the expansion of the grey economy in the Republic of Serbia include:11 a great reduction in production and aggregate supply; high unemployment; low standard of living; the emergence of a large number of refugees and displaced persons who cannot resolve their status; a multitude of mixed households, whose members work in the social sector of the economy; distrust of the citizens in the banking system; deplorable fear of inflation; relatively mild punitive policy and inefficient functioning of state bodies; tolerant attitude of authorities, especially according to the grey economy segment in which foreign trade is being carried out; inconsistency and instability of legal regulations.

The growth of the underground economy is also caused by the emergence of various factors, among which are the growth of tax burden and contributions for compulsory social insurance, strengthening regulations related to the economy and the labour market, forced reduction of working hours, early retirement, unemployment, and weakening civic awareness, non-devotion to public institutions and tax morality.

It is interesting to see that many grey economy actors decide to perform legal activity in a hidden form for various reasons. Schneider lists12 four common reasons: - avoiding payment of value added tax or any other tax; - avoiding payment of social security contributions; - avoiding the application of prescribed standards (minimum wages, maximum working hours, occupational safety and the like), and - avoiding the implementation of prescribed administrative procedure (sending statistical reports on business).

Therefore, the causes of grey economy are different, starting from general social morality and economic situation in the country, the extent of grey economy and the prevalence of corruption, the amount of tax burden, the tax form, the efficiency of the control of tax authorities, the severity of penalties and their consistent application to the purpose of evaded funds. If the state of economy of a country is more stable, the less reason there is for taxpayers to avoid paying taxes. However, in the countries where the economic crisis prevails crime is higher. The bigger the crisis, the bigger the opportunities to avoid paying taxes. Therefore, grey economy has an undeniable effect on deterioration of the overall macroeconomic situation, and to the Serbian economy as well.

## SEVERAL FORMS OF GREY ECONOMY

Grey economy implies carrying out economic activities beyond the relevant legal regulations. It appears in various forms, in almost all areas of the economy and beyond. In the countries in transition the dual economy is flourishing. In the economic realities of these countries, given the great changes that these countries are experiencing, it is a very pronounced phenomenon. It is much of a form of informal economy. For an effective fight against it, it is very important to know all these forms. The effective measures of the competent authorities depend directly on the knowledge of all areas of the informal sector.

11 Kulić M. ‘’Poreska utaja i krijumčarenje” BMG, Beograd 1999. pp. 45-56
12 Schneider, F.: The Shadow Economy in Germany: ABlessing or a Curse for the Official Economy, *Economic Analysis and Policy*, Vol. 38, No. l, March (2008), pp. 90.

The modernization of a society also changes the forms and ways of performing such offences. The rapidly changing forms that are very difficult to detect make the state administration effort more difficult. The grey economy in Serbia appears in various forms and in almost all areas of economic activity. So we can list some of them:[13] illegal import and export; withdrawing and retaining cash outside the payment system; sale of cash without recording traffic; the movement of goods in a legal or illegal place without proof of origin; distribution of illegal and unregistered goods and services; avoidance of taxes; illegal production; incomplete inclusion of income of agricultural holdings as well as incomplete inclusion of income from agriculture; illegal construction; unlawful appropriation of common premises in residential buildings and their upgrading for personal needs; speculation in the real estate market; machinations in the privatization process; unauthorized trade in excise goods; illegal logging of state forests and usurpation of public goods; hiring workers without contract, and many others;

One of the most common forms of grey economy are criminal acts which include employment without contract and their not being registered for social and health insurance, as well as the registration of employees at the statutory minimum wage, while part of the salary is paid "cash in hand". In this way, employers save on the taxes and contributions should be paid to the state, having in mind that they are calculated as a percentage of the "official" salary of the workers. The second most common form of grey economy is the sale of goods and services without supporting documentation and the issuance of fiscal accounts. In the grey zone excise products such as alcohol, cigarettes, tobacco and fuel are mostly traded, where tax revenue is the largest, and the most common places are sales in markets, undeclared shops, or street stalls. Informal trade, or the purchase of products without adequate control before release into the market, can have negative consequences for the health of the population, general safety and the functioning of the state.

From the foregoing it is clear that in practice the most varied forms of grey economy are encountered in practice. There are various ways for the execution of this group of criminal offenses. Knowing the method of their execution is necessary to effectively take measures by the competent authorities in order to suppress these acts. These modes are rapidly changing and are difficult to detect. In practice, this group of criminal offenses can be very difficult to detect and prove, first of all, because their perpetrators are connected, have expertise, and the place of execution is not only related to one legal entity, but to several legal entities, while they are working to conceal criminal activities whichcreates an illusion of legal business, with the help of falsification of documentation. Therefore, it is very important to respond in time and find documentation, internal records, as well as other evidence, in order to be expertized later on. Otherwise, the field of evasion of fiscal revenues is very wide and covers all the moments that can be marked as an opportunity to avoid these revenues. These incriminated behaviours are present in all forms of business.

## SUPPRESSION OF THE GREY ECONOMY IN THE REPUBLIC OF SERBIA

Combating the grey economy is a key step in establishing a predictable and stable business environment and an equitable market game and requires coordinated efforts by public administrations and market participants. Combating this crime can be effective only if it is permanent, planned and based on scientific achievements. This struggle must be pursued on

13 Stevanov, V. (2014) *Uzroci i pojavni oblici sive ekonomije u Republici Srbiji na pragu trećeg milenijuma,* specijalistički rad, Kriminalističko - poliijska akademija, pp.41

a wider scale with the engagement of all social factors, and above all, the elimination of those factors that cause its existence. Timely detection of these works and their effective prosecution play an important role.

At this point, the frequency of crimes in the field of grey economy will be analysed (tax evasion, non-payment of tax on deduction, illicit trade, smuggling and unauthorized production) in relation to the total number of reported crime and economic crime, as well as the structure of this group of criminal offenses in the period 2006-2015. As a source of data, the annual statistical reports of the Ministry of the Interior of the Republic of Serbia on reported crimes were used.[14]

*Table 2. Total number of criminal offenses, structure and number of offenses in the field of grey economy*

| Year | Total CO | Total CO of economic crime | Tax evasion Article 229 | Unpaid withholding tax Article 229a[15] | Smuggling Article 230 | Illicit trade Article 243 | Illicit production Article 242 |
|---|---|---|---|---|---|---|---|
| 2006. | 98.414 | 10.499 | 178 | | 132 | 416 | 21 |
| 2007. | 104.118 | 10.697 | 223 | | 274 | 277 | 7 |
| 2008. | 105.203 | 10.481 | 273 | | 253 | 284 | 11 |
| 2009. | 102.261 | 10.889 | 294 | | 403 | 197 | 8 |
| 2010. | 100.028 | 10.451 | 421 | 17 | 368 | 287 | 7 |
| 2011. | 101.309 | 9.677 | 275 | 13 | 205 | 240 | 10 |
| 2012. | 97.015 | 8.678 | 352 | 102 | 127 | 271 | 10 |
| 2013. | 113.600 | 7.421 | 257 | 36 | 75 | 356 | 25 |
| 2014. | 102.715 | 7.836 | 202 | 12 | 118 | 398 | 89 |
| 2015. | 98.545 | 8.175 | 185 | 23 | 138 | 562 | 88 |

*Source: Ministry of Internal Affairs of the Republic of Serbia.*

In 2006, a total of 98,414 criminal offenses were reported, out of which 10,499 criminal acts of economic crime. Of the total number of registered criminal offenses of economic crime, in 2006, 747 crimes were committed in the field of grey economy, which represents 7.1% of the registered economic crime, and 0.76% in relation to the total number of criminal offenses reported in 2006. Of the total number of reported criminal offenses in the field of grey economy, 416 offences of illegal trafficking, 178 of tax evasion, 132 of smuggling, and only 21 are illegal work. The structure of this group of offenses is dominated by illicit trafficking, followed by the criminal acts of tax evasion and smuggling, while the participation of illicit production is significantly lower.

14 According to the police records - statistics on crime and records of the prosecution and the court. Data on the criminality of adults and minors are published by the Statistical Office of the Republic of Serbia in the annual bulletins, which provide statistical data on the number of registered, accused and convicted persons.

15 Законом о изменама и допунама Кривичног законика ("Службени гласник РС", br. 72/2009, који је ступио на снагу 11.9.2009. године) чланом 88. прописује се новичлан 229а – Неуплаћивање пореза по одбитку, чије одредбе су преузете из чл. 173. Закона о пореском поступку и пореској администрацији ("Службени гласник РС"", бр. 80/2002, 84/2002, 23/2003, 70/2003, 55/2004, 61/2005, 85/2005,62/2006, 63/2006 , 61/2007 і 20/2009), чиме је предузет још један корак ка кодификацији Кривичног законика.

In 2007, a total of 104,118 criminal offenses were reported, out of which 10,697 were reported as economic crimes. This year, a total of 781 criminal offenses in the field of grey economy were reported, accounting for 7.3% of the total registered commercial crime, and 0.75% in relation to the total number of criminal offenses committed. Out of the total number of reported criminal offenses in the field of grey economy, 277 were of illicit trade, 274 were smuggling, 223 were tax evasion, and only 7 criminal offenses were illicit production. At first glance, it can be concluded that the number of reported criminal offenses in the field of grey economy in 2007, apart from the criminal offense of illicit production, is almost equal or without significant difference. The largest number of registered criminal offensesin the field of grey economy is in the category of the offense of illegal trade, followed by criminal offenses of evasion and smuggling, while the number of reported criminal offenses is unacceptable production is extremely small, practically negligible.

In the territory of Serbia in 2008, a total of 105,203 criminal offenses were reported, out of which 10,481 were economic crimes, which was a slight decrease compared to the previous year. Of the total number of criminal offenses of economic crime, that year 821 criminal offenses were in the field of grey economy, which made up 7.8% of the registered economic crime, and 0.78% in relation to the total number of crimes in 2008. Out of the total number of reported crimes in the field of grey economy, 284 are illicit trade, 273 tax evasion, 253 are smuggling, and only 11 criminal offenses are illegal production. In 2008, we have a uniform number of reported, previously mentioned crimes in the field of grey economy, apart from the criminal offense of illicit production. Namely, illicit trade accounts for 35%, tax evasion 33%, smuggling 30%, and 1.3% of the total number of reported acts in the field of grey economy make the illegal work illegal.

In the territory of Serbia in 2009, a total of 102,261 criminal offenses were reported, out of which 10,889 cases were reported from the group of criminal offenses against the economy, which was a slight increase compared to the previous year. That year, a total of 972 crimes in the field of grey economy were registered, accounting for 8.9% of economic crime, and 0.95% of the total reported crime. Out of the total number of reported crimes in the field of grey economy, 403 works are smuggling, 294 tax evasion, 197 illegal trade, and 78 criminal offenses are illegal production. At first glance, it can be concluded that the number of criminal offenses of smuggling in 2009 is marked by a marked increase, while the crimes of tax evasion and illicit production are without significant oscillation, and the criminal offenses of illicit production also recorded growth, but there is still no significant participation in the total number of reported crimes in the field of grey economy.

During 2010, a total of 100,028 criminal offenses were reported in the territory of Serbia, out of which 10,451 were from the field of economic crime, so that economic crime that year recorded a slight decline in comparison with the previous year. That year, a total of 1,100 crimes in the field of grey economy were registered, accounting for 10.5% of economic crime, and 1% of the total reported crime. Out of the total number of reported criminal offenses in the field of grey economy, 421 cases are tax evasion, 368 cases are smuggling, 287 illicit trade, 17 non-payment of tax on deduction and only 7 criminal offenses of illicit production. The number of criminal offenses recorded an increase compared to the previous year as well as unauthorized production, while smuggling in 2010 registered a slight decline, while the illegal work of illegal production also decreased, and there is still no significant participation in the total number of reported criminal offenses from the field of grey economy.

In 2011, a total of 101,309 criminal offenses were reported, out of which 9,677 were in the field of economic crime, which in this year registered a slight decline. In 2011, a total of 743 crimes in the field of grey economy were reported, accounting for 7.7% of economic crime and 0.7% of the total reported crime. Out of the total number of reported crimes in the field of

grey economy, 275 works are tax evasion, 240 are illicit trafficking, 205 are smuggling, 13 are non-payment of tax on deduction, and 10 crimes are illicit production. This group of criminal offenses recorded a fall compared to the previous year, apart from the criminal offense of illicit production, which recorded slight growth, but there is still no significant participation in the total number of reported criminal offenses in the field of grey economy.

During 2012, a total of 97,015 criminal offenses were reported, out of which 8,768 were reported as part of economic crime, so that economic crime continued a downward trend in this year. This year, a total of 862 crimes in the field of grey economy were reported, which makes up close to 10% of economic crime and 0.9% of total crime. Of the total number of reported crimes in the field of grey economy, 352 are tax evasion, 271 are illegal trade, 127 are smuggling, 102 are non-payment of tax on deduction, and 10 criminal offenses are illegal production. In 2012, tax evasion is increasing as well as illicit trade, while smuggling declines, while unauthorized production is at the same level as in the previous year, and there is still no significant participation in the total number of reported criminal offenses in the field of grey economy.

During 2013, 113,600 criminal cases were reported to the competent prosecutor's offices in Serbia, of which 7,421 were reported as economic crimes, so that economic crime this year registered a downward trend. This year, a total of 749 crimes in the field of grey economy were registered, which constitutes 10.1% of economic crime, and 0.6% of the total reported crime. Out of the total number of reported crimes in the field of grey economy, 356 is illegal trade, 257 works are tax evasion, 75 are smuggling, 36 are non-payment of tax on deduction, and 25 criminal offenses are illegal production. In 2013, tax evasion and smuggling declined, while illicit trade and illicit production registered significant growth compared to the previous year, and stimulated the continued production of no significant participation in this group of criminal offenses.

During 2014, a total of 102,715 criminal offenses were reported, out of which 7,836 were in the field of economic crime, which in this year recorded a slight increase compared to the previous year. In 2014, a total of 819 crimes in the field of grey economy were registered, accounting for 10.5% of economic crime and 0.8% of the total reported crime. Of the total number of reported crimes in the field of grey economy, 398 are illicit trade, 202 are works of tax evasion, 118 works are smuggling, 89 criminal offenses are illegal production and 12 criminal offenses are not tax deductible. In this year, illicit trade and illicit production recorded significant growth in comparison to the previous year, and the unauthorized production assumes a significant share in the total share of this group of criminal offenses.

In 2015, a total of 98,545 criminal offenses were reported, out of which 10,697 criminal offenses were committed in the field of economic crime. This year, a total of 996 crimes in the field of the grey economy were registered, accounting for 12% of economic crime and 1% of the total reported crime. Of the total number of reported criminal offenses in the area of grey economy, 562 were illicit trade, 185 tax evasion, 138 smuggling, 88 illicit production and 23 non-payment of deduction taxes. At first glance it can be concluded that the number of reported crimes in the field of grey economy in 2015 was the highest in the observed period and that their participation in the total reported economic crime recorded significant growth. There is also a significant increase in the criminal offense of illicit trade, the registration of which is the highest in the observed period and in relation to the previous year the number of this criminal offenses is almost 30% higher. Other crimes from this group include tax evasion, smuggling and unauthorized production that do not record significant changes in their respective shares, as well as non-payment of tax on deduction.

When it comes to the scope of criminal offenses in the field of grey economy in the territory of the Republic of Serbia and their relative participation in total and economic crime,

Table 2 indicates that, even in one year of the observed period, the participation of this group of criminal offenses in the total mass of reported criminal acts of economic crime exceeded for 12%.

It can be clearly seen that the smallest number of criminal offenses of tax evasion were recorded in 2006 and the largest in 2010, the smallest number of criminal offenses were recorded in 2013 and in 2009, the smallest number of criminal offenses of illicit trafficking were recorded in 2009, and in 2015, the smallest number of criminal offenses of illicit production were recorded in 2007 and 2010 and the largest in 2014, the smallest number of criminal offenses of non-payment after deduction was recorded in 2014 and the largest in 2012.

Finally, it should be noted that grey economy is significantly represented in the Republic of Serbia, so the state must take appropriate measures to reduce it.

## CONCLUSION

Grey economy, as well as corruption, are very widespread phenomena in the whole world and beyond any doubt they are very complex, multidimensional and harmful phenomena. Criminal offenses in the field of grey economy have direct impact on the reduction of public revenues, which jeopardizes the efficiency of the operations of public institutions, forcing them to offer both a smaller scope of public services and goods and a lower quality of the same. This affects the reduction of the living standards of budget users and the reduction of the well-being of all citizens.

The complexity of this problem is reflected in numerous forms of grey economy in the context of economic criminality, especially in the emphasized adaptability to the existing social conditions, as well as the emergence of new forms of these socially harmful phenomena. Because of its illegal nature, the informal economy above all has no access to government stimulus measures, development loans, professional support of professional associations, business and trade chambers, so it is ineffective in fostering development, applying modern technology and knowledge.

Successful detection and prevention of grey economy can be carried out by well-trained and professionally trained police, tax police, prosecutors and others. The fight against this phenomenon can only be effective if its place is considered in the global socio-economic and political system and if all the competent authorities act organized, bearing in mind that this is a phenomenon that has its system roots. This struggle can be effective only if it is permanent, planned and based on scientific achievements. Repressive measures give results in the short term and are insufficient. Only planning and implementation of system solutions can affect the long-term reduction of grey economy and its consequences. In line with the above, it is necessary to achieve public interest in order to improve transparency and interaction not only between holders of public authorizations and taxpayers, but also among taxpayers themselves.

Based on the given analysis, it is possible to determine the number of crimes committed in the field of grey economy in the observed ten-year period, as well as in the specific year, and the frequency of their performance in relation to the total number of criminal offenses. The paper presents a tabular presentation of the above data, which enables clearer visibility and a better insight into the frequency of the manifestation of this group of criminal offenses. The mentioned analysis showed that the disrupted economic flows led to the expansion of grey economy and economic crime. The increasing criminality caused a certain reaction of the authorities, which reflected in the constant increase in the number of crimes discovered in the

area of grey economy as well as economic crime, but also their perpetrators, who moved with smaller oscillations during the observed period.

From all the above, it is clear that the research of this phenomenon has great scientific and social significance, especially because of the dangers and consequences that they pose at the individual and social plan. The seriousness and complexity of this problem, as well as its actuality, obliges us to pay more attention to it in order to prevent and detect such negative phenomena more successfully.

## 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. Godišnji statistički izveštaji Ministarstva unutrašnjih poslova Republike Srbije
3. Dell'Anno, R. (2003), Estimating the shadow economy in Italy: a structural equation approach, Working Paper 2003–7, Department of Economics, University of Aarhus.
4. Ekonomski rečnik (2006) Ekonomski fakultet Univerziteta u Beogradu, Beograd.
5. Jelačić M. i N. Teofilović (2006) Sprečavanje, otkrivanje i dokazivanje krivičnih dela korupcije i pranja novca, Policijska akademija, Beograd.
6. Jovašević , D. i Gajić-Glamočija, M. (2008), Poreska utaja: oblici ispoljavanja i mere suzbijanja, Beosing, Beograd.
7. Krivični zakonik („Službeni glasnik RS" br. 72/11...45/13)
8. Zakon o izmenama i dopunama Krivičnog zakonika, Službeni glasnik RS , br. 121/12
9. Kulić, M. (1999) Poreska utaja i krijumčarenje, BMG, Beograd.
10. Kulić, M., Milošević, G., Milašinović, S. (2011) Fiskalni kriminalitet u Srbiji, Industrija, Ekonomski institut, Beograd, br.4
11. Madžar, L.(2013) Siva ekonomija u Srbiji u svetlu tendencija u evropskim zemljama, Škola biznisa, Novi Sad, br. 3-4/2013
12. Mirković Z. (2016) Siva ekonomija i pranje novca kao finansijska osnova terorizma, doktorska disertacija, Fakultet za trgovinu i bankarstvo, Univerzitet Alfa, Beograd.
13. Nacionalni program za suzbijanje sive ekonomije, „Službeniglasnik RS", broj 110 od 28. decembra 2015.
14. Nikolić, Đ.,Čudan, A., Đorđević, B. (2016) Carinski organi u funkciji suzbijanja sive ekonomije. Nauka, bezbednost, policija, 21(2) Kriminalističko-policijska akademija Beograd.
15. Smith, P. (1994), Assessing the size of the underground economy: the Canadian statistical perspectives, Canadian Economic Observer, Catalogue no. 11–010
16. Socijalno ekonomski savet RS (2010), Efikasno suzbijanje sive ekonomije, Beograd: NIP Radnička štampa.
17. Stevanov, V. (2014), Uzroci i pojavni oblici sive ekonomije u Republici Srbiji na pragu trećeg milenijuma, specijalistički rad, Kriminalističko - policijska akademija, Beograd.
18. Stojanović Z., Perić, O. (2009), Krivičnopravo-posebni deo, XIII izmenjeno izdanje, Beograd.
19. Stojanović, Z. (2009), Komentar Krivičnog zakonika, JP „Službeniglasnik"

20. Schneider, F. (2008), The Shadow Ekonomy in Germany: A. Blessing or a Curse for the Official Ekonomy, Ekonomys, Analysis, Policy, Vol. 38, No. l, March
21. Čudan A. (2014), Neformalna ekonomija - mogućnost smanjenja, šansa ili zabluda, Kriminalističko-policijska akademija; Beograd

# PRIVATIZATION AND GROWTH OF GREY ECONOMY AS FOLLOWERS OF TRANSITION

**Ivica Lazovic**[1]**,**
RAMRRS Belgrade, Republic of Serbia

**Abstract:** Grey economy is present even in modern economic flows of the most developed countries in the world, but it is particularly distinguished in economies affected by crises, war economies and the process of transition. Expansion of grey economy causes a great damage to reform processes in post-socialist countries, in other words, the countries in transition, since it takes control over the most sensitive economic, production and market flows, destroys business rules and ethical standards by promoting bribe, corruption, black-markets, etc.

Disregarded for a long time, grey economy researches are becoming more and more relevant in the last three decades in developed economic markets and east-European economies in transition as well. We can process this subject matter as multidisciplinary, as it encompasses economic, legal and sociological topics, but it is interesting for many other scientific disciplines.

**Key words:** *privatization, grey economy, transition, process, property*

## INTRODUCTION

All social systems, regardless of whether they are more or less democratic, operate with a certain percentage of grey economy that is in a certain way the cause of development and a factor of stability of the community. Grey economy gives vitality to the functioning of political and legal systems in a specific way. In addition, grey economy was the initiator of development but also it has hampered the development during the transition process in a specific way.

The system of ideological, political, social, and economic values which was dominant in the societies of Eastern Europe for several decades began to collapse twenty-five years ago. This has led to major changes that have been affecting bothideological and political spheres, legal and economic ones, social and cultural, as well asthe spiritual sphere in some of these societies. These changes are usually related to the concept of transition.

These are very complicated, long-term, multi-dimensional and contradictory processes which involve certain assumptions, operators and tools that require a complex analysis.

This is a process with no clear outcome, as it is a well-known fact that changes involve facing with the unknown, which contributes to the complexity of the process. It is clear when the transition starts and what is transformed, but itis not clear in which direction the process may be going and what its results will be. The transition is supposed to represent an attempt to modernize societies of Eastern Europe, wheretherole models are developed Western societies, with all their similarities and differences.

The key feature of this process is the transformation of social property relations in the direction of privatization and public property and leaving guided, state-planned economy and the promotion of market and market mechanisms of regulation of economic life.

1 ivica_lazovic@yahoo.com

All of this has caused closing the industrial production and job losses for many workers, along with violations of basic economic and social rights of employees through lack of earnings or drastic cuts in wages, benefits and other income. In such conditions, a large number of jobless people and impoverished workers who often only have a formal job, have been turning to alternative ways of earning income such asgrey economy.

It is not necessary to emphasise the detrimental effects of grey economy. There is a high risk that grey economy may become a regular and the most powerful form of economic and other trends in the transition countries.

Grey economy, in its scope, consequences and effects,becomes an essential factor of analysis, research and scientific consideration at present.

Research of grey economy was mostly neglected in our country until this phenomenon reached alarming proportions in the last decade of the last century.

## PROCESS OF PRIVATIZATION AND SOCIO-ECONOMIC RESULTS

The process of transition, or, in other words, transformation of state and public property into private, privatization, is a base and a key factor of all other transitional changes. This topic continues in 2017, although it was believed that privatization would be completed soon. It is the most important process in the transition of former socialistic countries. It appears to be a necessity because the former socialistic system was economically inefficient and it encountered low growth rates and weaker quality production considering market economy. Besides, public property represents political and economic support of totalitarian regimes, while private property is a material foundation of individual freedom, personal safety and democracy. Practically all previous reforms which were conducted did not have anticipated results because there was no property transition, in other words, privatization was not performed. Privatization represents the key link in successful implementation of the transitional process. Namely, without properly defined ownership relations, one cannot expect efficient economic activities, a reduction in the unemployment rate, the creation of the free market, price stabilization, elimination of the foreign debt, etc. In essence, privatization determines the rhythm and the character of the transitional process.[2]

The main goal of privatization is to increase the efficiency of enterprises, which arises from healthier business motivations and is achieved through the reduction of expenses, financial re-capitalization, better work discipline, better organization, new investments, etc. Another goal of the privatization process is to improve the financial situation of the state, which is to be done by means of the following three methods: based on the revenues gained from the process of privatization; based on the revocation of subsidies for state and social enterprises; and based on the increase in tax revenues from improved economic activities. For the cabinet, the attempt to increase its own political rating through the choice of a demagogically convincing privatization program may become an important goal of the privatization process, yet this goal is in contradiction with the first two goals[3].

The word "privatization" was an essential concept and subject of interest of common people, politicians, the public and scientists in the last decade of the last century and the first

2 See: Đorđević M, "Proces privatizacije u Srbiji u periodu od 2000. do 2008. godine", Škola biznisa Naučnostručni časopis, Novi Sad, 2009.
3 Begovic B, Mijatovic B, Zivkovic B, "The New Model of Privatization in Serbia" Center for Liberal Democratic Studies Belgrade, December 2000.

decade this century. The transition, privatization, structural adjustment, the establishment of a new economic and social system were the magic words, which had a connotations of binding progress and the magic formula that would solve all problems. The entrepreneurial spirit would solve all the problems, and the free market and his forces would lead to the development of employment and social welfare.

It was already said and there were too many believers of thisstoryuntil 2008, until the disclosure of the global financial crisis. Suddenly, the topics related to the prospects and benefits of privatization in professional and scientific circles became undesirable. Suddenly, the problems and the consequences of privatization are the interest of nobody[4].

The basic starting point for discussion on privatization represents the premise thatprivate property is more efficient than public ownership.[5]

However, privatization processes represent a turning point in respect of property types and change the ways of business and life. They are very painful, since they are accompanied by production decrease, reduced national income, high inflation and unemployment, with decrease of standard for the majority of population. Fast privatization processes are accompanied by various socio-economic results and grey economy in various forms. The fact is that there is no painless and ideal privatization. This affects all citizens, directly or indirectly. The privatization is easier in a setting of macro-economic stability (which was not a case in any of the socialist countries), socio-economic stability and readiness of a country to develop fair competition and to stimulate the development of private sector and initiative.

Practically all former socialist countries, more or less, finished crucial changes – transition of the entire socio-economic system, in other words, they carried out privatization and moved to market competition and multiparty systems. State property kept its presence only partially at strategically important sectors. Post-socialist countries performed these changes from a legal-technical standpoint rather than by becoming really developed market economies.

Until now, all privatization processes that were carried out and transitions to market business caused also big social problems which could be identified as a decrease in production and real income, as well as an increase of inflation and unemployment. Decreased production levels and employment resulted in decreased standard of living of population, followed by growing social differences.

Some authors[6]think that original acquisition of property is genuinely unfair. This applies to nationalization,but also to privatization. That is an exchange of unequal values. Asking for fairness in the exchange of unequal values is simply pointless. There is only a question whether the new system of property is superior to the old system of property in terms of increased of economic efficiency (accumulation of capital, its more productive use and lager profit, as a result of better management).

Besides, there are a few very significant controversial issues with the privatization like: the tempo of the privatization, assessment of capital, privileges of future buyers, possibility of stock sale after privileged sale, amount of stocks which make a stock package, participation of foreign investors, stimulation of privatization agencies, etc. Economic and legal experts offered different principles and models of privatization, since each country had a specific socio-economic structure.

4 See: Drašković, B. (recenzija). (2011). Efekti privatizacije u Srbiji,Socijalno-ekonomski saveta R. Srbije, Beograd, SOLIDAR Suisse, http://www.socijalnoekonomskisavet.rs/cir/publikacije/efektiprivatizacijeusr.pdf

5 See more: Privatizacija - dokle se stiglo i kuda dalje, Transparentnost Srbija, Beograd, 2004, www.transparentnost.org.rs/privatizacija.pdf

6 See more: Labus M. Osnovi ekonomije: savremena teorija i primena, Beograd: Jugoslovenska knjiga, 1997.

One of the basic dilemmas of the privatization process is whether this process should be centralized ("the privatization from the top", as an obligatory process which is managed by government) or decentralized ("the privatization from the bottom"). Both principles have advantages and disadvantages.

The centralized approach enables steering and direct control of the privatization by state, which should provide a high level of legality and transparency for which concrete individuals are responsible. This means a chance for mass privatization, in other words, for setting of the procedure by state which enables the privatization of a large number of enterprises, so that the large part of the economy could be privatized quickly, avoiding a danger of blockage form employees in the enterprises. However, there is some skepticism related to such actions due to limited capabilities of the state to achieve efficient economic results, as well as possibilities of systematically implanted mistakes in the concept or realization of the process. Besides, centralized privatization puts great information demands to the state (government), impartial assessment, etc.

Decentralized privatization is based and conducted by employees or enterprises, limited by predefined rules: legal regulations and decisions of privatization agencies. It includes a large number of people and gets political support and it is also supported by interested individuals, relieving the state of certain obligations. In spite of that, without enough supervision by the state, it did not give good results in any east-European country.

*Privatization by sale.* Generally, there are two basic options for the sale of enterprises. The first one is the sale in which the state assesses the value of enterprises and searches for a buyer by open sale of stocks, auction or direct agreement. The second one means thatan enterprise starts the process of privatization by transforming itself into a stock company, giving stocks to interested individuals. The sale of enterprises by the state can be conducted by public registration of stocks which is appropriate for more successful enterprises in a country where there is a stock market, or private sale of stocks of public enterprises to previously identified investors, which is suitable for unsuccessful enterprises which need strong and skilled owners.

Buying of enterprises by a manager or employees occurs when they provide the capital necessary for buying form loans, and the guaranty is the value of the enterprise which they buy. An alternative option is to set up another holding company which would buy stocks of the enterprise. However, managers usually buy up enterprises which make profit, while employees usually buy up enterprises which have financial difficulties.

The advantages of privatization are that it mostly focuses on the interest of new owners in profit and successfulness of the enterprise and also provides the greatest management efficiency. Besides, the state acquires necessary funds and trough sale of state enterprises to foreign investors it is possible to attract foreign capital and obtain qualified managers very quickly. If we speak about buying of foreign managers or employees, their knowledge and capabilities are maximally activated, since there is also a personal interest in the enterprise. The basic problems with the privatization by sale are the following:

- Methods for the assessment of enterprises value in absence of market of capital, which represents one of the most complicated problems of the privatization, facing obstacles like historical heritage and burdens of the previous period, political, legal and economic uncertainty, etc.

- Amount of capital in a country, i.e. a lack of domestic capital because the value of enterprises which are to be privatized exceeds economy of population. Neither of the possible solutions like greater participation of foreign investors or postponed payment is ideal;

- Inequality of citizens, considering available capital, chance to buy enterprises contrary to the rule of justice; and

- Slowness, noticed from experiences of some east-European countries, first of all Hungary and Poland.

*Labor stock model (internal privatization)*. This model of privatization encourages employees to whom various privilegesare given on occasion of stock buying.

Labor stock model is, in an administrative sense, very simple, as the offer of enterprises under privileged conditions increase interest of majority of population, which could lead to acceleration of the whole process. However, this model does not make income that would increase the state budget, and it is practically impossible to provide equality of all citizens, because some of them work in successful and others in unsuccessful enterprises. Besides, it is disputable whether giving privileges to employees brings more efficient management than some other options.

*Voucher privatization*. This model of privatization means free distribution of collective ownership of a state to all its citizens.

Advantages of voucher privatization are significant and various. It set up clear and universal ownership rights with realization of principles of justice and transparency. The state is excluded, to a large extent, from the process of privatization and vouchers provide fast privatization, since they solve the problem with lack of capital, which decelerates privatization by sale. The value of enterprises, i.e. the stocks value is defined freely (auction), avoiding the technical and conceptual problem of previously defined values of enterprises and preventing possible irregularities. The most serious disadvantage of this concept refers to the management problem, because everyone would try to transfer management expenses to other owners, but to get profit from positive effects of management supervision. Besides, voucher privatization could lead to an increase in consumption of population and stir up inflation.

*Privatization by investment funds*. Essence of the idea is to transfer property over economy to newly founded funds freely, trying to change property relations in a very short period and set up ownership regime, which is suitable for market economies.

The investment fund model shares some advantages with the voucher privatization. They are related transformation, speed, justice and problems with lack of capital and assessment problems. The most significant problem with this model refers to the management of investment funds (holding company). It is a very unfavourable option to nationalize these funds or turn them into state (political party) funds, which would lead to a departure from economic course and predomination of political goals. Besides, a dispersion of property represents the management problem bigger that it is with the voucher privatization, since nobody would supervise the management work, so that it could maximize its own interests contrary to the interests of the owner. The risk from too strong and badly supervised funds could be solved by decreasing their 'lives', in other words, by transformingthem into privatization agencies of limited existence, which would allow the market to form an upcoming ownership structure. But, there is a problem with motivation of privatization agencies' management, which could not bring a legal action against thousands of owners. Besides, it is hard to believe in rationality and efficiency of the organizations whose duration is legally limited in advanced.

The precedence should be given to voucher privatization which brings better management, particularly in the mid-term period of privatization by intermediary of institutional investors. With other two criteria (justice and speed) both types of free privatization are equal. Labor stock model is competitive in terms of speed, but less fair and giving weaker management results.

The choice among the methods of privatization does not depend exclusively on economic issues. In this process, political and social issues also have an important role.

Some authors suggest that the process of privatization should be staged. The foundation of this concept is an analysis of institutional and legal conditions for performing privatization, evaluation of common economic circumstances under which it is to be carried out, dislocation of employees, etc. Eventually, this includes determination of developing strategy and instructions for every concrete step which is to be done, concerning the existing economic and political environment (whether to privatize enterprises one by one or a whole economic branch or the whole economy at once, etc.). Answers to these questions are very important as they regulate issues such as the goals of privatization, analysis of expenses, in other words, production or service unit. Employee issues are also very important, that is to say how many employees would be laid off, trained or secured in other ways.

Specific researches for the adequate model of privatization in Serbia were affected by the fact that public (not state) property over production resources was predominant in the political system of socialist self-management. This was exactly what gave rise to many dilemmas and opened theoretical disputes.

Some authors who first dealt with this issue[7], came to conclusion that the structure of property in Serbia was so irrational and deficient, with management mechanisms which did not fulfil even the most modest demands regarding efficiency, so that ultimately, due to the ineffective management regime, the whole economy recorded huge loses of potential national product, which could have been avoided if the economy had possessed normal, market-based mechanisms of management, in other words, if it was based on private property. According to this opinion, the process of privatization is so complex that is almost impossible to be completed in less than a few decades. Namely, it calls for complete replacement of the entire economy system in which a new management structurehas to be created, new administrative bodies should be introduced, along with new accounting standards and procedures, new type of revision and control, new banking type, instruments and institutions of financial intermediary, new experts in economic laws, new judicial network, etc. All of it requires a lot of knowledge which this country does not possess, knowledge which could (and must) be created for decades. The whole drama of our property transition could be summarized in a statement that it is an urgent action, and that it willtake decades to achieve.

Privatization in Serbia has had five models for the last 25 years. Privatization in Serbia was started by the adoption of the Law on Social Assets in 1989.The Law on conditions and procedure of turning public property into other forms of ownership was adopted in 1991 and the Law on Ownership Transformation in 1997[8]. After the political changes in 2000, the new government was faced with the challenge of introducing reforms in the economy, devastated after decades of disinvestment, sanctions and war and it adopted an ambitious program of economic reforms, committing to change the trends of the past decade and integrate the country into the European and global political and economic trends.The Law on Privatization was adopted in 2001 and it was subsequently subject to numerous amendments.A new Law on Privatization which is currently in use was passed in 2014[9] and has been amended on a number of occasions.

Political elites in Serbia have adopted the concept of neo-liberal reforms known as the Washington Consensus. Its creators and controllers are the International Monetary Fund and the World Bank. The essence is contained in the stabilization of the national currency, privatization, deregulation and liberalization[10].

7 Madžar Lj. Putevi privatizacije u Jugoslaviji – zakonski modaliteti i neke prepreke, Beograd: SANU – Centar za ekonomska istraživanja, 1992.
8 Read more in: Stojiljković Z. Lavirinti tranzicije, Friedrich Ebert Stiftung, Beograd 2012.
9 Privatization Act (Official Gazette RS no. 83/14, 46/15, 112/15, 20/16)
10 Novaković N, Štrajkovi, sindikati i privatizacija u Srbiji, Sociološki pregled, vol. XLVII (2013), no. 1, pp. 23–52.

# PRIVATIZATION AND GROWTH OF GREY ECONOMY

Grey economy (also referred to in English as "hidden economy", "shadow economy", "informal economy"), is a global phenomenon, more or less customary, present in all countries, regardless of the type of society and the degree of socio-economic development.

There are many different definitions of the term"grey economy" and the most often used among them include: "informal economy", "concealed economy", "the illegal economy", "irregular economy" and many other terms. However, there are still some differences because of the meaning of these concepts and it is important to point out to them at the beginning.

According to the Dictionary of Economics, informal economy is "a part of the economy which is characterized by irregular and illegal business. It can be seen as a shadow economy or operations that can be legalized by taking certain actions (for example, payment of taxes), and the black economy, which cannot be legalized (e.g. drug trafficking). It is present in the underdeveloped and developed countries, but the economic development reduces its stake in society. All countries implement measures for its reduction in order to increase tax revenues"[11]

According to Economics, the grey economy is: "a set of economic activities that are carried out outside the institutionalized economic environment. It includes criminal business, fictitious business, informal economy, and other covert and unlawful business transactions. From the statistical point of view it is classified as registered and unregistered, from the aspect of legality - to legal and illegal, from the fiscal point of view - taxed, taxable (whole revenue or a part is hidden from the tax authorities) and other (there are clear tax regulations but they are carried out using gaps in the legal regulations). Special attention should be paid to the so-called third economy (black economy) which is explicitly prohibited and which is connected with criminal and mafia activities".

The grey economy in the Republic of Serbia is comprised of three pillars

1) Prohibited business (illegal business entities)

2) Black work (employees who work illegally)

3) Money laundering and financial fraud (illegal transactions, tax fraud, etc.).[12]

Informal employment is defined by The International LabourOrganization as "employment without safe contracts, benefits for workers or without social protection. It consistsof two basic components: self-employment in informal enterprises and paid employment on non-formal jobs."[13]

It is widely accepted alongside with privatization there is a growth of grey economy. However, it is hard to prove connections between each privatization and different forms of grey economy. There are different ways of privatization abuse:

- It is a fact that some managers of state companies resort to various abuses to decrease the levels of company value in order to buy up in future privatization; a lack of reference indicators and special discount rates which differentiate the market, contribute to these issues.

- Acquiring of commissions to intervene in privatization.

- Usage of management credits to buy up companies and return of worthless amounts.

- Purchase of enterprises at very low prices and sale at higher prices later, without adequate taxation on capital profit.

11 See: Efikasno suzbijanje sive ekonomije, Socijalno-ekonomski Savet Republike Srbije Kancelarija Swiss Labour Assistance u Srbiji, Beograd, 2010.http://www.solidarsuisse-serbia.org/rs/uploaded/efikasno_suzbijanje_sive_ekonomije.pdf
12 Ibid, pp. 11.
13 Ibid.

- Transfer of values created in the enterprise into foreign companies through transferring prices of input.

- Foundation of private "satellite" companies which are used for sale and purchase, and also financing of privatized enterprises.

- Money transfer of enterprises into accounts of foreign banks.

- Usage of company resources for personal purposes, etc.

There is no doubt that fast transitioncreates conditions for flourishing grey economy. Many prominent economists in the world are against fast transition[14]. Jozef Stiglic noticed that advocates of fast privatization were in trouble, because, in countries where it was done there was no "legitimate challenge of private property, which could perform the privatization". Therefore a country has to choose one out of four possibilities:

- to sell national wealth to someone abroad;

- to carry out voucher privatization;

- to restrain "spontaneous" privatization, or

- to face something that could be named "negative" privatization.

Stiglic says that the last of these occurred after 1995 "loans for shares". The state allowed private entrepreneurs to set up banks which would lend money to individuals for the purpose of buying state enterprises (alternatively, in an arrangement of "loans for shares", money is lent to the state, and shares of state enterprises are guaranties for the loan). Anyone who could obtain a license to do such business would also obtain a license to issue money, which would give him a chance to become the owner of state enterprises. Although, the corruption in this case would be less transparent than if the state simply gave away national wealth to its friends, there is actually no big difference between these two processes.

Since the whole process was mainly taken to be illegitimate, this "robbery" privatization showed that capitalism was even worse than in the indoctrination pamphlets from communist era. Since there was no reason for assumption that those who obtained their property that way were good managers, it could not have been expected that privatized wealth would be used better than it was. Honest individuals who recommended this process did not take much care about political influence or incapability of managers and they believed that there was a real possibility to create "additional market", so that the enterprises would be eventually sold to those who would run them better. They hoped that these new entrepreneurs, at least, would conduct fair auction. However, that did not happen due to several reasons: first, there is the basic problem – where to find the manager teams with necessary capital? What is even worse, there has been a decrease of trust in economy and administration which makes the country less attractive for foreign investors. The oligarchs realized that more wealth could be taken from "overflowing of funds" than by its distribution, which created a setting for creating wealth[15].

Stiglic states that instead of trying to set up control over managers in state enterprises by more stimulating contracts, the usual advice was to carry out privatization and let "private property rights" to generate initiative naturally as they do in the West. However, the fact that in large western companies property and control are separated means that the control is not simply an outcome of "clearly defined rights of private property". The ownership over shares or bonds is clearly defined; shareholder can buy, sell or keep them. However, in situations where the shareholders are scattered, holding of shares does not mean real control over the company.

14 See more: Štiglic J. Kuda idu reforme? Deset godina tranzicije, https://radmilovicwebsite.com/2016/09/28/stiglic-kuda-idu-reforme/

15 See more: Štiglic J. Kuda idu reforme? Deset godina tranzicije, https://radmilovicwebsite.com/2016/09/28/stiglic-kuda-idu-reforme/

## SOME MEASURES FOR REDUCTION OF GREY ECONOMY IN SERBIA

Experience of countries which successfully decreased rates of grey economy to acceptable levels has shown that grey economy cannot be attacked at once and frontally in all segments. Combating grey economy represents an organized and long-term process which involves a set of mutually consistent measures. It is necessary to consider social factors (high rate of unemployment, low wages) and actual impossibility to reduce all forms of the grey economy to acceptable levels.

In Serbia, the shadow economy contracted from 33.2 percent of GDP in 2001 to 30.1 percent in 2010[16].

In accordance with the program of fiscal consolidation, further efforts have been planned towards combating tax evasion and grey economy. If the expected effects in that field were not achieved or in case of further deterioration, there may be some shortfalls on the revenue side. The fight against grey economy in particular must include the reduction in illicit trade in tobacco products, reducing grey economy in the area of labor and employment, and the continuation of good results in the field of trade in petroleum products.[17]

To stop grey economy, the state has changed some regulations concerning taxes, introduced an institution of finance inspection and takena range of other systematic measures. Besides these, repressive measures have not been neglected. Some bodies have made significant efforts to curb grey economy.

The police effectively detect forms of economic crime, particularly in cases of grey economy where certain economic subjects or parts thereof got privatizedby a series of criminal activities.

Efforts are made to stop perpetrators of crime, who are popularly known as "perpetrators of privileges". This category of perpetrators abuses privileges which are granted by law in order to stimulate some business sectors. Here we have various and extensive abuses, starting from tax-free services, unrestricted use of funds, irretrievable giving of funds to stimulate employment, production, etc. and also abuse of the export-import regime.

The Serbian government invested substantial effort in curbing grey economy. It also embarked on combating organized crime, which significantly contributed the fight against grey and black economy.

As a phenomenon, grey economy has found a fertile soil on Serbian territory, not only due to economic crisis, but also because of mentality of the population. People who engage in grey and black economy become idols to many young people, who dream of earning money "overnight".

According to recent data, grey economy accounts for about 30 percent of GDP, which is about 15 percent more than in most other countries in the region, according to a study conducted by USAID and the Foundation for the Advancement of Economics[18].

The objective is to restrain the scope of grey economy and reduce it no more than 10%of the national product.

16 See: The Shadow Economy in Serbia New Findings and Recommendations for Reform, March 2013, USAID, http://pdf.usaid.gov/pdf_docs/pnaec461.pdf
17 See: National Economic Reform Programme for 2015-2017, http://www.mfin.gov.rs/UserFiles/File/dokumenti/2015/NERP%202015%20ENG%20za%20WEB%2018_3_2015.pdf
18 See: www.fren.org.rs

Fiscal policy measures are aimed at reducing incentives for operating in the shadow economy and the benefits of doing so, on the one hand, and increasing the associated costs and risks, on the other. In that sense, the most important fiscal policy measures for tackling the shadow economy are: to reduce distortions introduced by the tax system; reduce tax compliance costs; reduce the return to tax evasion; and reduce tolerance for the shadow economy[19].

Given the high share of grey economy in the Republic of Serbia, it is necessary tocontinue the systematic fight against grey economy through the improvement of tax administration and tax fraud detection, reduction in the number of tax procedures and their simplification, better control of taxpayers, more efficient control and collection of taxes, cross control of assets and income, better work of inspection services.[20]

## CONCLUSION

A rapid growth of the informal economy accompanied the transition process. Given its nature and economic, political, social and other consequences, grey economy is a harmful phenomenon. Although it is officially prohibited in almost all systems, it is generally tolerated. For this reason, we may say that grey economy reflects double standards.

Human resources involved in this phenomenon are not employed in the formal and legal sense, because they have no social security or health insurance, but their work often generates significant revenue.

The grey market will never provide the goods for which there is no real demand. In that respect, grey economy is often more efficient that the formal economy. Grey economy is an expression of the real needs of individuals, and has a strong foothold among those who benefit from it.

Grey economy is developed on the ground of capitalism, following the economics and politics of the developed countries of the world. It is an unavoidable phenomenon inall countries of real socialism and itbecomes especially evident during the transition period.

It has its roots in corruption and it is often tolerated by the society and developed in the various forms of criminal behaviours and crime.

Transition countries were faced with the rapid expansion of the informal economy in the process of privatization of social and state ownership, which was proportional to the amount of closed job positions. During the economic crisis of 2008, these tendencies were reinforced.

Grey economy, as a complex phenomenon of the modern world trends, followed by the economic crisis in terms of globalization, has had a major impact on all societies. This influence is noticeable in the political developments, social organization and standardization in the field of legal relations. It is particularly harmful to the prevailing trends in the economies of countries in transition.

The complexity of grey economy requires interdisciplinary research. Modern trends and forms of grey economy and their impact on social processes in the countriesseem almost dramatic. There is no doubt that - in the transition from socialismto capitalism- grey economy has had a big impactin many countries,where it affects the most vital part of economy and social relations, directly predetermining their destiny and prospects.

19 See: The Shadow Economy in Serbia New Findings and Recommendations for Reform, March 2013, USAID, http://pdf.usaid.gov/pdf_docs/pnaec461.pdf
20 See: National Economic Reform Programme for 2015-2017, http://www.mfin.gov.rs/UserFiles/File/dokumenti/2015/NERP%202015%20ENG%20za%20WEB%2018_3_2015.pdf

The social side of this phenomenon reveals a number of problems, trends and challenges for the various forms of engagement and organization of the radical social change. Present situation warns of the complexity and many uncertainties about grey economy and its impacts. The conflicts with regular economic relations and economic-system regulations indicate that the area of the informal economy cannot be transformed and integrated into legal flows by appealing to ethics and morality, or only by coercion and repression.

Combating grey economy is additionally aggravated by the fact that it operates out of range of administrative methods. The way to solve this problem isin gradual legalization of this sector, which is performed so as to mitigate or completely abolish conditions that led to its creation. This primarily impliesdecreased taxes and increased liberalization of labor legislation.

## REFERENCES

1. Begovic B, Mijatovic B, Zivkovic B, "The New Model of Privatization in Serbia"Center for Liberal Democratic Studies Belgrade, December 2000.
2. Đorđević M, "Proces privatizacije u Srbiji u periodu od 2000. do 2008. godine", Škola biznisa, Naučnostručni časopis, Novi Sad, 2009.
3. Drašković, B. Efekti privatizacije u Srbiji, Socijalno-ekonomski saveta R. Srbije, Beograd, SOLIDAR Suisse, 2011.
4. Efikasno suzbijanje sive ekonomije, Socijalno-ekonomski Savet Republike Srbije I Kancelarija Swiss Labour Assistance u Srbiji, Beograd, 2010.
5. Labus M. Osnovi ekonomije: savremena teorija i primena, Beograd: Jugoslovenska knjiga 1997.
6. Madžar Lj. Putevi privatizacije u Jugoslaviji – zakonski modaliteti i neke prepreke, Beograd: SANU – Centar za ekonomska istraživanja, 1992.
7. National Economic Reform Programme for 2015-2017
8. Novaković N, Štrajkovi, sindikati i privatizacija u Srbiji, Sociološki pregled, vol. XLVII (2013), no. 1, str. 23–52.
9. Novaković, N "Siva ekonomija, kriza i tranzicija u Srbiji, Zbornik radova Filozofskog Fakulteta HLV (2)/2015,
10. Privatizacija - dokle se stiglo i kuda dalje, Transparentnost Srbija, Beograd, 2004,
11. Privatization Act (Official Gazette RS no. 83/14, 46/15, 112/15, 20/16)
12. Štiglic J. "Kuda idu reforme? Deset godina tranzicije ", Smisao 8-9, 1999.
13. Stojiljković Z. Lavirinti tranzicije, Friedrich Ebert Stiftung, Beograd 2012.
14. The Shadow Economy in Serbia New Findings and Recommendations for Reform, March, 2013
15. https://radmilovicwebsite.com
16. www.usaid.gov
17. www.mfin.gov.rs
18. www.socijalnoekonomskisavet.rs
19. www.fren.org.rs
20. http://www.solidarsuisse-serbia.org

# Topic VII

# CYBERCRIME

# INTERNET OF INSECURE THINGS

**Dr Milan Čabarkapa**
School of Electrical Engineering, University of Belgrade
**Prof. dr Milan Prokin**
School of Electrical Engineering, University of Belgrade1
**Prof. dr Goran Šimić**
Military Academy, University of Defense, Belgrade
**Prof. dr Nataša Nešković**
School of Electrical Engineering, University of Belgrade
**Prof. dr Đurađ Budimir**
University of Westminster, London, United Kingdom2

**Abstract:** The term Internet of Things (IoT) is related to any object or device, which connects to the Internet in order to automatically send/receive data. Firstly, this paper will discuss IoT as a part of 5G wireless communications. Secondly, the paper will overview potential security issues in IoT networks as one of the main type of problems in IoT and 5G. The attackers on IoT networks can cause serious damages and industry distractions. Therefore, information security in this type of networks is more important than ever, in order to combat cybercrime.

**Keywords:** 5G, Internet of Things, information security, cybercrime, wireless communications.

## INTRODUCTION

IoT services,such as climate control or elderly people monitoring, offer several benefits for huge companies and end-users. There are many consumer-facing devices such as workout trackers, health observers, and home security systems. However, the most significant value for the economy is result of enterprise IoT applications, particularly those that focus on businesses. These technologies impact the most important industries such as manufacturing, agriculture, and infrastructure. Broken down by industry, the manufacturing sector appears to have the most to gain from the adoption of IoT, with connected factories increasing productivity, optimizing inventory planning, reducing waste, and saving on energy costs and equipment maintenance. The safety and reliability of complex industrial processes as well as greater energy and operational efficiencies are in focus of manufacturers in terms of how IoT products can advance them.[3]

In order to track environmental factors, help secure indoor and outdoor facilities, enhance information related to distribution centre and seaports, connected devices will play a main role in the future. From the perspective of manufacturers and supply chains, IoT tools and technologies can also help identifying inefficiencies or shipping delays, or confirming product integrity in lifetime way from production plant to a retail store. IoT devices are also

1 Email: proka@etf.rs.
2 Email: d.budimir@wmin.ac.uk.
3 P. Swathi, M. Sravani, "Fostering the advancement of Internet of Things", International Journal of Computer Science and Mobile Computing, Vol. 6 Issue 6, June 2017, pp. 285–288.

typically established in tasks in which rapid reaction and control are crucial, such as in the energetics industry. The companies can use this value-added data to eliminate inadequacies in businesses such as health care, transportation, energy, retail, manufacturing, etc.[4],[5]

Regardless of the industry, IoT tools could produce data that help companies to make better decisions with improved productivity, management, efficiency or quality. For instance, using sensors on the airplane during pancontinental flights can generate data that could be used to advance passenger's safety and flight supervision. Second example can be using of tens of thousands of telematics sensors for delivery vehicles in order to track engine performance and improve routing as well as to reduce fuel consumption and pollutant emissions. Thirdly, manufacturing facility operator with robotic assembly lines can reflexively track every action. Therefore, any issue can be solved instantly as they are detected, which decreases the impact on fabrication process.

Relationship between 5G technology and IoT is discussed in second section. The third section of the paper presents several cybercrime examples related to IoT technology. Main security issues and their impact on hacker's attack possibility are overviewed in fourth section. Finally, conclusion is derived infifth section.

## 5G AND INTERNET OF THINGS

To meet the demands for the higher data rates and developments of new services, 5G technology will have to use new spectrum above and below 6 GHz, introduce massive multiple input multiple output (MIMO) and define new air interface. The goal is to increase mobile data per area, number of connected devices, battery life while reducing end-to-end latency. The next generation of wireless network, 5G, is aimed at handling Gb/s data[6]and billions of users, devices and connections reliably and with a very low latency. 5G is a heterogeneous network with a variety of frequency bands ranging from below 6 GHz to almost 100 GHz. Indeed, a 5G wireless mm-wave communication network will be an appropriate medium to support a huge increase in outdoor and indoor high-speed wireless activities including watching HD videos & TV, playing HD video games and downloading large amounts of data. There is a consensus among industry and academia that 5G will eventually develop towards using mm-wave bands as more innovations in devices, antennas and signal processing reduce the mm-wave components and implementation costs.

A recent study released in 2016 by Rappaport's group[7]suggests that at mm-wave bands near optical network data rates (with 15 and 50 times higher bandwidth than the present entire cellular spectrum) are achievable by wireless transmission over a few kilometers in open environment. But, in built-up areas the line of sight range subsides. The problem with large signal attenuation and fluctuation including fading caused by static or dynamic scattering, reflection, diffraction and refraction of signals by obstacles in the transmission path can be resolved using the MIMO technology requiring multiple antennas at the transmitter and receiver. MIMO technology takes advantage of multipath and this can be provided even

4 "Industry 4.0 new digitization strategy", September 2016, available online: https://www.strategyand.pwc.com/media/file/Industry4.0.pdf.
5 "The Internet of Things Business Revolution", Information Age Report, September 2014, available online: http://www.information-age.com/internet-things-will-turn-hadoop-architectures-their-head-123458445/.
6 "5G technology evolution recommendations", 4G Americas, Oct. 2015.
7 G. R. MacCartney, Jr., S. Sun, T. S. Rappaport, Y. Xing, H. Yan, J. Koka, R. Wang, & D. Yu, "Millimeter wave wireless communications: New results for rural connectivity", All Things Cellular'16, in conj. with ACM MobiCom, workshop, NY, Oct. 2016.

at mm-wave communications by slightly compromising the antenna pattern directionality (beam-width).[8,9,10]

IoTas a part of 5G offers an environment of interconnected physical objects which capture meaningful data and communicate that information through IP networks and different kinds of software applications.Though different definitions of IoT exist today, it is agreed among researchers that smart objects, machine-to-machine communications and radio frequency (RF) technologies are the integral aspects of IoT. While many other emerging technologies could contribute to the development of IoT, with the recent trend it is evident that *radio frequency identification* (RFID) technology will shape a key part of IoT.[11]

According to the predictions of Gartner, Inc.[12], by the year 2020, there will be nearly *26 billion devices* on the Internet of Things.There will be various types of devices that would participate in it, some of which may not use RFID, but for automated identification of most of the objects and people in IoT, RFID will surely play a very critical role. We have recently seen noticeable advancements in RFID technologies, but there still remain many other issues and considerable scope of improvement of services via RFID technologies.[13]

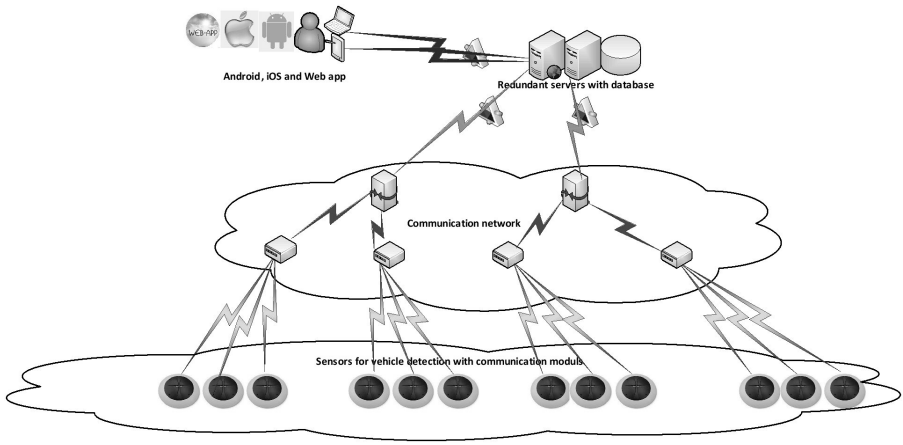



*Figure 1.IoT smart parking service architecture.*

IoTconsists of sensors and smart things/objects that are connected to the Internet anytime, anywhere. Acting as a perception layer of IoTs, the wireless sensor networks play an important role by detecting events and collecting surrounding context and environment information.Since sensors are battery powered, replacing the batteries in each smart object/thing/sensor is very difficult to implement. For sustainability of network operations, energy

8 E. Bjornson, E. G. Larsson, and T. L. Marzetta, "Massive MIMO: Ten Myths and One Critical Question", IEEE Communications Magazine, Vol. 54, no. 2, 114–123, Feb. 2016.
9 R. Heath et al, "An overview of signal processing techniques for millimeter wave MIMO systems", IEEE J. on Selected Topics in Signal Processing, Vol. 10, No. 3, 436–441, Apr. 2016.
10 S. Sun et al, "MIMO for millimeter-wave wireless communications: beamforming, spatial Multiplexing, or both?", IEEE Communications Magazine, 110–121, Dec. 2014.
11 "The internet of things: mapping the value beyond the hype", McKinsey&Company Report, June 2015, available online: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx.
12 "Gardner IoT technical study", available online: http://www.gartner.com/newsroom/id/3598917.
13 "ETSI RFID standard", available online: http://www.etsi.org/deliver/etsi_tr/102400_102499/102449/01.01.01_60/tr_102449v010101p.pdf.

harvesting and energy management technologies have obtained much attention recently. Energy management is the most important technology for prolonging the network lifetime of Wireless Sensor Networks (WSNs). The design of efficient energy management covers several layers, including physical, MAC, network as well as application layers.[14]

There are several smart IoT distributed systems. One of them is smart parking IoT system shown in Figure 1. It can be seen that there are four parts of this system: sensors that detected vehicles, communication network used for distribution of detection information, redundant servers with database for storing detection information as well as client web and mobile application for presentation of detection information. As will be shown in next section, this distributed architecture with several different function nodes is much more vulnerable to cybersecurity attacks than previously implemented centralized IT systems.

## IOT CYBERCRIME EXAMPLES

Cybersecurity will be one of the main engineering topic in 21st century. Business Intelligence forecast[15] shown in Figure 2 demonstrates that the IoT technology impact increases ten times from 2015 to 2020. Moreover, one can see that Connected Car, Smart Wearables and Connected TV, separately presented in Figure 2, could be also considered as IoT applications. Therefore, IoT cybercrime impact is even greater in total security market.

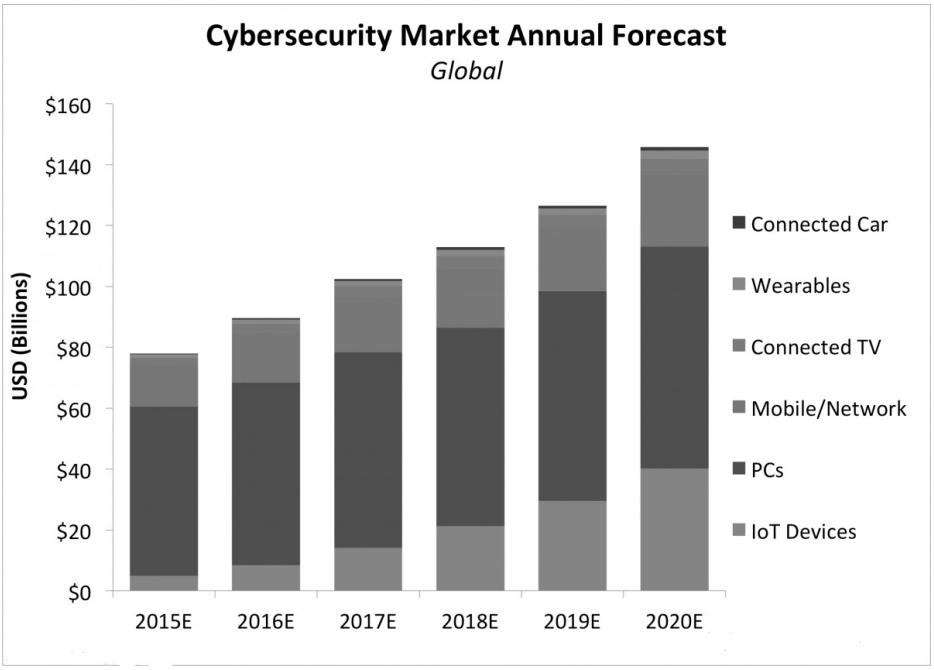



*Figure 2.IoT cybercrime impact in global cybercrime annual forecast (Source: BI).*

14 F. Labeau, A. Agarwal, B. Agba, "Comparative study of Wireless Sensor Network standards for application in Electrical Substations", 2015 International Conference on Computing, Communication and Security (ICCCS), December 2015.
15 "Business Intelligence cybercrime report", available online: http://www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3.

There are several types of cybercrime related to IoT. In this paper,the most important issues related to IoT cybercrimes will be discussed:[16,17]

- Smart vehicles paradigm is becoming one of the main IoT industry goals. The state-of-the-art literature recommends standards, such as ZigBee, Passive RFID, UWB or 60 GHz mmW technology. There are many potential holes in security of these wireless standards, and this is the major cybersecurity issue in the 21st century. It should be underlined that cybercrime examples in this field such as getting direct wireless connection to the car components and controlling vehicle's driving, obtaining access to the car's diagnostic equipment or blocking garage entrance or car entrance could be enormously dangerous mainly for the human lives.

- Safety cameras used by private companies or integrated cameras on baby monitors used in homes and day care centres can be attacked by the cyber criminals. This is due to the fact that they can take the advantage of security oversights in the configuration of closed circuits television. Majority of these devices have default passwords that cyber criminals are easily aware of and broadcast their location to the Internet. These systems are not properly secured and can be positioned and broken by cyber actors who wish to live stream video content on the Internet for anyone to see. In order to decrease this type of cybercrime, any default password should be changed as soon as possible, and the wireless networks must have a strong passwords and firewalls.

- A serious destruction could be caused if criminals gain access to unprotected devices used in home health care systems, such as those used to collect and transmit personal health monitoring data or systems used for delivering medicines. Once cybercriminals have broken these systems, they gain access to personal and medical information stored. They also can change the coding controlling process for the dispensing of medicines or health data collection. All these devices may be attacked especially if they are set for long-range wireless connectivity.

- Criminals in a cyber space can attack unsafe wireless connections for programmed devices, such as security systems, automatic garage doors, smart thermostats and smart home lighting. These exploits allow cybercriminals to get administrative privileges on the automated systems. If the criminals have obtained the owner's privileges, they could access the home/business network and accumulate personal information or distantly observe the owner's behaviours and network traffic. If the owner did not change the default password or create a strong password, criminals could easily access these devices to open smart doors, turn off home safety systems, record audio and video material, and have access to other important and sensitive data.

- Cybercriminals are also using home-networking routers, connected multi-media centres, TVs, and home appliances having wireless network connections as the input vectors for sending malicious email messages. In other words, email spam attacks are not only sent from PCs, laptops or personal mobile devices. IoT devices and systems are usually risky because the factory default password is used even in IoT system production phase or the wireless network nodes are not secured properly.

- Smart locks are used in various types of IoT devices (for instance Samsung's open SmartThings platform). These locks are popular standard among the world of smart devices. As it was demonstrated in research lab, various vulnerabilities in the tech would permit cybercriminals to capture pin codes, reset them, or even worse produce a few secret ones for their own usage.

16 "Cyber Security and Resilience of smart cars", ENISA EU cyber security report, December 2016, available online: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/at_download/fullReport.
17 "FBI Public Service Announcement", available online: https://www.ic3.gov/media/2015/150910.aspx.

- IoT application in industry can cause serious problems as well. For instance, there was one attack in iron manufacturing company. During this attack, the hackers were able to gain access to the production process and cause explosions inside the production floor, causing enormous damage to the equipment inside the factory. This attack put in danger both human lives and highly expensive equipment. The interruption of the manufacturing process is the lowest damage that can occur during this type of IoT cybercrime.

- Business-critical systems are also vulnerable and can be attacked by cybercriminals through the Internet. For example, this system can be the monitoring systems on gas pumps. Using wireless internet connection, the cybercriminals could effect that the pump register incorrect levels. On one hand, they can create a false gas shortage. On the other hand, they can allow overfilling the tanks in vehicles and create a fire hazard. They can also interrupt the connection to the point of sale system. In this case, fuel can be dispensed into vehicle without registration of money transaction.[18]

## MAIN IOT CYBERSECURITY PROBLEMS

In this section we are going to overview the main problems related to IoTcybersecurity which cause previously reported cybercrime types.[19]

**Insecure IoT cloud interface**

Testing of mobile app has showed that seventy percent of developed IoT systems use cloud-based web interfaces. Unfortunately, it was discovered that all these web interfaces exhibited account enumeration problems. Valid user accounts can be recognised through the http feedback messages received from reset password procedures, login pages or sign-up pages. Majority of implemented IoT systems allow unrestricted account enumeration through its cloud-based web interface.

**Insecure IoT mobile interfaces**

Fifty percent of IoT systems tested exhibited account enumeration concerns with their mobile app interfaces. Identically as with cloud interfaces valid user accounts can be identified through feedback received from reset password procedures and login information inputs. Half of IoT systems allow unlimited account enumeration through their mobile app interfaces.[20]

**Insecure IoT software and firmware**

There are a lot of problems during software and firmware updates procedures that cybercriminals can use in order to attack IoT systems. Majority of developed IoT systems do not protect firmware update procedures including transferring updates without any encryption or without encrypting main update files. In many cases, firmware has been updated via standard FTP protocol allowing cybercriminals to capture credentials or to give an attacker write permission to the server where update files are stored. It was shown in experiments that more than fifty percent of IoT systems offer any kind of protection during update procedures. Moreover, majority of the systems do not provide any kind of user control weather to accept or decline firmware or software updates. There was no system tested in these experiments that indicate the latest firmware date and version. These facts give several opportunities to attackers to cause the serious damages in IoT systems.

18 "FBI Public Service Announcement", available online: https://www.ic3.gov/media/2015/150910.aspx.
19 "Hewlett Packard IoT research study", available online: http://files.asset.microfocus.com/4aa5-4759/en/4aa5-4759.pdf.
20 "OWASP Insecure mobile interfaces report", available online: https://www.owasp.org/index.php/Top_10_2014-I7_Insecure_Mobile_Interface.

**Lack of IoT transport encryption**

Transport encryption is crucial for all communications through the Internet in order to guard delicate IoT data such as personal information and credentials, private video material, device safety settings, etc. The importance of properly configured transport encryption is especially important since security is a primary function of these home security systems. While all systems implemented transport encryption using SSL/TLS standard, it was discovered recently that many of the cloud IoT connections are vulnerable to the cyber-attack even if SSL v2 standard is used. The recent research work has showed that incorrectly set up or poorly implemented SSL/TLS is case in about fifty percent of operative IoT systems.

**Insufficient authentication and authorization in IoT systems**

There are several vulnerabilities such as weak passwords, unconfident password recovery procedures, poorly protected personal credentials, and many other gaps that cyber attackers can use to gain admission to anIoT system.

All IoT systems that included their Web and mobile interfaces failed to require passwords of sufficient complexity and length with most only requiring a six character alphanumeric password. Most systems also do not have the capability to lock accounts after a certain number of unsuccessful login attempts. These problems could lead to account collecting, which permits an attacker to guess login credentials and thus, have access to the system. There are single systems offered two-factor authentication. However, only one implemented ID for authentication to the mobile application interface (Apple's Touch).

Furthermore, majority of these systems include the ability to insert new users to the system. Even if the new users are known from the perspective of person who adds them, the additional accounts typically use weak passwords, therefore allowing access to IoT facilities.

Almost all IoT systems allow the use of unsecured passwords. Moreover, almost all do not possess an account lockout mechanism that would stop automation cybersecurity attacks. Recently, majority of IoT systems were vulnerable to account harvesting, allowing attackers to easily guess login credentials and gain system access. Majority of IoT systems that had cameras inherently give the owner the ability to provide video access to additional users, further increase probability of account harvesting cybercrime. Furthermore, there are IoT systems that allow video to be streamed locally without any authentication.[21]

**IoT privacy concerns**

All IoT systems store some kind of personal information such as name, address, date of birth, phone number, and credit card numbers. Stealing of this personal information as a result of the account enumeration issues or weak passwords usage is a serious issue in IoT wireless communication systems. One can see that the use of video is a key feature in several IoT systems. These systems carry data privacy concerns especially in situations when the privacy of video images from inside the home due to the use of video cameras can be a target of cybercriminals. It is frightening that majority of video streaming available through IoT cloud-based web interface or mobile app interface is completely unsecured.

## CONCLUSION

The overview of recent IoT technologies as a part of 5G technologies and its cybersecurity related problems have been presented in this paper. Different types of IoT cybercrimes were discussed in detail. The main problems have been detected and overviewed. One can see that

21 "HP IoT research study", available online:https://media.scmagazine.com/documents/88/hp_-_internet_of_things_21971.pdf.

the IoT problems related to cybersecurity will be one of the main engineering problems in 21st century. It has been shown that IoT cybercriminals can cause huge distractions in our everyday life. Therefore, in order to protect people and things, information security is much more essential than ever. It can be concluded that there will be several tasks for IoTcybersecurity engineers in the future in order to stop the process of Internet of Things becoming Internet of Evil Things.

## REFERENCES

1. "5G technology evolution recommendations," 4G Americas, Oct. 2015.
2. "Business Intelligence cybercrime report", available online: http://www.businessinsider.com/cybersecurity-report-threats-and-opportunities-2016-3.
3. "Cyber Security and Resilience of smart cars", ENISA EU cyber security report, December 2016, available online: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/at_download/fullReport.
4. E. Bjornson, E. G. Larsson, and T. L. Marzetta, "Massive MIMO: Ten Myths and One Critical Question", IEEE Communications Magazine, Vol. 54, no. 2, 114–123, Feb. 2016.
5. "ETSI RFID standard", available online: http://www.etsi.org/deliver/etsi_tr/102400_102499/102449/01.01.01_60/tr_102449v010101p.pdf.
6. F. Labeau, A. Agarwal, B. Agba, "Comparative study of Wireless Sensor Network standards for application in Electrical Substations", 2015 International Conference on Computing, Communication and Security (ICCCS), December 2015.
7. "FBI Public Service Announcement", available online: https://www.ic3.gov/media/2015/150910.aspx.
8. G. R. MacCartney, Jr., S. Sun, T. S. Rappaport, Y. Xing, H. Yan, J. Koka, R. Wang, & D. Yu, "Millimeter wave wireless communications: New results for rural connectivity", All Things Cellular'16, in conj. with ACM MobiCom, workshop, NY, Oct. 2016.
9. "Gardner IoT technical study", available online: http://www.gartner.com/newsroom/id/3598917.
10. "Hewlett Packard IoT research study", available online: http://files.asset.microfocus.com/4aa5-4759/en/4aa5-4759.pdf.
11. "HP IoT research study", available online: https://media.scmagazine.com/documents/88/hp_-_internet_of_things_21971.pdf.
12. "Industry 4.0 new digitization strategy", September 2016, available online: https://www.strategyand.pwc.com/media/file/Industry4.0.pdf.
13. "OWASP Insecure mobile interfaces report", available online: https://www.owasp.org/index.php/Top_10_2014-I7_Insecure_Mobile_Interface.
14. P. Swathi, M. Sravani, "Fostering the advancement of Internet of Things", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.6, June 2017, pp. 285–288.
15. R. Heath et al, "An overview of signal processing techniques for millimeter wave MIMO systems", IEEE J. on Selected Topics in Signal Processing, Vol. 10, No. 3, 436–441, Apr. 2016.
16. S. Sun et al, "MIMO for millimeter-wave wireless communications: beamforming, spatial Multiplexing, or both?", IEEE Communications Magazine, 110–121, Dec. 2014.

17. "The Internet of Things Business Revolution", Information Age Report, September 2014, available online: http://www.information-age.com/internet-things-will-turn-hadoop-architectures-their-head-123458445/

18. "The internet of things: mapping the value beyond the hype", McKinsey&Company Report, June 2015, online:https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx.

# POSSIBILITIES FOR COMPARISON OF DATA RECOVERY SOFTWARE FOR MOBILE DEVICES

**Dragan Randjelović PhD**
Academy for Criminalistic and Police Studies
**Aleksandar Miljković**[1]
**Vladimir Stojanović**
**Vladimir Jovanović**
**Aleksa Maksimović**

**Abstract:** The significance of information has been growing hand in hand with the advancement of technology and proportionally to the growth of its significance, both for the individual and for the corporate business. The information themselves are getting more important and can easily become crucial in and present the basis of the work of individuals and modern organizations. In order to be able to manipulate data safely and without any concern, in the terms of their storage and sharing, systems have been developed to save or recover lost data in case of an accidental delete or corruption by an unwanted software. Concerning the above mentioned, the focus of this paper will be on the comparison of potentials of Data Recovery Software (DRS) for mobile devices in four aspects: 1) success in data recovery, 2) elapsed time of data recovery, 3) operating system compatibility, 4) operating systems used to run Data Recovery Software. The term of success in data recovery of DRS means the probability of success for the software to salvage deleted or corrupted content from mobile device memory. Elapsed time of data recovery of DRS is the time necessary to recover the data and it runs from the start of the process to the moment in which the wanted data has been recovered, and that can be divided into three types: text files, audio files and image files. Besides these two aspects, DRS can be differentiated by the compatibility with the operating systems it should recover data from and the type of operating systems Data Recovery Software can be run from. A case study was done on a random sample of text files, and also on audio and the video type data.

**Keywords:** data recovery, mobile, comparison, Data Recovery Software

## INTRODUCTION

Along with the advancement of technology, proportionally to the growth of both its importance for the individual as well as for the corporate business, grows the importance of information. The information itself gains value, can easily be of crucial significance and represents the basis of work done both by modern organizations and individuals. In order for such important information to be available at any moment, in contrast with the personal computers which are static, the users demanded to always be in touch with their information. Thus, the manufacturers have designed the portable computer technology which enabled the users to have constant access to their personal and business information. Following the further advance of technology, the mobile phone was, until recently, used only for communication purposes.Today, alongside the technological developments of web clouds and the ever

1 miljkomocnik@gmail.com

decreasing size of computer components, it is becoming a device which, together with the possibility of mobile communication, offers the ability to manipulate data by using personal or portable computers.

In order to safely manipulate the data in terms of storage and communication exchange, systemswhich can preserve or restore data lost by unintentional deletion from the device memory or through corruption by unwanted software have been developed. Moreover, some of the data can be deliberately deleted by the user in order to conceal specific information.

Taking everything into account, this paper will deal with the comparison of the capabilities of Data Recovery Software (DRS) for mobile devices.This will raise awareness of the possibilities of salvaging data and that a deleted piece of data is never forever lost, but that it always remains hidden in the device's memory until it is necessary to completely rewrite it with new data.

The paper is divided into four chapters which will cover the stated analyses. Chapter 'Tools' will explain why special DRS tools for mobile devices are necessary and will list the tools which will be used. 'Case Study' chapter will define the main postulate of each experiment which needs to be carried out on each DRS used in the research. 'Jihosoft Android Phone Recovery' will describe the experiment on DRS carried out by the company 'Jihosoft' and present the results of the experiment. 'Wondershare dr.fone for Android' will focus on testing and describing the DRS from the company Wondershare and show the results for this software. 'Final Considerations' will in the end compare and give the final evaluation of each piece of the experimentally tested software and literature.

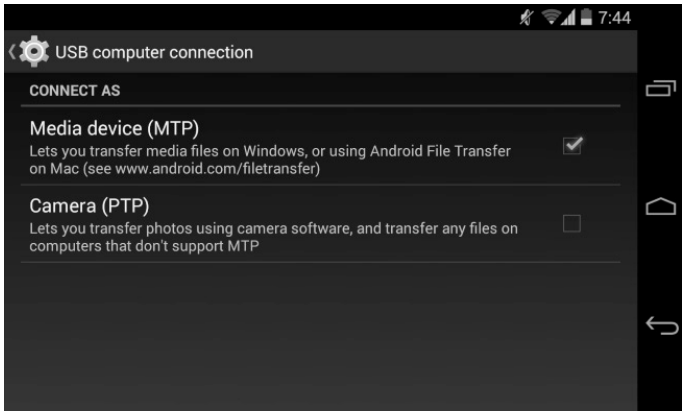
## TOOLS

One of the most frequently used tools for Data Recovery in the world is Piriform's **Recuva**. This software offers the possibility of file recovery from a computer, but along with this primary function allows the possibility of their retrieval from memory and micro SD cards which are used as memory storage upgrades in mobile phones. This tool searches only for the deleted files, and afterwards executes a deeper analysis of possible retrievals and the quality of the discovered files. After the process finishes, it presents the user with the list of discovered files together with the display of the possible quality the files can be recovered in (a red circle indicates unsatisfactory quality, an orange circle indicates acceptable quality and a green circle indicates excellent quality). It also offers the possibility to reviewthe file first, but it depends on the quality of the discovered file. More recent Android and iOS devices use MTP and PTP protocols for communication while communicating and transferring files with a computer. Android operating systems used to use USB mass storage as a way of communication.

**USB mass storage** is the standard protocol used by flash drives, external hard drives, SD cards and other USB storage devices. The device which communicates with the computer via this protocol offers complete accessibility to the computer. Once a device is connected with the computer using this protocol, the device would disconnect from the Android operating system which would have been run on the device (Picture 1). Moreover, in order to establish the communication with Windows operating systems for this type of connection, the memory system on the device has to be compatible with the Windows operating system, which would require the Android devices to contain FAT memory systems. FAT file system is older and slower than some more recent systems like ext4. Even though the connection between the phone with the computer via the standard USB memory device is highly practical, especially in the case of Data Recovery, this protocol had too many disadvantages and had to be replaced with the MTP protocol which would deal with them.


*Picture 1. Display of the Android OS status while communicating with the computer via USB mass storage*

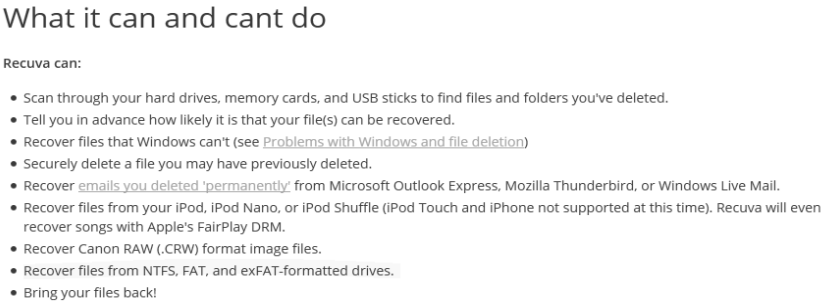
The **MTP** protocol functions differently from the USB mass storage (Picture 2). Instead of displaying raw data from the mobile phone to the operating system, MTP functions on the level of files. The mobile device cannot display all of its memory to the computer. Instead of that, when a mobile device connects to the computer, the computer sends a query to the device, and the device answers with a list of files and directories. The computer can then transfer the file by sending a request to the device to send it. The deletion of files and the transfer of files from the computer to the mobile device functions in a similar way. In this manner the device is protected from possible damage. The PTP protocol and iOS mobile device protocols work on a similar principle.




*Picture 2. Display of the screen status while connecting more recent mobile devices with Android operating systems with the computer*

Recuva doesn't offer the possibility to access the memory connected via MTP protocols, but it is convenient when the mobile device itself suffers physical damage and there is no way to recover the files from its internal memory. Nevertheless, if there was a micro SD card inside the device (in case it did not suffer major physical damage), it would be possible to recover the data via this tool. This possibility makes it completely independent from the OS of the mobile device. However, Recuva is supported only by Windows OS computers and is therefore restricted from working on other operating systems.

Another problem which Recuva tackles while working with Android operating systems concerns the types of file systems. Namely, on its web page, Piriform states that their Tool for data recovery is supported only by NTFS, FAT and exFAT file systems (Picture 3). EXT4, as well as F2FS and VFAT file systems are the most common file systems supported by Android. That way, even by rooting the phone (which will be discussed in the third chapter of this paper) and installing additional software on the mobile device which enables FTP communication or some other type of protocol in order to establish the communication, software such as Recuva would not be suitable for this type of data recovery.




*Picture 3. Piriform's Web Page*

For the reasons stated above, Recuva and similar DRS tools designed for computers are not suitable for data recovery from mobile platforms. Having that in mind, tools were chosen which were adjusted to recover data from mobile phones. Some of the most represented DRS products encountered by a common Android or iOS platform user were chosen which, along with their ease of use in all respects are also very diverse in terms of file type. The chosen software products are:

- Jihosoft Phone Recovery
- dr.fone Data Recovery

These two software products were chosen as the most demanded in the global market.

## JIHOSOFT ANDROID PHONE RECOVERY

This tool for data recovery offers the possibility of recovering deleted files for the most popular Android brands, including Samsung, HTC, LG, Sony, Motorola, ZTE, Huawei, etc. It also supports all versions of Android OS, including the newest Android 7.0 Nougat. Jihosoft IPhoneData Recovery software represents the version of this software which allows working with Apple mobile devices. Along with the Windows version which we used for this experiment, a Mac version is also available for Mac operating system. This software has four versions, two of which work on Windows OS, one of which allows the recovery of data from iOS and Android OS, and two of which can do the same thing on Mac OS.

The software was downloaded from Jihosoft's official website (http://www.jihosoft.com/android/android-phone-recovery.html).

## DR FONE WONDERSHARE

Dr.fone Android Data Recovery is a part of a software package dr.fone toolkit, developed by the company Wondershare. It is one of the first tools for recovering lost data from mobile devices with Android OS. Together with Android Data Recovery tools for recovering lost data, there is an iOS Data Recovery tool for iOS mobile devices.

It is also possible for the user to download a free trial version in order to scan the device first, if the user is not sure whether data recovery is plausible or not. Afterwards, the user can check the discovered data which is possible to recover. This software for recovering lost data from Android mobile devices enables the retrieval of deleted or lost contact information, text messages, photos, WhatsApp messages, sound files, video files, etc.

On their Internet page, https://drfone.wondershare.com/android-data-recovery.html, dr.fone, Wondershare states that it is possible to use this application to recover data from an Android device on over 6000 Android mobile telephones and tablets from companies such as Samsung, HTC, LG, Motorola, ZET, Huawei, etc.

This software for data recovery from Android OS mobile devices is capable of only reading telephone or tablet files. It does not modify, keep or transfer data from your device to other parties. All users of this program will be able to enjoy free upgrades in the future. Customer service is also available.

## CASE STUDY

In order to carry out the mentioned examinations, it is necessary to perform a case study ('experiment' from now on) which will essentially present the analysis of implemented procedures of data recovery under clearly defined conditions and on clearly defined devices.

Text, audio and video types of data were used during the comparison. Text files used were files in DOCX standard. Audio files used were M4A files, while the video or, more precisely, image files used were in JPG standard. These standards were chosen as the most represented standards in mobile devices.

Test files were defined the same way the file type standards were: the **image** example (Picture 4) with JPG standard named "grb kpa" ("KPA crest"), the **audio file** which is five seconds long with M4A standard, named "KPA", the **text file** with the title "Kriminalističko-policijska akademija" ("The Academy of Criminalistic and Police Studies"), named "KPA test" with DOCX standard. The three test files (photo, audio file and text document) were placed in the device memory before the beginning of the process, and later deleted with the intention of discovering them later with the tools mentioned.


*Picture 4. Image test file*

Together with these basic file types which this paper will consider, these software products offer the possibility of recovering data such as messages – for example different software solutions for message exchange, contact information, message attachments and call history. Even though this paper deals with examining three file types exactly, we will emphasize that it is important that each software product offers additional possibilities together with the already mentioned basic ones.

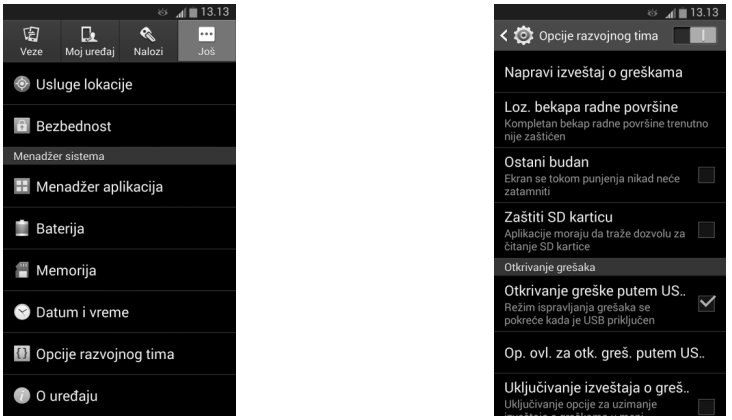
While evaluating the software by criteria, we will use scores from 1 to 3, 1 representing the weakest, 2 the moderate, and 3 the best score. The comparison will be performed according to the following criteria:

- The amount of discovered data, i.e. the number of discovered files on the analyzed mobile device
- Time elapsed from the moment the device started being analyzed until the end of the scan
- The number of supported operating systems of mobile devices from which it is possible to recover data via the tools mentioned
- The number of operating systems from which the software is run

Samsung Galaxy S3 with the Android OS, version 4.3, was used for this experiment, with the total working memory capacity of 16GB. The performance of the computer used to run this software is: processor Intel i5 2.30GHz; RAM memory 4,00GB; operating system Windows 7 Home Premium 64-bit with a stopwatch software.

A software supplement Blue Stopwatch was used in the part of the experiment dealing with the measure of the time elapsed during the analysis and scanning of the mobile devices. This tool was downloaded from thewebsite win7gadgets.com.

An essential thing to do while working with every software product is to establish a physical connection with the computer via the USB cable. Afterwards, it is necessary to use the mobile device to enable the software's access to the system files via the USB connection. This is done by ticking the option for error correction via USB in the developer options.




*Picture 5. The adjustments were done on Samsung Galaxy S3, Android OS Version 4.3*

In order to access the part of the memory containing the deleted files, each of these software products requires working with rooted mobile devices. Rooting represents a procedure which gives the user administrator privileges and, by the same token, allows them to access the root folder. If the telephone goes through the rooting process, in the majority (if not all) cases, the telephone user will lose the warranty granted by the manufacturer or supplier.

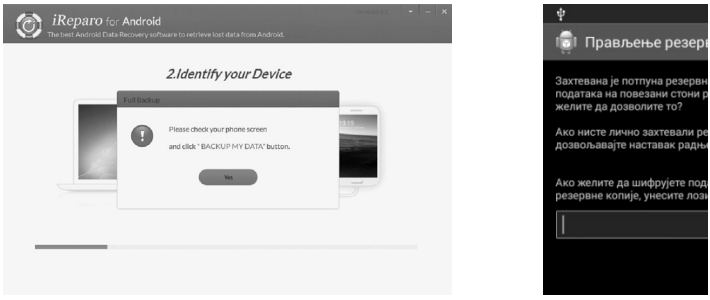
Moreover, if the rooting process of the telephone was not performed successfully or was interrupted, either due to the power outage or the negligence of the person performing the process, it could lead to the loss of all data. Therefore, inexperienced users are not advised to perform the rooting procedure.

The chosen tools for recovering lost data from mobile devices with Android OS work on both rooted and unrooted Android devices, i.e. the rooted device will remain rooted, and the unrooted device will remain unrooted after the process. During the data recovery process, if it is necessary, the software will perform the mobile device's OS rooting by default and will, upon finishing this process, return the mobile device's OS to its previous state.

## JIHOSOFT PHONE RECOVERY

When running the software, the communication connection is first established between the software and the mobile device, during which it is checked whether all of the actions related to the mobile device options are in order before the communication starts. If yes, it performs the finalization of establishing the connection and allows the possibility of starting the process of analysis or the search for deleted files. Establishing the connection and its check take longer than what is usually expected, sometimes showing that some settings were not applied, where, in fact, it takes more time to obtain the confirmation. It shows a highly-detailed display of solutions for each problem in order to accelerate the continuation of the process.

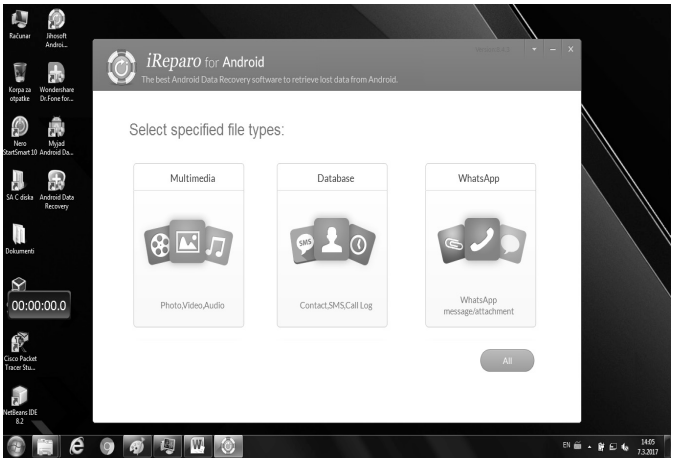
While setting up the connection and checking the correctness of the communication, the software prompts the user to create a "Reserve copy of all files" on their mobile device (Picture 6), which further secures the files after the process ends.




*Picture 6. The software's prompt for creating a reserve copy on the mobile device (left) and the menu for creating a reserve copy on the mobile device (right)*

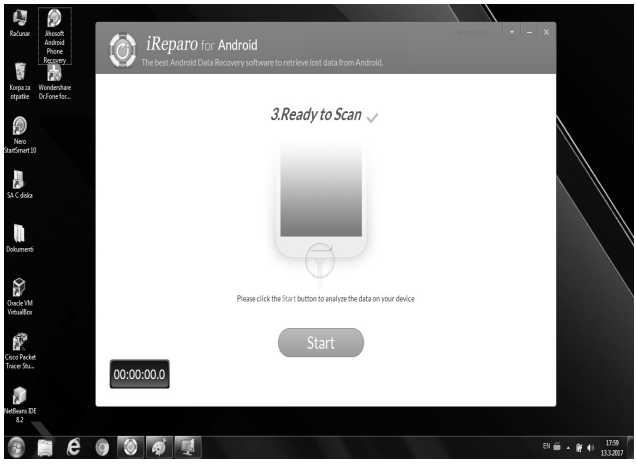
1. After the successful initialization with the mobile device, a window appears which allows the users to choose the type of files they want to recover (Picture 7). The available types are: Multimedia (Photos, Video, and Audio); Database (Contact information, SMS messages, and call history); WhatsApp (WhatsApp messages and message attachments). Seeing that we opted for photos, we will use the option "Multimedia". Since the experiment was done on the photo, text and audio files, we will select the option "**All**", with which we will search for all file types. The software offers the possibility of searching for the file in **Photo** formats (JPG, PNG, GIF, BMP), and it also offers to search for the photos located only in the "Gallery" directory, with which we can avoid looking through numerous photos from web pages, applications, etc. Moreover, it offers the possibility to search for the file in **Video** (MP4, 3GP, AVI, MOV, WMV, 3G2, M4V, MXF, FLV, SWF, MPG, TOD, MTS, MXF) and **Audio** formats (MP3, WAV, AIFF, MID, M4A, AU, OGG, WMA, AAC, RA, AMR, ACD, CAF, APE, RIFF). These are only the

multimedia file types that can be selected – other file types are searched through mandatory settings.



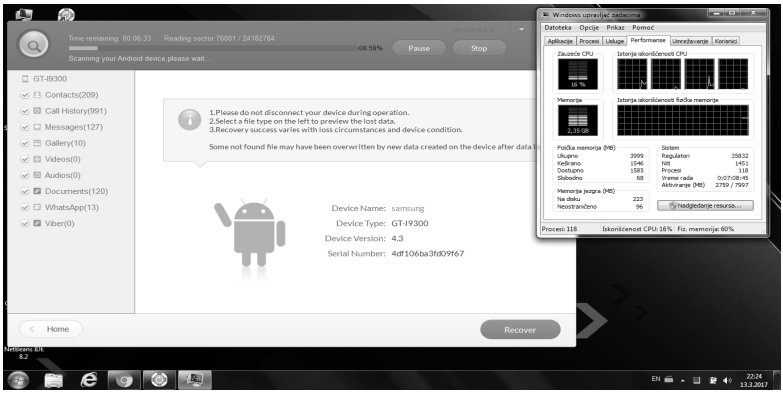

*Picture 7. Window with the options of the desired file format*

2. After choosing the desired formats we want to search for, the software performs a new connection check and notifies us that it is ready to scan the mobile device for the desired files after the check finishes (Picture 8). Clicking "Start"initializes the scan. The stopwatch is located in the lower left corner and it will be used to measure the time required for the complete scanning procedure.



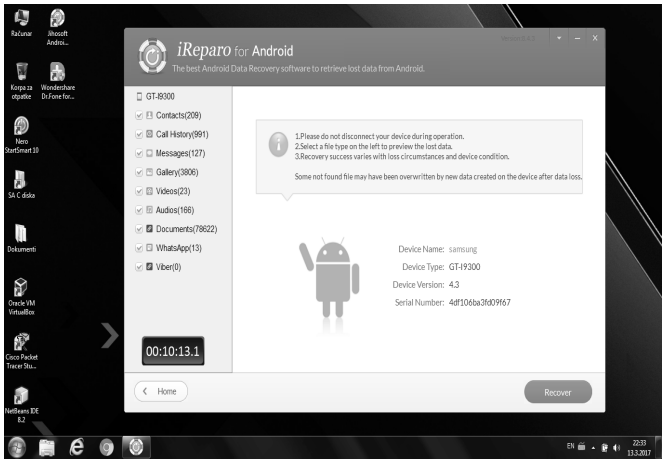

*Picture 8. Display of the window before the mobile device scan starts*

3. During the device scan, the processor activity did not increase significantly (from 12% to 16%), while the occupied RAM memory was around 2.35 GB, i.e. around 58% of the total capacity (Picture 9).




*Picture 9. Display of the computer's resources use during the scanning process*

4. The mobile device's scanning process lasted 10 minutes and 13 seconds, which can be seen on the stopwatch in the lower left corner of the screen (Picture 10). After the process finished, it offered the possibility of recovering all discovered files.




*Picture 10. Display of the end of the scanning process*

Among the discovered files, together with the originally defined ones, are also contacts, call history, messages, documents, WhatsApp, and Viber.

Jihosoft Android Phone Recovery software offers the possibility of recovering data under the following categories:

- **Contacts** (209) – While reviewing, it is possible to see the names (declared by the user of the mobile device), phone numbers (regardless of whether they were located on the SIM card or the device's direct memory) and e-mail addresses; contacts colored orange represent deleted contacts, while the ones in black are the contacts currently located on the mobile device;

- **Realized Communication History** (991) – offers the access to exclusively realized communication from the SIM card via the mobile device – both SMS messages and call history; with this option we have can have insight into the name of the person (if it is about a specific contact), telephone number, the date of the realized communication, type

(incoming or outgoing), and length (SMS messages were marked with 0 seconds); deleted communications are shown in orange;

- **Messages** (127) – the option which offers the possibility of displaying text messages, where a number of realized communications can be seen, which are almost always linked to the contact of the person and show the information about the date and time when the message had been sent or received; deleted messages are shown in orange;

- **Photos** (3,806) – the possibility of recovering the photos found on the device, depending on whether we chose the photos found only in the "Gallery" directory or all of the photos which have been read on the mobile device (in case we are interested in the applications which were used on the mobile device and from which websites the pictures were loaded, all of which can be used in the field of digital forensics); the discovered photos are declared in names different from their original ones, therefore our test file named "grb kpa" was discovered as a photo "17310320.jpg"; also, it is not possible to display all of the photos visually, which does not offer us many options when selecting individual photos and some of the photos are not in their full integrity;

- **Video** (23) – when considering the possibility of reviewing the discovered video content, the video recordings are declared individually, inspection of the video file format is allowed, the size and status which can be declared as either "Good" or "Bad", depending on the quality of the video file and the possibility of its review, which makes the individual search easier. However, among the 23 video files found, only one file allowed the possibility of a specific "review", because clicking on it results in playing the sound only, with a red background, which also shows that the file is not completely secured and that it is not possible to recover it in its original quality;

- **Audio** (166) – allows the recovery of audio files in originally defined formats, the names are declared by the software's defined criteria, which are not related to the original values, the size of the file, its format and status which is either "Good" or "Bad", the good quality of this software is illustrated by the possibility of listening to the audio files, and therefore the better coordination through the multitude of audio files;

- **Documents** (78,622) – among the basic documents which are usually of text type, files in PDF format were also found, but most of the files discovered were TXT files, along with the information about their sizes and statuses, without their original names and the possibility of reviewing them;

- **WhatsApp** (13) – display of text and multimedia messages realized via the mobile application WhatsApp, together with the display of the number of realized communications and the deleted messages and calls in orange;

- **Viber** (0) – even though the mobile application for sending and receiving messages of both text and multimedia content called "Viber" was installed on the mobile device on which the experiment was performed, no results were found when choosing this option;

The Jihosoft Android Phone Recovery software proved to be a tool which is useful for data recovery from mobile devices. However, it has shown various weaknesses as well. Establishing the connection with the mobile device lasts longer than usual, sometimes requiring the restart of the mobile device before its initialization because of possible difficulties during the device recognition. After successfully establishing the communication, the software requires that a reserve copy is created, which adds to the significance of the security and precaution factors during and after the process in case of unforeseen problems. The installation of the mobile application "MobileManager" is performed during the initialization on the device, 1.56MB in size, which enables the rooting required for the next step. This software's use is commercial and therefore, except for the possibility of scanning and the possibility of recovering data, it

does not allow the access to advanced features in its "trial version". A big disadvantage to this software is the fact that it declares the names of the discovered files by itself, which, considering everything, slows down the process of searching for the desired file. This software version is useful because it offers insight into SMS messages, contact information, the realized communication history, WhatsApp messages and attached files, along with the detailed display of intervals, dates, user-declared names, which, to a certain extent, helps us from the viewpoint of digital forensics.

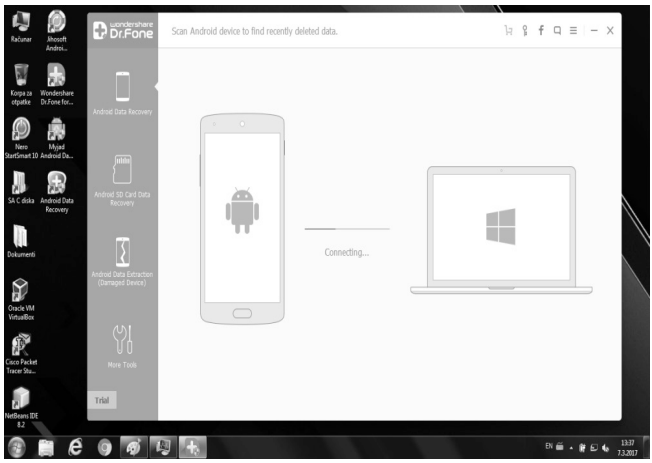
The advantage of this software is the possibility of reviewing and listening to video and audio files, which makes the choice of specific files we search for easier. This option is applicable to image files as well, but it is not available for all files. Some files were found to be more damaged that they really were, and some were not deleted in the first place.

From the first three types of test files mentioned – the image file, audio file and text file – the image file was discovered successfully but under a different name (17310320.jpg), the search for the text file was futile to say the least, because the search listed 78,622 files, with different names than the original ones, and, considering the audio file, even though it is possible to listen to the discovered files, none of them were in M4A format (the format type in which the test file was originally). In the end, we can say that one of the three original files was found successfully.

## DR FONE DATA RECOVERY

1. Running the software starts a window which graphically presents the process of establishing the connection between the device and the computer (Picture 11). Establishing the connection is performed automatically, without any additional manual operation. Of course, the software will prompt the user if the connection failed to establish and the reason. On the left side, the users can choose the device from which they want to recover the files. It offers the possibility of file recovery from mobile devices, SD cards and partial recovery of files from the internal memory of a damaged mobile device.

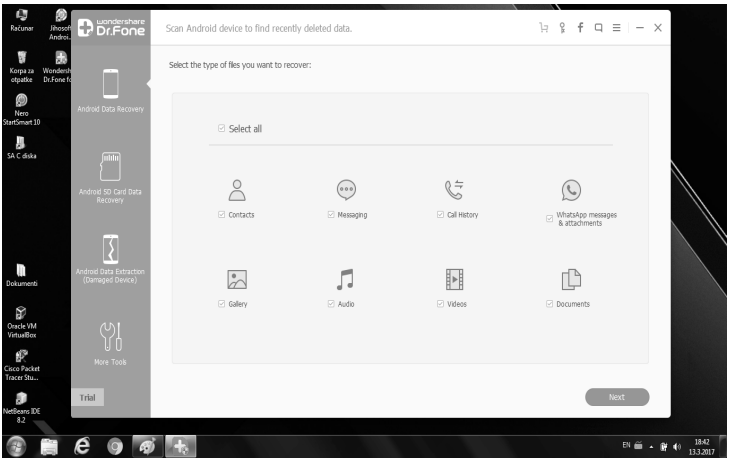
*In order to establish the connection, it is necessary to perform the mentioned settings on the mobile device.




*Picture 11. "Dr.fone" software's starting screen, displaying the process of establishing the communication between the mobile device and the computer*

2. After the establishing the connection, the software offers us the possibility of choosing the file type of the file we want to recover (Picture 12). The files which are possible to be re-

covered with this software are contact information with the option “Contacts”, text messages with the option “Messaging”, call history with the option “Call History”, photo galleries with the option “Gallery”, audio content with the option “Audio”, video content with the option “Video” and text files and similar documents with the option “Documents”. We will choose all file types by ticking the option “Select All”, and clicking the “Next” button afterwards.



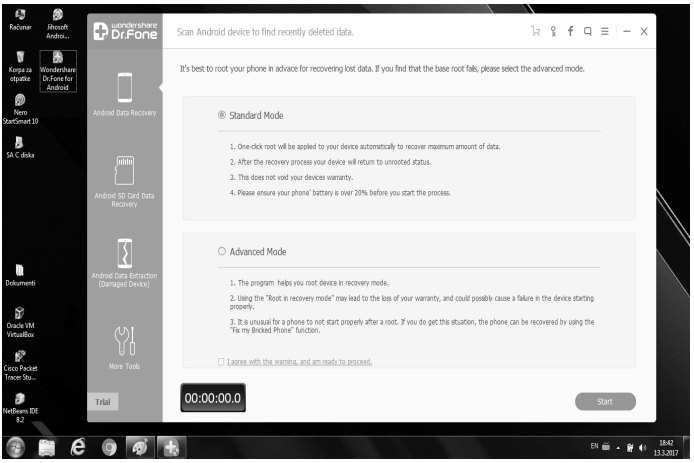

*Picture 12. Display of the menu where the users can check the file types they want to recover*

3. The next window offers two options of the scanning procedure:

- Standard Mode – enables automatic rooting of the mobile device without the user’s involvement

- Advanced Mode – requires the users themselves to do the rooting of the mobile device

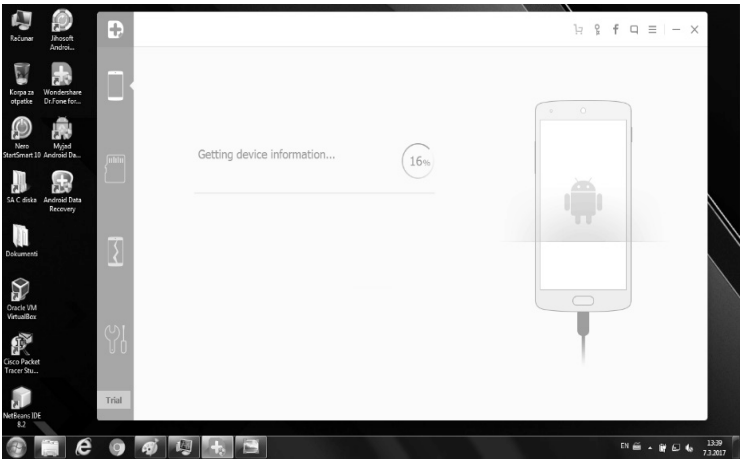
The stopwatch is positioned in the lower left corner (Picture 13), and we use it to establish how much time is required from the start of analyzing the device, through the scanning and until the final phase (display of the files which can be recovered).




*Picture 13. Display of the window where the users are prompted to choose the option in which the software will continue its process and the rooting mode*

This software does not offer the option of choosing the file extensions, but "roughly" searches for anything which can be considered a "photo". Also, the software offers the possibility ti recover all data and files from the above mentioned categories all at once. After choosing the file type, a search of the memory locations of the mobile device is performed, along with collecting additional information about the device which might help the software determine what to search for or where the file is located more precisely.

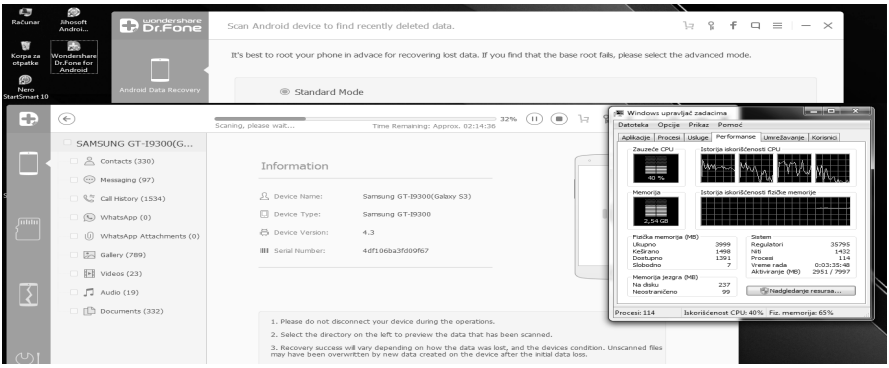
During the analysis of the device and collecting the information, we noticed that through the search, the software goes through a number of phases before the start of the device's scanning process, and at the same moment prepares the mobile device for the scan, which is seen through the restart of the device (all of this is done by the software, automatically).




*Picture 14. Display of getting the mobile device information needed for the continuation of the software's process*

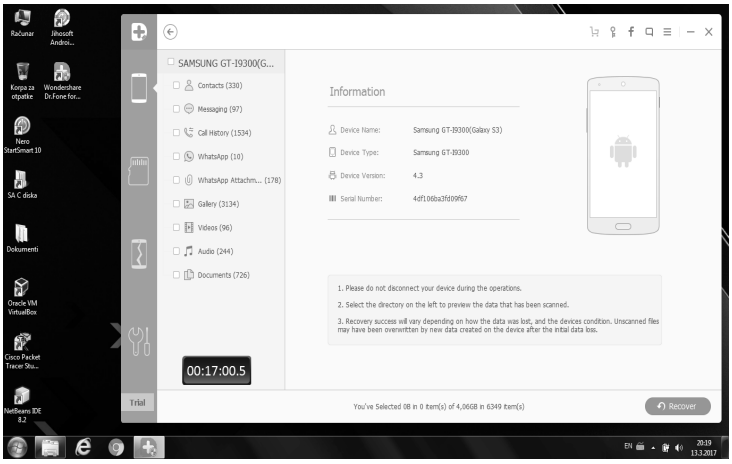
The process of preparation lasted for 4 minutes and 28 seconds, followed by the main scanning of the device, which can be followed through the window which offers the device information, the remaining time, as well as the percentage of the amount of work done (Picture 14).

4. During the scanning process, we noticed that the total processor usage was from 25% to 40%, and when it comes to the RAM memory usage, it amounted to around 2.54 GB, which is a little more than 60% of its total (Picture 14).

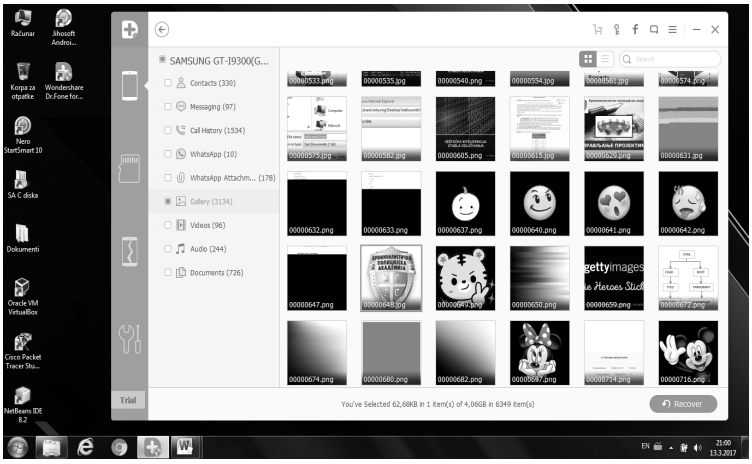



*Picture 15.Display of the use of computer's resources during the mobile device's scanning process*

5. The process of the main scan lasted for 12 minutes and 32 seconds, and the total time of both the device's preparation and the scanning process was 17 minutes, which can be seen on the stopwatch in the lower left corner of the window.




*Picture 16. Display of the last window with the results and the time spent during the process*




*Picture 17. Display of the discovered test photo*

"Wondershare dr.fone for Android" software offered the recovery of the following data after the scanning process:

- **Contacts** (330) – it is possible to have a look at the names (declared by the user of the mobile device), telephone numbers (regardless of them being on the SIM card or the device's direct memory) and e-mail addresses, as well as the option of further filtration in order to show a clearer display of deleted contacts only.

- **SMS messages** (97) – enables the display of all SMS messages realized via the mobile device, offers the possibility of looking at the name of the person with whom the user communicated through messages, their telephone number, the list of all text messages exchanged with that person, as well as the option of further filtration in order to show a clearer

display of deleted SMS messages only; number 97 does not represent the number of messages but the number of realized communications with the other person or group of people;

- **RealizedCommunication History** (1,354) – displays telephone numbers, names, dates, types (outgoing or incoming), length of a specific call, including the communication realized via e-mail and SMS messages, as well as the additional option of further filtration in order to show a clearer display of deleted communication history only;

- **WhatsApp** (10) - displays text and multimedia messages realized via the mobile application WhatsApp, as well as the number of realized communications;

- **WhatsApp Attachment** (178) – offers the possibility of checking sent or received multimedia content via the mobile application WhatsApp without a detailed display (the person who sent or received the content);

- **Gallery** (3,134) – offers the possibility of checking photos which are possible to be recovered, among which we found the test file (the crest of the Academy for Criminalistic and Police Studies), but with a few faults:

- The discovered photos were mainly those implemented into specific web pages or applications, and not photos usually found in the "Gallery", therefore most of them were worthless.

- Among the photos mentioned, some photos were, by some unaware users' actions on the device (through the zooming feature), saved on the device's memory, thus, the software found only segments of a particular photo, resulting in several individual photos, which greatly decelerates the search for the desired test file.

- All photos were declared by names generated by the software itself (an 8-digit number), which makes the search even more difficult because the test file was saved under the name "grb kpa", where the software discovered it under the name "00000647.jpg" after the search.

- Discovered photos are not chronologically ordered, which makes the search for the desired photo more difficult.

- The integrity of the discovered photos is not the same as original, there are significant differences in their wholeness.

- **Video** (96) – offers the possibility of checking the discovered video content, the problem with the names is the same as with photos, but an even bigger problem is the inability of reviewing the discovered content – you have to recover the data in order to review it, which requires more time and memory capacity;

- **Audio** (244) – offers the possibility of checking the discovered audio files, and the files found were usually with the ".m4a" extension, in which the files recorded on the mobile device are declared, and what is also lacking is again related to the names of the files – the software again declares new names on its own and the inability of listening to the files;

- **Documents** (726) – among the basic documents which are predominantly of the text type, some files with the ".zip" extension were found which means that the software can discover the "packaged" files as well, without detailed names or information

From the given experiment, dr.fone has shown that it can be useful in the search and recovery of files from mobile devices. The software showed excellent stability during its use, where no unexpected process cancellations or communication interruptions occurred. The communication establishment is performed as quickly as possible, the waiting time reduced to the lowest level, and, in case of insufficient options, the software redirects the user to the web page with instructions detailed and comprehensive enough for users who are not experts in the field of information technology. The additional requirements for the successful func-

tioning of the software itself and the implementation on the mobile device is that, during the analysis of the device, two more applications need to be automatically installed without the user's approval – "Dr. Fone for Android", 3.44 MB in size, and "Mobil Go", 16.07 MB in size. These applications are necessary because the rooting would not be possible without them, disabling the access to the internal memory of the mobile device. Furthermore, both of the applications remain in the mobile device after the process finishes. What needs to be mentioned also is that, during the analyzing process of the device, the mobile device automatically resets, which might lead to unwanted situations in case the mobile device was password-protected, for example with a "SIM code", but it will not hinder the software in finishing what it started.

The use of dr.fone is commercial, and requires specific financial investments for its complete utilization. In the given experiment, one of the three files tested was discovered, but we need to keep in mind that the experiment was done on the "trial version" of the software, therefore with limited possibilities and with the possibility to visually review only the photo test file, which is not the case with the text and audio files. However, a big drawback is the fact that the majority of the discovered files are declared in software-generated names, which makes the discovery of desired files more difficult. The fact which surely goes in this software's favor is that even this "non-commercial" version offers a detailed display of SMS messages, the communication history and contacts, WhatsApp messages and attachments, together with a detailed display of time intervals, dates, user-declared names, which might help much as an extension of the hand of digital forensics on mobile devices.

## FINAL CONSIDERATIONS

Dr.fone Data Recovery Software showed a much faster and secure connection establishment with the mobile device, while Jihosoft Phone Recovery had certain difficulties with recognizing the device and later with establishing a secure connection with it, together with displaying an error without a reasonsince the necessary adjustments were done immediately before the start and everything lasted longer when compared with dr.fone Data Recovery tool.

During the analysis and scanning process of the device, both pieces of software performed the mentioned processes without any delays, showing an almost identical visual display of the current status and the number of scanned sequences. The use of computer resources was shown to be higher while using dr.fone Data Recovery tool (+2% RAM memory and +10% CPU).

After the end of the experimental part of work of both software products, which included the scanning of the mobile device and the review of the files which can be recovered, the following results were obtained, which can be observed in the table given:

Table 1. The comparison of both versions of the software by the time spent and the number of discovered files

| | **Jihosoft Phone Recovery** | **dr.fone Data Recovery** |
|---|---|---|
| **TIME** | 10 minutes 13 seconds | 17 minutes |
| **CONTAS** | 209 | 330 |
| **CALL LOG** | 991 | 1354 |
| **MESSAGES** | 127 | 97 |
| **PHOTOS** | 3806 | 3154 |

| | | |
|---|---|---|
| **VIDEO** | 23 | 96 |
| **AUDIO** | 166 | 244 |
| **DOCUMENTS** | 78622 | 726 |
| **WhatsApp** | 13 | 10 |

The time spent during the scanning process is 58% higher with dr.fone Data Recovery, which in this case amounted to 6 minutes and 47 seconds. The display of the discovered contacts is larger with dr.fone Data Recovery, where the discovered contacts include both the deleted and undeleted contacts, together with the filtration option which results in the display of the deleted contacts only. Through the display of contacts we can also see the names which the users chose when saving them on their devices (regardless of them being on the SIM card or on the device directly). The communication history on both pieces of software include communications via regular calls, sending SMS messages, as well as sending e-mails, and dr.fone Data Recovery proved to be more efficient in all of them as well. When it comes to the number of discovered messages, including some e-mails, Jihosoft Phone Recovery found a larger number of them, anddid not offer the possibility of direct filtration of the deleted messages, and instead presented the deleted messages and contacts in red. A convenient feature of both software products is that the messages are linked to contacts and the tools themselves group the discovered messages and contacts together. The first three categories (Contacts, Communication History and Messages) can be checked in the trial versions of both software products without the review limit, which is, as we mentioned before, a very convenient feature in the field of digital forensics. Both pieces of software showed very similar results when considering the category of photos, primarily when it comes to the visual display of the discovered photos, as well as their renaming. However, Jihosoft Phone Recovery found a larger number of photos, offering the searchfor photos locatedexclusively in the "Gallery" directory on the device before the scan. Both software products found the test file successfully, but with different names. The number of discovered video files was much larger with dr.fone Data Recovery – 24% more. However, by using Jihosoft Phone Recovery, the user has the option of reviewing a specific part of the video content before the recovery process begins, which is not supported by dr.fone Data Recovery. When it comes to audio content, the situation is more or less the same because dr.fone Data Recovery discovered more files to recover, but Jihosoft Phone Recovery here offers the user to play the files before the recovery process as well, saving a lot of time. However, neither Jihosoft Phone Recovery nor dr.fone Data Recovery found the targeted test file because the discovered files could not be played, so the user would need to listen to almost all of the recovered files because all of them were renamed with digits. The Jihosoft Phone Recovery tool discovered 78,622 text documents, however, without the additional search options, this number is almost worthless taking into account that some documents are represented a number of times in different parts, and is therefore not very relevant. WhatsApp communication offers the display of the conversation realized via the service of text message and multimedia content exchange WhatsApp. The Jihosoft Phone Recovery tool discovered three more conversations, but it also displays the messages and the multimedia content together, while dr.fone Data Recovery uses an additional category for the attached content (WhatsApp Attachment).

The interface of both tools is almost equal since the differences are only in the nuances. From the given results, dr.fone Data Recovery performed better in 4 categories (Contacts, Communication history, Video and Audio), but the video and audio content could not be played. Jihosoft Phone Recovery also performed better in 4 categories (Messages, Photos, Documents and WhatsApp conversation), however, it was almost impossible to get around the confusing multitude of documents. Both pieces of software could clearly discover only the photo test file, so it is not possible to confirm their capabilities with certainty.

**The quantity of the files found:**
Jihosoft Phone Recovery – 3
Dr.fone Data Recovery – 2

Both pieces of software have individual variations in quality of the discovered files. However, Jihosoft proved to be more efficient in terms of file types relevant to the experiment by discovering 3,806 photos in contrast to the 3,154 found by dr.fone. Moreover, Jihosoft discovered 78,622 document files compared with the 726 document files found by dr.fone. However, dr.fone proved more efficient when it came to audio file types with 244 against the 166 found by Jihosoft. Therefore, Jihosoft gained a score of 3 and dr.fone a score of 2. Except for the category of photos, dr.fone Data Recovery did not offer any display of other files, while Jihosoft Phone Recovery offered the possibility of checking the audio and video content before the recovery process.

**Time passed from the moment of the device's analysis start until the end of the scanning process:**
Jihosoft Phone Recovery – 3
Dr.fone Data Recovery – 2

The Jihosoft software performed the analysis and the scanning process of the mobile device in 10 minutes, while the dr.fone software finished it in 17 minutes. The difference of 7 minutes is too large, which gives a significant advantage to the Jihosoft Phone Recovery software, gaining the score of 3, while dr.fone gained a score of 2.

**The number of supported mobile device operating systems from which it is able to recover data via the stated tools:**
Jihosoft Phone Recovery – 2
Dr.fone Data Recovery – 3

Dr.fone Data Recovery is much more competitive when it comes to the number of supported mobile device operating systems. Therefore, it gains a score of 3.

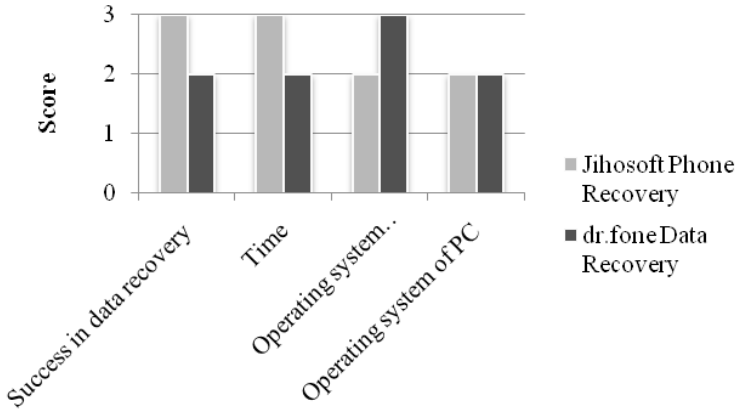
**The number of operating systems from which the software is run:**
Jihosoft Phone Recovery – 2
Dr.fone Data Recovery – 2

Both pieces of software can be run only on Windows OS and MAC OS. They both received scores of 2.

*Table 2. Table display of the evaluated software by categories*

| | Jihosoft Phone Recovery | dr.fone Data Recovery |
|---|---|---|
| Success in data recovery | 3 | 2 |
| Time | 3 | 2 |

| | | |
|---|---|---|
| Operating system compatibility | 2 | 3 |
| Operating system of PC | 2 | 2 |




*Graph 1. Graphical display of the evaluated software by categories*

It can be seen in the final graph that Jihosoft was more successful, gaining higher scores in two categories compared to dr.fone which gained a higher score in one category.

## REFERENCES

1. Top 5 Android Data Recovery Software, 2017, http://www.bestiphonedatarecovery.com/android-data-recovery
2. Dr. Fone Wondreshare, https://drfone.wondershare.com/android-data-recovery.html
3. Jihosoft, http://www.jihosoft.com/android/android-phone-recovery.html
4. Recuva, https://www.piriform.com/docs/recuva/introducing-recuva/what-it-can-and-cant-do
5. Bommisetty, S., Practical Mobile Forensics, PACKT, Brimingham (2014)
6. Joshi, R.C., Emmanuel S.P., Fundamentals of Network Forensics, Springer, London (2016)

# THE ROLE OF CYBER SPACE IN TRANSFORMING CONFLICT PARADIGM[1]

**Srđan Milašinović, Ph.D.**
Academy of Criminalistic and Police Studies, Belgrade
**Zoran Jevtović, Ph.D.**
Faculty of Philosophy, University of Niš

**Abstract:** In the society of risks in which we live, the ability to use the Internet, wireless technologies, and computers becomes one of the key parameters for the overall safety. The authors discuss conflictological changes that take place in the cyber environment, pointing out that communicational and technological tools with the new techniques of symbolic influence significantly transform the nature of the risks. Hence, the emergence of the market of personal safety is becoming more vulnerable, with the loss of privacy and the growing potential of neuro-technological techniques used to control the thinking and behavior of citizens.

Planetary growth of poverty, energy, demographics, climate, religion, migration and trading creates a new perception of global and national security that requires an adequate response by the relevant scientific community in terms of conflict paradigm reviewing. If terrorists affect the voters, by their activities, criminals, by phishing, document forging, money laundering, hacking "enter" into the global industrial complexes, and by purchasing the political influence into the highest institutions of the state, more dangerous gap within the social processes and between them is evident. Digital security rests on the management and control of information, as new risks with more threats from the growing terrorism and migration through crime and tectonic economic disorders change the existing forms of life, encouraging fear and uncertainty.

**Keywords:** cyber conflicts, information, security, public management, invisible war.

Violent socio-communicational changes that occur almost daily across the globe have significantly transformed conflictological-security paradigm, but it has still not enough been debated within the academic community. The Internet discovery enabled the information to limit geographic restrictions, but it also enabled barely seen patterns of networking between people by producing new routes and safety risks significantly differing from those in the past. From the conception of the German sociologist Ulrich Beck of the social and political potential of the new society, according to whom the world we live in is not at all riskier than before, but it is the nature of risk that is different, the authors discuss the concept of cyber conflict as a perspective of *soft conflicts* that will dominate future.[2] Globalization networked the world in matters of success and cooperation, but also in the risks and threats. Hence, the subject of interest offers a form of conflict fundamentally different from the traditional conflict in the physical environment, because it is based on anonymous and hidden opportunities to apply knowledge of information security with the invaluable and unrepaired damage to the affected side.

1 The paper was written under the Project No. 179045 funded by Academy of Criminalistic and Police Studies, Belgrade as well as Project No. 179008, implemented by the University of Belgrade – Faculty of Political Sciences, and the University of Niš – Faculty of Philosophy funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia.

2 Today *social produced risks* prevail, not as before - *natural risks and hazards*. This means less risk today comes from natural hazards, but more from the uncertainty produced by the social development and the development of science and technology. See in: *Rizično društvo*, Beograd: FilipVišnjić, 2001.

When the former official of the Central Intelligence Agency (CIA) and adviser to the National Security Agency USA (NSA) Edward Joseph Snowden publicly presented the data on *Prism* and other control programs (for example: *Xkeyscore*, *Upstream*, *Quantuminsert*, *Bullrun*, *Dishfire* ...) sharing the data with selected allies (for example, the United Kingdom Government communications Headquarters - GCHQ, the program *Tempora*), it became clear that the classical estimate of the volume, scope and nature of contemporary forms of surveillance and eavesdropping have dramatically changed. Thanks to the social networks, many platforms and modal forms of telecommunications networking of information the Interne has grown in specific, hybrid power that is most manifested in the media sphere, while it is more sophisticated and influential in the intelligence-security and political community in which commerce and information management became the conditions for preserving the security of security order. Safety concept is essentially transformed since any armed conflict is followed by a series of political, diplomatic, propaganda, economic, legal, special and clandestine activities limited in scope and time, with the intention of spreading its influence. In this paper the authors will discuss how the traditional concept of war between the states changes the concept of information conflicts which are latent and invisible to the lay public.

The word that symbolizes the information and communication changes is the term "cyber". It originated in the United States,[3] although etymologically it originates from old Greek language.[4] The term "cyber" became an integral part of the word "cyberspace", which denotes a specific area in the practice of computer science and application of information and communication technology in various areas including military operations, safety and effects similar to intelligence activities.[5] In contemporary military and security-intelligence application of the term is assigned to a series of semantically related forms, such as: "cyber warfare", "cyber conflict", "cyber-attack", "cyber weapon", etc. In the following text we will use the term *cyber conflict* assuming the operating set of digitized information-communication activities, procedures and activities that aim at changing the current security situation without using force.

The focus of the information and intelligence are the changes that occur in the cyber community, wherein the communications hubs are observed as a separate network of the security interests. In a global environment, the most of the international and national cyber-security institutions regard primarily the information security in cyberspace,[6], [7], [8] based on the construction of the defensive abilities of users or owners of information and information systems to defend against various types of cyber-attacks, whoever their perpetrator (a state or para-state organizations, groups or even individuals). In practice, we see how new technology is becoming a part of human reality, which means that cyber security cannot be seen as isolated from the overall security and conflictological paradigm. Preclusion and forecasting of cyber risk therefore becomes part of the current security strategy, and the hybridization of public services and specialized cyber units becomes an effective way of protecting vital national in-

3 The concept originated as a project of the Ministry of Defense - ARPA (later DARPA) and evolutionary developed in the whole world, together with the expansion of information and communication technologies.

4 Term "cyber" originates from old Greek κυβερνητικός, meaning: manage, govern or steer. Merriam-Webster Online Dictionary, s.v. „cyber," http://www.merriam-webster.com/dictionary/cybernetic.

5 Information Operations, Joint Publication 3-13. Washington, DC: U.S. Joint Chiefs of Staff, 2014, Taken on: 16.3.2017. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

6 International Organization for Standardization, ISO/IEC Glossary of IT Security Terminology, ISO/IEC, 2013, http://www.jtc1sc27.din.de/cmd?level=tplbereich&menuid=64540&languageid=en&cmsareaid=64540.

7 United States of America, Committee on National Security Systems, National Information Assurance Glossary, 2010, 22, http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf.

8 Совет Федерации, Федералыного Собрания Российской Федерации, Концепция стратеги и кибер безопасности Российской Федерации - Проект, (10 января 2014), 2, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (posećeno 18. marta 2017).

terests. Owning the right information or controlling other information and communication means the power to govern the political environment, but few individuals observe the reversal. Cyber security is increasingly in direct conjunction with its power to create, control and manage the information-flow, which means that the loss of control is often threatened by the loss of sovereignty of the territory. Is it possible to displace the social conflicts as "large and massive social action or conscious, focused, dynamic and practical mutual confrontation and struggle for collective social entities for significant and by their nature limited resources"[9] from reality into cyber sphere? Where are the boundaries of privacy on the Internet and how deep the intelligence community has access to their content? In the end, how many conflict situations arise in the cyber sphere and with what impact they mobilize and encourage individuals and groups to join, or assist in gaining public support? The attitude of the authors is that the conflict paradigm in the real world increasingly manifests itself as the realization of previously harmonized and coordinated activities in the offline community, which is further discussed in the paper.

## SPECIFICS OF CONFLICTS IN CYBERSPACE

The changes that the telecommunications revolution brought into the existing structure and distribution of power transformed current security paradigm. Traditional elements remained important, but no longer dominant in the world affairs as considered by Bajagić.[10] The term "soft forms of power"[11] meaning the ability to encourage the design, selection and spinning of certain information or to direct interests and opinions to the public in accordance with certain values and ideas of propaganda was introduced in the security sphere. With the Internet and new media "hard power" has lost its monopoly distributed by the state and its communication centers. In fact, the authors of this paper highlight several trends that have significantly influenced these changes: globalization has encouraged economic interdependence, unevenness in the process of technology dissemination, the growth of nationalism in weak states, the growth of terrorism and the reconstruction of the *Cold War*. The *informational power* came to the fore, because those who create, control and have access to information have the advantage in international politics and security practices compared to those possessing the greatest source of power that cannot threaten by the use of armed forces. "Power is, therefore, not only spilled from the state to the non-government/private actors, but also from the *rich in money* to the *rich in information*".[12]

Looking at the changes in the transformation of the conflict paradigm, we see more frequent application of cyber conflict based on the use of information technology and information. So we get a new, flexible and multidisciplinary concept in relation to all previous theories because it uses different methods, techniques and tools of conflict that can be applied in everyday environment, no matter whether it is a state of peace or war. The essential advantage is in invisible actors, as participants are not exposed in public places, do not wear uniforms and are not officially in conflict. States usually do not acknowledge the existence of these units, nor their activities to the other side. This implies the unpredictability of the outcome, because the area of cyber warfare has no rules, boundaries or objectives as a cause of the attack at which

9 Milašinović R., Milašinović S., Putnik R.: *Konfliktologija*, 2010: 18.
10 More in: Bajagić, M., *Osnovi bezbednosti*, Kriminalističko-policijska akademija, Beograd, 2007.
11 As specific dimensions (mild forms) of power terms technology, information, trade and finance are cited (Bžežinski, Z., *Velika šahovska tabla*, CID, Podgorica 1999. p.7 Nye talks about the new, soft, intangible and less coercive forms of power compared to traditional, rigid forms of power; Nye J., Jr. Think Again: *Soft Power*, Foreign Policy, 2006, February 23, str. 153-170.
12 More in: Milašinović, S. i Jevtović, Z. (2013): *Metodologija istraživanja konflikata i komuniciranje u savremenom društvu*, Kriminalističko-policijska akademija, Beograd.

point the conflict ends. Although implemented in cyber (*online*) space, the consequences are manifested in the *offline* reality (the physical environment, the civilian population, technical systems, as well as in the sphere of psychological media environment), so we can conclude that it produces significant effects on society. In order to manage a crisis or social conflict, it is important to have control and management of meanings, because sociability is expressed through the mediating powers to participate in the creation of the security environment. Exclusion from communication is, therefore, precisely the exclusion of the conflict process. Crisis management theorists distinguish several stages and that the first set of problems is related to the collection, selection, processing and circulation of information "where the usual course of the crisis significantly changes".[13] Cyber conflict has not been precisely legally framed, which means that traditional international law of armed conflict is not applicable in an adequate way because it is not adapted to a specificity of cyber conflict.[14]

Due to limited space, we are unable to analyze all cyber-attacks of high importance, but we can see that the actors commonly use *zero-day vulnerabilities*.[15]For example, on September 22, 2016, the company *Yahoo* confirmed that hackers stole personal data of at least 500 million users of the service. The secret was hidden from the public, but when the hacker group called "Peace" listed the information to sell data on 200 million users of *Yahoo*, it was clear that something was wrong. How transparent is the sphere of security was also shown by the data of the German Bundestag where the first attack on the network was registered on May 8, 2015, having at that moment not special attention. The alarm sounded just four days later when the Federal Security Service of the constitutional order (intelligence authorities responsible for defense against cyber espionage) informed the MPs of the hacking event. All attempts by experts of the Federal Office for Information Technology Security (BSI) to eliminate the intruders in the system failed, because the main hub connection of IT-systems was infected. Market vulnerabilities and zero-day exploits are increasingly expanding and evolving and key customers of such data are States or their intelligence agencies.

Cyber-attacks are a manifestation of the proactive intrusion to the information of the other using the knowledge and skills in the field of information security. The attacker always has the advantage for bringing the decision on selection, vulnerability and effects mode and has a time advantage often allowing him to be imperceptible in the beginning. Hence, the security assessment of an analyst is an important stage of potential conflicts because different attackers can perform on the same target with different raids in completely different ways. A cyber conflict is characterized by anonymity of opponents and short duration because of misinformation, spin and misinformation placed to produce a moral panic in the targeted society even before the conflict began. In fact, the paradox is that the technology represents a limiting factor that prevents unambiguous and reliable detection of cyber hub, identification and attribution of attackers and establishes state responsibility for the attacks.

There are significant differences between the information and cyber security, but in this paper we do not have space for more clarification. Those familiar with this field point out that those concepts should not be seen as mutually interchangeable, but fundamentally different,

13 "Actors of crisis management must properly assess the needs of the public for information. The emergence of the crisis in the public creates an information gap that must be filled quickly and precise information…" (Kešetović, Ž. i Toth, I.; 2012, p. 113)

14 "International public law regulates relations between the international legal entities in the state of armed conflict, and is called the International Humanitarian Law or the law of war."(Policastri and Sergio D.2013)

15 *Zero-day Vulnerability* is based on a security flaw or defect in the software information system, which is unknown to the manufacturer, user or department that deals with the protection of information. Weakness is known to attackers, the information about it is kept secret which allows them to control effectively zero-day cyber-attack. Zero-day exploit is a term used for the software system that prepares the attacker to exploit zero-day vulnerability to unauthorized intrusion into a system or cyber-attack.

because they refer to different facilities and areas. "While cyber security is related to all elements of cyberspace (involving systems, information and people), information security refers to the security of information, regardless of the nature and environment of information (digital, analog, or not)".[16] For instance, people are actors, attackers and targets in the cyber-security, while in the information security the data security depends on them.

## SOCIAL NETWORKS AS POLYGONS OF CONFLICT

There are many definitions of social networks, but in conflictology it is common to imply Web services that allow individuals to build their profile in limited systems and information to connect with other users, whose number is not limited. The very concept is more detailed in the terms "hub" and "connection", wherein the first considers each individual participant or member of the network, while the other is determined by the mutual relation of two or more members. Along the connection it is possible to create different relationships based on similarities in interests, desires, emotions, ideas, attitudes, and so on. Characteristics of social networks make the detachment for a particular space, the anonymity of the participants, their internationality, speed, the ability to achieve low-cost large effects and the like. Quick exchange of information with the power of interactive intimacy with others offered an advantage that the old media are no longer able to reach.[17]Social and mobile media platforms have become dominant in the lives of young people, because they offer something that old media never did and will not: the opportunity to each participant to connect and share their lives with close friends and acquaintances, but also the entire planet through photos, blogs, messages or video presentations. Combining specific digital tools allows social networking to specialize in certain types of interaction - *Twitter*, *Facebook*, *YouTube*[18] – as the most popular. Specific tools within the network enable terrorists or criminals to address their own micro-communities, without fear that they will easily be discovered! In terms of security, the possibility of the spread of extremism and violence through the activities of frustrated individuals or independent terrorist groups that carried their own dissatisfaction act on the field has increased.[19]

The easiest way to trade data and information is available on the so-called "black market" because it is "open" to everyone, from individuals of the criminal groups, through representatives of security companies and organizations close to the state apparatus (police, judicial and intelligence and security agencies).[20]These sites are of a virtual character, because they operate within the online forum whose number with the spread of "Dark Web" has signifi-

16 Rossouw von Solms and Johan van Niekerk.: "From Information Security to Cyber Security". *Computers and Security* 38, (October 2013): 97-102

17 "Interactivity can be defined as the degree of involvement of users in modifying the content and form of the media environment in real time" (Petković 2007: 109).

18 The combination is an easy way to explain the case by YouTube, which is open as a service for sharing videos with an infinite number of users. Today it includes uploading videos, search videos and user registration, a number of mechanisms for storing and sorting our own histories, creating and sharing lists of clips, finding friends, commenting on videos, answering to comments, voting for the most interesting comment, voting for the video, measuring the number of views video, video sharing with other networks off YouTube...

19 An example of "lone wolves" are brothers Dzhokhar and Tamerlan Tsarnaev, the Boston Marathon bombers on April 15, 2013. Three people were killed in the explosion including an eight-year boy, while more than 260 people were injured.

20 Group UMBRAGE, belonging to the CIA department for remote devices, collects and maintains huge file offensive techniques that are "stolen" from malware produced in other countries. Thus, the US can redirect the service identification of the perpetrator by leaving behind a "fingerprint" of the groups from which the attack technique is stolen.

cantly increased. It gives various offers of illegal trade matters, from narcotics, weapons and criminal services, to information about vulnerabilities or even service cyber-attacks, such as for example: *The Real Deal Market*, *Silk Road* and others. Digital markets are unlimited, hence they are dynamic due to the rapidly changing nature of crime sites, which is understandable because the same information that is the subject of trade has long life as it can be used only until being unknown. In practice, it is quite common that representatives of the intelligence and security agencies are involved in covert trade and monitoring activities on these forums.[21]

With the digitization, the sphere of security, particularly crime and terrorism, has undergone deep and significant changes since all common digital series of strikes have resulted in conflictological activities that disrupt the stability of other social subsystems. Hence, the semantic interpretation of reality turns into a specific power that breaks the security mechanisms of the state border or preventive barriers, directing the entire community to redefined patterns of behavior and safety culture. *YouTube*, *Facebook*, *MySpace*, *Twitter* and the like social networks, with the convergence of IT tools imperceptibly change the traditional communicational techniques whereby increasingly becoming the important sources of information, especially in crisis situations. Life in virtual communities is increasingly being reflected in developments in the real environment which in the field of security is reflected in the radicalization of information management and increasing tendency of terrorism, crime, violence and related forms of deviant behavior. Using new technologies, hostile attack or criminal activity can be realized from a long distance and hidden locations, with actors who have never met or known each other, which in practice results in new forms of conflict.

The amount of data in transnational environment in a short time has increased enormously, so that its processing requires specific tools, algorithms and programs that are constantly upgrading and improving. Digital sphere is not alienated from reality, because it exists where the information can create, store, disclose, send, receive, process and destroy the application of computer information systems within the electromagnetic fields. Their comprehensiveness, interactivity and invisibility in new forms of monitoring provide unimaginable scope because the chain of control increases with each contact "persons of special interests", constantly expanding the network structure. For example, if the operative person of interest has only 10 friends on *Facebook*, the analyst responsible for tracking personal contacts at the NSA or in some private agencies working for this service may without a writ follow the communication of friends of friends' friends, up to three "jumps" - as some 266.955 people.[22]With only 300 likes that someone left on the social network, an expert in the data science can create a psychological profile of all relevant data to be used for trade in the world's largest companies! *Instagram* uses a camera to take pictures and shots, *Gmail* has the access to our directory, *Viber* knows our exact location at any time, while *Facebook* can read all of our SMS messages. When WikiLeaks officially announced that the US intelligence services have developed effective methods for hacking devices such as *iPhone* and *Android phones* as well as *Samsung* "smart" TVs, allowing them to monitor communications even when the devices are turned off, the public was puzzled if that was true. Available documents also reveal malware, viruses and security holes called "zero days", along with hundreds of millions of lines of computer code used by the CIA, and the ability of its staff to hack devices and messages before they are encrypted by applications like *WhatsApp*, *Signal*, *Telegram*, *Confide* and others, for which the public feels that they are safe. This means that the Internet canceled the privacy of users, but also that the way of collecting, processing and diffusion of data is radically altered. Digitization has brought large amounts of trans-national data in the sphere of national security which

21 Andy Greenberg, „New Dark-web Market is Selling Zero-day Exploits to Hackers," Wired, April 17, 2015, http://www.wired.com/2015/04/therealdeal-zero-day-exploits/ (Accessed March 22, 2017).
22 "Three degrees of separation: breaking down the NSA's 'hops' surveillance method", *Guardian*, 28.october 2013.

has caused the national sovereignty to disappear, but at the same time blurring once solid line between law enforcement and intelligence and security service.

## CONCLUDING REMARKS

Cyberspace is increasingly transforming the concept of modern conflictological paradigm, whereby the leading strategists of large states recognize that they are being actively involved in the new field of confrontation. The Russian Defense Minister Sergei Shoigu, referring, to the deputies of the Duma by the end of February this year announced the creation of "information-information unit", responsible for "counter-propaganda", with Russian media reporting that he used the term "cyber army". The first man of defense said that such forces are established "to defend Russia against cyber and propaganda attacks from the West" exclusively for defensive purposes, but some of the generals disagreed with that assessment considering that Russia must have the initiative even during the peace periods. President of the *Academy of Geostrategic Issues* Colonel-General Leonid Ivashov has proposed to establish a national center that will not deal only with the western counter-propaganda, but will plan information and psychological offensive operations because the image in the minds of people is more important than the armed conflict.

A completely new era is emerging in which the possession of real information including those in the private sphere mean the power to govern the political and security environment, but some people are of the opposite opinion. For example, during the decade of searching for terrorists suspected of killing a dozen Turkish citizens for religious reasons, the German intelligence officials intercepted more than 20 million mobile phone calls, collected the data on payment transactions of 13 million credit cards, controlled more than one million data of rent-a-car users' services, registered about three hundred thousand potential suspects, which means that they tracked at the same time about 30 million people! By following digital contacts, based on the analyzed "scheme of conduct" it can reliably be predicted when some person will become "potentially dangerous", as well as the moment when that person will become a "security risk"! Security of entire community is increasingly in direct conjunction with its power to create, control and manage information flows, which means that the crisis situation occurring at the scenario can be predicted in detail.[23]

Social networks are largely influenced by the mass, but also interpersonal forms of communication emphasizing the picture and its power in the subconscious, which also reveals the increasing number of false news. Nicola Mendelsohn, the vice president of *Facebook* for Europe, Middle East and Africa, a market that holds over 430 million users, indicated the trend in the way in which users increasingly communicate, noting the explosive growth of video materials (especially after the launch *live video* option) at the expense of text messages.[24] The number of video views during 2016 increased eight times compared to the previous year (from one to over eight billion) with almost twice reduced number of text messages and print status. In fact, this is not the result of *Facebook* forcing video material but the fact that users recognize the image as a way of better, more dynamic and concise way of conveying information. In the sphere of conflictology, this means that the visual information will gain importance, whereby the privacy and ethics will increasingly be less protected.

23 US NSA is already working on a program of the so-called "dark" or "deep" Internet, which hides encrypted communications and closed networks of other countries. In the desert of Utah a new super-secret center for cyber spying and cyber-security is being built, which will cost over ten billion dollars!
24 At the press conference held on January 19, 2017 she stated that Facebook users watched per day up to 100 million hours of video of various materials, which served her as the basis for the hypothesis that **in about five years, most of our communication could be in the form of video**!

In the future, we anticipate further expansion of information technologies; it will become more complex but also more vulnerable, which means that the number of conflicts in cyberspace will grow. The comprehensive repertoire of techniques is becoming more comprehensive, from the packing of large amounts of data with some having manipulative character through the development of quantum computing, robotics and artificial intelligence to the new forms of cyber-attacks. The best method of prevention of the effective opposition is the development of safety culture and hence, the cyber conflict can be viewed through the implementation of information security in order to manage information.

## LITERATURE

1. Бајагић, М. (2007): *Основи безбедности*, Криминалистичко-полицијска академија, Београд.
2. Bek, U. (2001): *Rizično društvo*, FilipVišnjić, Beograd:.
3. Bžežinski, Z. (1999): *Velika šahovska tabla*, CID, Podgorica.
4. Kešetović, Ž. i Toth, I. (2012): *Problemi kriznog menadžmenta*, Veleučilište Velika Gorica, Visoka škola za sigurnost s pravom javnosti, Centar za međunarodne i sigurnosne studije i Fakultet političkih znanosti u Zagrebu, Velika Gorica.
5. Милашиновић, С. и Јевтовић, З. (2013): *Методологија истраживања конфликата и комуницирање у савременом друштву*, Криминалистичко-полицијска академија, Београд
6. Petković, D. (2007): Uticaj internet na tradicionalne medije. *Internet i javna sfera u Srbiji* (Sitarski, Milan), Beogradska otvorena škola, Beograd.
7. Policastri, J. and Sergio D. Stone, *International Humanitarian Law*, American Society of International Law (ASIL), https://www.asil.org/sites/default/files/ERG_International%20Humanitarian%20Law%20(test).pdf (2013).
8. Rossouw von Solms and Johan van Niekerk. "From Information Security to Cyber Security". *Computers and Security* 38, (October 2013)
9. Nye J., Jr. Think Again: *Soft Power* , Foreign Policy, 2006, February

# SOCIAL NETWORKS AS A SAFETY FACTOR OF THE MIGRANT CRISIS[1]

**Zoran Aracki**[2]
University of Niš, Faculty of Philosophy, Niš
**Ladin Gostimirović**
Visokaposlovnotehničkaškola, Doboj, RepublikaSrpska, BiH

**Abstract:** The tidal waves of the world migrant crisis are still crashing onto European shores. Millions of people start from Asian and African continents towards the European states that they perceive as salvation for themselves and their families. Their movement along the pathway is to a considerable extent alleviated by new information technologies, most of all, mobile phones. Thanks to them and especially to the users' networking, it is possible to provide for an exceptionally fast delivery of information about the state and the challenges awaiting these desperate people on the way ahead.

The contemporary migrant flows are constrained by the space-time dimension since it is in this way that the process of movement is managed in a communication-skilled way. The emphasis is on permanent communication among actors (by mobile phones and GPS tracking), financial logistics (by foreign currency transfers through certain banks that keep track of them during the journey) as well as support from the previous migrants who, by pointing to weak points of the corridor that the migrants are passing through, enable successful networks functioning.

The social networks that basically represent modified channels for distribution of contents are at the same time means of forming and publishing information organized through nodes and links. The danger from their abuse is quite real. In the paper the author points to safety challenges brought about by the use of new communication technologies as well as the need for their monitoring.

**Key Words:** Safety, Social Networks, Migrants, Mobile Phones, Communication

## INTRODUCTION

Population migrations are not a new phenomenon; they take place, with different intensities, almost ceaselessly, always when at some territories, for one reason or another, the life of the local population is jeopardized to a considerable extent. It is estimated that close to 34 million of people who could rightfully be called migrants are living in Europe.[3] Regarding the overall population number which is within the range of 50 millions, this amounts to some 7 percent. This fact cannot be ignored by any means since it substantially influences political, cultural, social and safety situations on the given territories.

1 The paper is done within Project No 179074 realized by the Center for Sociological Research of the Faculty of Philosophy, Niš, and financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia.
2 E mail: zoran.aracki@filfak.ni.ac.rs.
3 Of this number, 14,3 million people are citizens of the EU who used the opportunity of free movement within the Union while somewhat less than 20 millions came to the EU from the non-member countries, as reported by the AFP (Tanjug, 2017).

A common trait of most migrant movements, until recently, was of economic nature and conditioned by unequal development, that is, poverty of different parts of the world. Stephen Castles' opinion is that in the 60s of the last century, the then dominant migration model that was evident in the permanent settlement of particular territories, that is, countries, was expanded by new trends such as 1) temporary labor migrants that can result in the permanent settlement in the destination country, 2) hidden forms of migration, that is, illegal migrations, toward traditional immigration destinations as well as West European countries, 3) labor migrations from underdeveloped countries toward the destinations in which industrialization is in the process of development and 4) the movement of workers to new industrial areas in Third World countries (Castles, 1986, 1993).

However, in the last few years there has been a considerable change in the nature of migratory movements. The economic reasons are replaced by fear for one's own life. A decisive influence in all this was a series of failures of various "springs" in the north of Africa and in the Near East with the USA directly involved in them as well as many West European countries in addition to quickened pace of the information technologies development and increased transport capabilities. A great river of people from Africa and Asia started flowing from the mid-second decade of this century toward Europe. Hundreds of thousands of people ran away, and are still running, from the countries in which the great powers tried to impose the model of the so-called democratic system in which the given population should live "happily and with dignity." It has turned out, though, that the imposition of the global patterns of state systems was a wrong move for which all the parties involved are paying a high price now.

The migrant movements have always represented a great challenge for researchers of many sciences, especially economic, psychological and sociological and, more recently, communicological as well. The contemporary migrations, besides the old ones, comprise some quite new dimensions which, unfortunately, represent threats to the safety of people, states and international community. Among these new traits a special attention should be devoted to coupling of migrants with organized crime and international terrorism which is realized through the Internet and social networks.

This is the reason why this paper deals with the use, that is, abuse of the social networks among the migrants. We would like to point out that the Internet and social networks help migrants as much as people's smugglers, migrants and terrorists. The pathway of hope for many of the people who have left their homes very often turns into a death road. No precise data exist about the number of victims but it is quite certain that it is enormous since news about tragedies, especially about the sinking of ships and boats transporting these people are never off the pages of world press.[4] Not a small number of them, on the very same path, become victims of the traders with people. At the same time, there is increasing evidence that the rising terrorism in the Western countries is contributed by migrants themselves, regardless of whether they have just come to the European continent or they represent second or third generation of migrants. By using the Internet and the social networks these people become victims of criminals, all sorts of manipulators, adventurists and methodically trained religious fanatics. Hence we advocate for much needed wakefulness of safety agencies as well as for control of this kind of communication among migrants.

4 Total of 559 migrants died in the year of 2917 on the Mediterranean as reported by the International Organization for Migration. Last year the total of 5000 deaths of migrants was recorded, as reported by Reuters (Tanjug, 2017).

## GLOBAL MIGRATION AGENDA

The theorists mainly agree about the allegation that there are three major factors ushering in migrations. One of them is a demographic explosion in some parts of the world; another refers to wars while another is social engineering. All these factors must be observed on the whole since none of them are, on theirown, sufficient enough to launch such a big wave as the one Europe has been facing since 2015.

The contemporary migration story started with the USA and NATO military interventions in the Near East and in the north of Africa, that is, on the territories that can be considered as very active in the demographic sense. They caused deaths, poverty and religiously motivated massacres that were only sporadically spoken about in the Western public. Europe refused, for quite a long time, to recognize the real causes of the launched migrant wave. Only a small number of media – even less known ones – dared to say that the direct migration mover was, actually, a struggle for bare life. Less known German paper *DeutschenWirtschaftsNachrichten* from Berlin was among the first media to advocate such an opinion. As early as 2015 the paper wrote that those who would like to stop migrations would have to hinder thoughtless and careless long-lasting military operations. They would also have to change military alliances such as the NATO and turn them into purely defensive ones (*DeutschenWirtschaftsNachrichten*, 2015). The others, far better known and greater media reported on the statements of the West leaders implying that the main reason for one's home leaving was fear of dictator (such as Bashar al-Assad) that had to be dealt with and that had to be removed from power at any cost.

An even slightly more detailed analysis of the things really happening on the site soon showed that it is, in fact, the matter of another well-constructed and media-supported stories that, under the cover of the struggle for democracy, led to the imposition of the will of the powerful political, financial and military structures whose real goal was to spread the ideology of globalism.

A few years after the great migration crisis had begun, and on the basis of many political and scientific conferences held all over Europe as well as of learning from numerous reports of the world media, it can rightfully be claimed that most citizens of Europe feel that there is, behind the wave of refugees, a conspiracy of the world powers for the sake of achieving higher goals as well as a kind of social engineering.

The German researcher and publicist Friederike Beck, otherwise the chair of an association for international peace policy, in her book *The Secret Migration Agenda. How elite networks want to destroy Europe using super rich foundations, the EU, the UN and NGOs* explains how the migration crisis was initiated and organized by global political and financial shadow cabinets. In her opinion, these are complex network structures at a very high level. There is synergy of super-rich foundations and associations and non-government organizations with decision-makers in the European Commission and at the key positions in the European Parliament. All of them receive huge aid from the UN and organizations close to them such as International Organization for Migration (IOM) or individuals such as Peter Sutherland who has been, since 2006, the United Nations Special Representative of the Secretary-General (SRSG) for International Migration while, at the same time, founder of the Global Forum on Migration and Development (GFMD). Besides remarking how difficult it is to say who the people at the top of the global process dictating the population migrations are, Beck states that the key figure is Peter Sutherland himself. She also states that hardly is there any single important international organization or institution where Sutherland was neither chair or on the management board so that he is rightfully considered as a "father of globalization".[5]

5 Former Attorney General of Ireland who is unofficially credited with being the father of globalization.

In addition to her estimate that the until recently Secretary-General of the United Nations Ban Ki-moon could be regarded as a puppet of his counselor Peter Sutherland, Beck also reminds us of the statement of the leader organization which gathers together 193 world states under one roof given to the *Berliner-Zeitung*that it is a cliché saying that we are living in a global world. Little is known, Ki-moon added, that globalization takes place in phases and that we are now in the second one, in an age of mobility, while the first phase, when the capital flow and commodity was liberalized revealed all the advantages of globalization, especially to the developed industrial countries and their trade partners including Brazil, China and India. He also added that since we are entering a young age of mobility, people will start crossing borders in an ever increasing number. According to the remarks made by Friederike Beck, the aim of all that has been happening is in essence to meet the interests of the financial powers which are revealed in their tendency to bring cheap work force to the European territory.

In the European migrant reality, an unavoidable actor is, surely, a hyperactive globalist George Soros who is among the very richest people in the world. His wealth is estimated at about 24.2 billion dollars. Soros's involvement in the colored revolutions all over Europe as well as in Africa and Asia is many times confirmed so that we do not have to prove it at all. Hungarian Prime Minister Viktor Orbán (whose Americanized compatriot is Soros) has unambiguously confirmed that Soros is, together with his so-called non-government organizations that he financially supports, one of the organizers of the great migration wave that, under the alleged humanitarian goal, virtually represented an attempt to destabilize Europe. That is why Soros is proclaimed a persona non-grata in his own homeland (Mitrović, 2017).

Friederike Beck also states that Soros' foundation or the "Open Society Foundations", together with other rich foundations, established, as early as 2005, The European Programme for Integration and Migration (EPIM)[6], an initiative of currently 14 Partner Foundations and 11 associated Foundations, and thus it got engaged, in the most direct way, into the whole operation led from the globalist center. The aim of this and similar organizations is actually to exert influence upon politics, state weakening, promotion of Europe of non-obstructed migrations, without visa and borders.

## ACTORS OF THE BALKAN ROUTE

Since the first days of initiation of the great migrant wave no agreement has existed either in foreign or domestic public concerning the way of calling these people with small children in their arms, with bundles of clothes and some European or American money in their pockets, who come to the European territory, that is, whether they are migrants, asylees, irregular migrants, refugees, immigrants, illegal migrants, emigrants or illegal migrants. In the practice of domestic media – as shown in our last-year research project[7] - the most often used is an "impersonal term – migrants."[8] Almost twice less is used the word "refugees".

In his long career he performed many duties. He was European Commissioner responsible for Competition Policy; for many years he was (Founding) Director General of the World Trade Organization (formerly General Agreement on Tariffs and Trade). Leading Eurocrat; also was the chairman of oil giant British Petroleum. He served on the steering committee of the Bilderberg Group; also Consultor of the Extraordinary Section of the Administration of the Patrimony of the Apostolic See (a financial adviser to the Vatican), the United Nations Special Representative of the Secretary-General for International Migration, etc.

6 More about it in Beck, F. (2016).*Die geheimeMigrationsagenda*, Rottenburg: Kopp Verlag.

7 More about it in Aracki, Z. (2016). „Medijski diskurs izbeglištva" („Media Discourse of Refugeeism"), *Kulturapolisa*, Vol.XIII,No 31. Novi Sad/Belgrade: Kultura – Polis/InstitutzaEvropskestudije, p. 45-55.

8 Riha, A. (2015), "Zašto mediji izbeglice pretvaraju u migrante" („Why Do Media Turn Refugees into Migrants"), www.cenzolovka.rs, assessed October, 20, 2016.

The terminological disagreements about the basic concepts used for denoting people on the so-called Balkan route may appear less important only at first sight. And yet they directly induce safety confusion which is, in the critical situations, threatening to the stability of the overall system. Most of the influential media mostly use the term "migrants" to refer to hundreds of thousands of people who come to Europe running away from conflicts in their homelands. This makes ordinary people confused since they do not know how to interpret such a variety in defining these groups of people who leave their homes in such a massive number. Terminology is of great importance when it comes to different rights to be provided by one term or another. In view of all this, it becomes clear that different uses of the terms in media actually dictate the kind of the response the society at large has towards people on the Balkan routes. It is beyond any doubt that the concept of migrant is impersonal and indefinite so that it is well maneuvered to hide the fact that we are dealing with a huge inflow of refugees.

Regarding the international law, a great many of these people should be denoted as refugees since – as also confirmed by the UNHCR, even 95% of them come from the war torn countries.[9] 1951 Convention Relating to the Status of Refuges and additional 1967 Protocol relating to the Status of Stateless Persons clearly define criteria and reasons for allotting particular status. According to these documents, a refugee is "someone who is unable or unwilling to return to their country of origin owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group, or political opinion."[10] The migrants, on the other hand, leave their homes most often for economic reasons and have, after all, some sort of options to choose from.

The use of different concepts for the people on the Balkan Route is explained in a variety of ways but, in doing so, one should not ignore the fact that such inconsistency, that is, parallelism in critical situations in which the today's world finds itself, can hardly be only a product of professional ignorance (journalists) or social ignorance of the situation (public). It is, above all, the matter of dissolving a safety problem which lies underneath all such forms of conduct.

In the propaganda varieties what tends to get lost is social disorganization as well as disintegration of the whole countries and nations which can contribute to the escalation of crises to other territories as well. The leading theorists of the social disorganization, A. Elliott and F. Merrill[11], consider this as a phenomenon visible in disturbances in social communications. They also point to the degrees of its manifestation, confirming that formalism in public communication represents the first degree of disorganization that is, further on, built upon by conflicts leading to the total loss of social consensus. The problem is in the fact that in the critical situations an obscure conceptual category can easily be politicized so that part of more extreme oriented media can use the concept of "economic migrants" with an emphasis upon the waves of people as job seekers or for economic benefits thus leading to increasing xenophobia and risk from new confrontations. An example of this is sensationalist reporting on the part of media about an Islamic state being formed in Serbia with Belgrade turning into Tehran. Likewise, there are as well many reportages about the fates of the refugees who gather together by the Railway Station in Belgrade as well as a great number of articles and television features in which journalists calculate how much money is spent by refugees or how much they cost or whether they are disease-carriers.

The analysts of the migration movements are especially keen to notice that "among those who come to Europe there is more than 72 percent of male population in an age group be-

9 UNHCR Regional Spokesperson for Central Europe BarbarBaloh said, for the Radio Free Europe, that in Hungary, only this year (2015), 90.000 people applied for asylum with 60.000 of them coming from Syria, Iraq, Afghanistan and even Pakistan.

10 Convention and Protocol Relating to the Status of Refugees, http://www.unhcr.org/protect/PROTECTION/3b66c2aa10.pdf, accessed March, 2017.

11Elliott, A.&Merrill, F. (1961): *Social Disorganization*. New York : Harper and Brothers, Publishers.

tween 20 and 35 years. Almost all of them are Muslims while many of them are radical Islamists, members of ISIS" (Starčević, 2016). Many of them are well-trained in special camps; according to the military doctrine, their training is of a modular type that irresistibly recalls the one that Albanians applied in the late nineties of the 20th century at Kosovo and Metohija. This module looks like this; first come women with children in their arms or men carrying children on their shoulders or in their arms thus sending the message to the humanitarians that children should be taken care of. Behind them there follow twenty to forty years old people which is exactly the population that would expansively change a demographic picture of Europe.

What can also be noted while tracking the migrant flow is the fact that almost all of those moving in it have modern cell phones that enable them to keep a permanent contact with those governing their movement.

## TRADE WITH PEOPLE AND INTERNATIONAL TERRORISM

Contemporary migrations are marked with the use of modern technologies as well as an increased degree of communication among the actors. It is exactly the abuse of these technology-created opportunities, in a very serious way, which jeopardizes the safety of people, states and even the international community on the whole. It is the matter of the connections set up between migrations and organized crime, trade with people and international terrorism.

What is common to actual migrations could be regarded as organization of *social networks*, [12] which, along the migration route, creates an elastic and firm chain of interpersonal and group communication links not only among the migrants but also with the logistics centers in the countries of final destination and this through the relations of kinship, friendship or affiliation to particular religious or ethnic community. The networks considerably aid the quickened movement of people on the migrant tours as well as to simpler crossings of the European border lines.

The inter-state borders cannot be hermetically closed; about possible actions of armies and police the migrants are informed on time thus reducing the risk of the whole operation. They exchange information about routes, destinations and the ways they are received by local populations; also, at the very spot they improvise trails that are adjusted to the changed conditions. This is not any longer a network of kinship and friendship but it is rather intelligence, professional and expert organization of mass movements of population that, through a set of concrete instructions, obtain already established procedures that can help with the decision-making about migrating as well as in different phases of activities in the crisis.

The contemporary migrant flows are constrained by the space-time dimension since it is in this way that the process of movement is managed in a communication-skilled way. The emphasis is on permanent communication among actors (by mobile phones and GPS tracking), financial logistics (by foreign currency transfers through certain banks that keep track on them during the journey) as well as support from previous migrants who, by pointing to weak points of the corridor that the migrants are passing through, enable successful networks functioning.

No precise research of the use of social networks and the modern technologies on the migrant routes exists but it is quite certain that they are intensively used, especially Facebook

12 The social networks that basically represent modified channels for distribution of contents are at the same time means of forming and publishing information organized through nodes and links... they are essential for providing social and emotional support but also a source of information enabling establishment and preservation of contacts with other people (Milašinović&Jevtović 2013:135-136).

and Twitter as well as many other networks. They are equally used by those who set out on a journey to Europe as well as smugglers of people. Potential refugees use the social networks to find smugglers who organize, prepare and later on direct them to their desired destinations. In addition to the social networks, the migrants also use applications for texting such as WhatsApp and Viber.

Unscrupulous criminal networks almost daily organize journeys of a great many migrants who are desperate to get to the EU. Their organizers thus achieve great material gains though very often they endanger the lives of the migrants. In order to maximize their gain, the smugglers embark hundreds of migrants on unsuitable vessels – including small inflatable boats or waste disposal boats – or closed trucks. Multitudes of migrants get drowned in the sea in that way, or choke to death in containers or end their lives in the deserts. Regarding the data of the International Organization for Migration (IOM)[13] it is estimated that in 2014 more than 3000 migrants lost their lives in the Mediterranean. According to the yet-unconfirmed data, almost the same number is recorded in the first half of 2015 which shows that the number of victims is dramatically increasing. This also points to the fact that the illegal migration by sea routes, especially those of the Central and East Mediterranean, has been rising exponentially. Rising at the same time, in this way, are the dangers that the migrants are exposed to while crossing the Mediterranean Sea.

For smugglers, migrants are common goods to trade with like drugs or fire arms. They quickly change their travel routes so as to adapt to the given safety situation in the transition countries or to respond to the law enforcement services. They often abuse the procedures for legal entrance and stay. The smuggling of migrants is an exceptionally profitable job with the criminal networks profiteering from a low risk for detection and punishment. The proof of excellent gain has been presented on a recent press conference of the Bosnia and Herzegovina police at which the results of the action it undertook with the police from Turkey and some other countries are given. The action lasted from September, 2016 to March, 2017, and it confirmed that "smugglers for illegal transport of people kept on taking from migrants between three and five thousand euro" (Knežević, 2017).

Along with all the more popular "crime business" – smuggling of people over the borders of the European states – there is a trade with people and organs, sexual and working exploitation, compulsion to perform criminal activities and the like; this, taken as whole, represents a source of fast and easy gain. After illegal drug and arms trafficking this is the most profitable crime business of the organized crime which, as early as at the beginning of this century, brought a profit of several billion dollars only in Europe, with a minimal risk for people smugglers and traders to be revealed (Ghrib 2002:31).

There are, likewise, serious indications that the social networks have also been used in the preparation of mass attacks at female passers-by at the main railway station in Köln on New Year's Eve in 2016. German Federal Minister of Justice Heiko Maas, in an interview for the Sunday edition of the daily *Bild, Bild am Sonntag*, confirmed the reports given in the papers testifying that in the police reports it is written that the migrants from North African countries from the surroundings of Köln as well as from nearby Holland and Belgium called each other, through the social network, to come to the main railway station in Köln (HINA, 2016). The German police submitted, because of the attacks, even as many as 379 criminal charges against the persons who were mostly asylum-seekers or illegal immigrants from North Africa. About 40% of the charges referred to sexual assaults including two cases of rape.

Likewise indisputable are the links between the migrants and the international especially mass terrorism. The Internet and the social networks also play one of the key roles in the con-

13 International Organization for Migration, (2014) *Fatal Journeys.Tracking Lives Lost during Migration* in Action Plan against migrant smuggling (2015:2020), Brussels: European Commission, p. 2.

nections of the migrants with the centers of international, especially mass terrorism. Abraham R. Wagner considers the Internet and the social networks ideal for carrying out terrorist activities and operations since they provide for geographically unlimited and fast communication which is not costly (Wagner 2005: 1-28). He also states that the use and abuse of the Internet by the terrorists go into four main directions: 1) use of the Internet for inter-personal communication of terrorists, 2) access to various information found on the Internet which can also imply potential targets of attacks as well as technical details concerning, for instance, firearms assembly, 3) use of the Internet for spreading terrorist ideas and organization of terrorist activities, and 4) carrying out terrorist attacks *via* the Internet.

Also indisputable is the fact that among the terrorists in the Western countries there are immigrants, either those who have just arrived to the European continent or those who represent the second or even third generation of immigrants. Regardless of their not having any direct connections with today's migrants or their being most often born as non-Muslims, they are more often found among the protagonists of terrorist attacks. Thanks to the modern means of communication, most of all to the Internet and the social networks, they are so indoctrinated that they carry out the idea of "jihad".

Many researchers, scientists and people dealing with safety challenges have been pointing, for so many years, to the fact that the European safety is threatened by a great danger from a small base of enormous Muslim Diaspora (Hoffman 2006). Carlos Ortiz has warned that the political refugees after 1990 have become a medium for particular radical circles of Muslim communities in Europe that have ensured jihadists for conflicts in the Near East and influenced the formation of terrorist cells in Europe." „The attacks in Madrid on March 11, 2004, and Londonon July 7, 2005, were fed from this terrorist pool" (Ortiz 2010:106). However, when it comes to this very issue, it is necessary to be cautious in estimates since every simplified identification of radicalized and instrumentalized minority with the majority of the wretched ones, those who fight for their own lives, leads to stereotypes that are just a step away from prejudice or even other different unacceptable attitudes.

## CONCLUDING REMARKS

The migrations of populations are phenomena that the human civilization has been facing since the first days of its coming into being. Changes take place in circumstances, conditions and ways in which they are realized but not in man's aspiration to find a safer and better place to live in. The basic driving motive to migrate is most often of economic nature but in more recent times war devastations undertaken under the pretense of the struggle to impose democracy – which are, in fact, attempts to create the world monocentric globalized order – contributed to the launching of a huge migrant wave that, since 2015, has been splashing against the European shores. Under the changed technological conditions that have brought about an intensive growth of the information-communication means, the wave has created serious challenges to the human, national and international safety.

The contemporary international migrations cannot be studied without taking into consideration modern technologies, Internet and social networks. The global social networks have alleviated the lives of many migrants but they have, at the same time, fostered further growth of computer criminality. In many cases, and especially within the migrant wave, the computer networks are used as means or tools for achieving certain criminal goals, starting from on line offers of sexual services, human organs and people trade to the spread of racist or Nazi ideologies or preparation and completion of terrorist actions.

Generally speaking, it is the networks that provide for pathways and channels of the very migration processes. They function through intermediaries transferring information about the opportunities for movement and finding one's way both on the migrant trail and in the desired country that the migrant is aspiring to. Those channels can be developed through a series of personal connections – family, friendly, fellow collegial – as well as *via* the links that do not assume any personal contacts such as media, job ads, and the like. It is certain, however, that the importance of human intermediaries in the migration process is exceptionally great. Since the social networks are formed on the basis of different kinds of relations, it is quite certain that, if the aim is to monitor and affect a peaceful flow of the migrant process, the patterns of networking should be carefully studied. The networks created by the migrants fundamentally depend on the historical and cultural attitudes toward migrations as well as on those people who want to abuse these very processes. The building of the migration management system should be focused on the characteristic migration profile, trends, needs and chances in the countries that the migrants come from since it is the best way of efficiently responding to the future challenges along with the simultaneous use of some of their features.

The migration wave has fully affirmed people smuggling as a new „business" of organized crime. In fighting against people smugglers and their networking organization it is recommendable to be present at the Internet and the social networks as much as possible. The Europol, rightfully, insists upon the support to the national bodies in detecting the propaganda materials used by smugglers, in accordance with the national laws, and for the sake of their elimination. In this respect it is necessary to set up a closer cooperation with those offering Internet services and social networks. The evidence gathered from the migrants confirm that the smugglers use, to a large extent, social networks and mobile communication for sharing information about the services they provide. That is why it is important to develop counter argumentation in the media in order to reveal their lies, together with the communities in the Diaspora.

The monitoring of the communication statements on the social networks and in the Internet communities provides for safety stability in real time. Increasing is the number of countries in which this opinion is gaining in importance. The Internet and the networks are monitored in China, Turkey, Iran, Pakistan, North Korea and some other countries; the possibility of monitoring has even been announced by the United States Secretary of Homeland Security John Kelly saying that America could soon ask from all US visa applicants to hand over their social media passwords before being allowed into the country.[14] This attitude could be objected for not being in accordance with the commitment to the freedom of speech. Yet to this it cannot be objected that it fails to stress the need for full carefulness and tracking of the developments on the social networks, most of all because of the worries for the country's safety.

The gathering together of ideological and interest groups due to the Internet has made more dynamic the character and nature of terrorist and criminal activities that are, instead by organizational hierarchies, all the more often united by information activities. At the same time, the patterns of activity are becoming uniform while the interstate or even global cooperation is developing which means that the risks and threats of violence are becoming more and more prominent. The system of safety actions is undergoing a revolutionary transformation; without media there is neither stable communication among the actors themselves nor between actors and public.

Hence the identification and a detailed insight into various roles that the social networks have within the framework of international migrations – from the preparation of migrants to start a journey through their behavior on the road till the tracking of their stay in the coun-

14 More about it in TV N1. (2017). "Viza za SAD? Uslov: Šifre profila sa društvenih mreža" ("Visa for the USA? Condition: social media passwords"), *TV N1*, Belgrade, broadcast on February, 8, 2017.

try they arrive in – represent a key not only for enlarging the knowledge about international migrations and setting up a theoretical framework for their studies but, first of all, one of the essential conditions for preserving personal, national and international safety.

## REFERENCES


1. Aracki, Z. (2016). „Medijski diskurs izbeglištva“ („Media Discourse of Refugeeism“), *Kulturapolisa*, Vol. XIII, No 31. Novi Sad/Belgrade: Kultura – Polis/InstitutzaEvropskestudije
2. Beck, F. (2016). *Die geheimeMigrationsagenda*, Rottenburg: Kopp Verlag
3. Knežević, Ž. (2017), "Krijumčari migranata iz Turske transport plaćali do 5.000 evra" ("Smugglers of Migrants from Turkey Charged for Transport up to 5000 euro", *Blic*, Belgrade, March, 24, 2017
4. Castles, S. (1986). „The Guest Worker in Western Europe: An Obituary“. *International Migration Review*, 22(4)
5. Castles, S., Miller, M.J. (1993). *The Age of Migration – International PopulationMovements in the Modern World*. New York: The Guilford Press
6. DWN, (2015). "BF", *Deutschen Wirtschafts Nachrichten*, Blogform Social Media GmbH, Deutschland: Berlin
7. Elliott, A.&Merrill, F. (1961). *Social Disorganization*. New York: Harper and Brothers, Publishers
8. Ghrib, A. (2002). "Trafficking in Unaccompanied Minors – France", in *Trafficking in Unaccompanied Minors in the European Union*, IOM– IHESI, Brussels – Paris
9. HINA, (2017). "Masovni seksualni napadi dogovoreni preko društvenih mreža?" ("Mass Sexual Assaults Arranged for Through Social Networks", *NA HINA*, Zagreb
10. Hoffman B. (2006). *Inside Terrorism.* Columbia University Press. New York
11. International Organization for Migration, (2014) *Fatal Journeys. Tracking Lives Lost during Migration* in Action Plan against migrant smuggling (2015:2020), Brussels: European Commission
12. Milašinović, S. &Jevtović, Z. (2013), *Metodologija istraživanja konflikata i krizno komuniciranje u savremenom društvu*(*Methodology of Conflict Research and Crisis Communication in the Contemporary Society*), Kriminalističko-policijskaakademija, Belgrade
13. Mitrović, B. (2017). "Crvenikarton od Orbana: Soroš proglašen za "persona non grata" u Madjarskoj" ("Red Card from Orbán: Soros Declared *Persona Non Grata* in Hungary"), *Newsweek*, Belgrade, January, 23, 2017
14. Ortiz, C. (2010). *Private Armed Forces and Global Security: A Guide to the Issues.* Praeger, Santa Barbara, California
15. Starčević, M. (2016). "Globalno odvezivanje ljudske mase" ("Global Letting Loose of Human Mass"), *Geopolitika*, No. 101, Belgrade
16. Tanjug. (2017). "Oko 34 milionaljudi u EU smatraju se migrantima" ("About 34 million people in the EU are considered migrants"), *NA TANJUG*, Belgrade, broadcast on March, 19, 2017
17. Tanjug. (2017). "Nadjena tela petorice migranata, strahuje se da sustotin epoginule" ("Five dead bodies of migrants found; fear that hundreds of them died"), *NA Tanjug*, Belgrade, broadcast on March, 24, 2017

18. TV N1. (2017). "Vizaza SAD? Uslov: Šifre profila sa društvenih mreža" ("Visa for the USA? Condition: social media passwords"), *TV N1*, Belgrade, broadcast on February, 8, 2017
19. Wagner, R. A. (2005). "Terrorism and the Internet: Use and Abuse." In:e book: *Fighting Terror in Cyberspace,* Ed. By: Mark Last (*Ben-Gurion University of the Negev, Israel*), Abraham Kandel (*University of South Florida, Tampa, USA*).World Scientific, Series in Machine Perception and Artificial Intelligence, Vol. 65
20. Weaver, C.A.& Morrison, B.B. (2008). "Social Networking", *IEEE Computer* 41(2)

# PREVENTION OF CYBERCRIME BY PEDAGOGICAL WAYS

**Natalia Khodyakova, Doctor of Science (Pedagogy)**
Professor of the Department of Philosophy
of the Volgograd **Academy of the Ministry of Interior of Russia;**
**e-mail:** hodyakova@rambler.ru
**Olga Krachinskaya, Candidate of Science (Philosophy)**
Head of the Foreign Languages Department
of the Volgograd **Academy of the Ministry of Interior of Russia;**
**e-mail:** olga-krachinskaya@yandex.ru

**Summary:** The article deals with the phenomenon of modern cybercrime, threats to both society and person's safety it causes, the conditions of its origin (appearance) and spread. The authors determine directions of prevention of cybercrime. Special attention is paid to pedagogical ways of cybercrime prevention.

**Key-Words:** cybercrime, prevention, pedagogical prevention of cybercrime.

The official legal thesaurus of legislative and regulatory legal acts of the Russian Federation doesn't contain the concept of cybercrime. There are similar concepts in the Criminal Code of the Russian Federation:

- fraud in the field of computer information;
- illegal access to computer information;
- creation, use and distribution of the malicious computer programs;
- violation of rules of operation of means of storing, processing or transmissing computer information and information-telecommunication networks.

However, this concept is used and interpreted in some international documents.

For example, the European Convention on Cybercrime[1] adopted in 2001 in Budapest contains more crimes in the list of cybercrimes than mentioned in the Russian list. This Convention includes:

- offences against the confidentiality, integrity and availability of computer data and systems (illegal access and interception, data and system interference, misuse of devices);
- computer-related crimes (computer data forgery, computer fraud);
- crimes related to the content (child pornography);
- crimes related to copyright infringement.

The concept of cybercrime as it is viewed and interpreted by some Russian scholars is given below.

Some Russian scientists consider the term "cybercrime" to be true. In his thesis A. Heller[2] believes the terms "cybercrime" and "crimes in the field of computer information" to be equiv-

1 Evropeiskaya Konventsiya po kiberprestupleniyam (prestupleniyam v kiberprostranstve). Budapesht, 2001. http://mvd.gov.by / The European Convention on Cybercrime (Crimes in the Cyberspace). Budapest, 2001. http://mvd.gov.by

2 Geller A. V. Ugolovno-pravovyie i kriminologicheskiye aspekty obespecheniya zashchity electron-

alents. However, he indicates that cybercrimes are typical for big cities. Taking this statement into consideration we can conclude that it is there where the special work to prevent this type of crimes should be executed.

T. Tropina considers cybercrime to be "a body of crimes committed in cyberspace with (or through) the use of computer systems or computer networks, as well as any other means of access to cyberspace, within computer systems or computer networks and against computer systems, computer networks and computer data"[3]. In her opinion, owing to` their latent and transnational nature the fight against cybercrimes should not be limited (at the state level) by imposing a punishment in accordance with the Criminal Code of the Russian Federation. It requires developing common (unified) international approaches and standards, as well as both the legal and social forms of control. Among the specific characteristics of cybercrimes T. Tropina marks their thorough planning, the increasing number of both parties: juveniles as the subjects of cybercrimes commission and their victims due to the personal factors. These peculiariries make the pedagogical community socially responsible for becoming cybercriminals among the students, lack of the psycho-pedagogical work to ensure information safety of the person.

T. Lopatina[4] researches the need for preventive education that stimulates the personal activity of potential victims of computer-related crimes. In her opinion, such preventive work requires special training of the Internal Affairs bodies' officers, methodological work (documents) on the tactics of computer-related crimes prevention.

V. Bagdeyeva[5] pays her attention to the fact of non-stop (steady) appearance of new cybercrimes and modification of known ways of their commission. It means that cybercrimes prevention aimed solely to control the ways of their commission won't be enough effective. Preventive work should be focused on the subjects, inventing new ways and means of cybercrimes commission.

V. Mashlykin and A. Konovalov[6] list the following factors affecting the success of the fight against cybercrimes: political, economic, military, social, demographic, legal, religious, informational, cultural, psychological and other.

A. Zaporozhets[7] analyzes the early demonstration of antisocial behavior of some individuals in the information space while schooling (cyberhooliganism, computer addiction, cyber crimes, cyber terrorism). In his opinion, these negative phenomena can be prevented by such teaching measures as:

noi informatsii i Interneta: dissertatsiya kandidata juridicheskikh nauk. M., 2016. 219 s. / Heller A. V. Criminal Law and Criminological Aspects of the Protection of Electronic Information and the Internet: Thesis for Master Degree in Law. M., 2016. 219 p.

3 Tropina T.L. Kiberprestupnost: ponyatiye, sostoyaniye, ugolovno-pravovyie mery borby: dissertatsiya kandidata juridicheskikh nauk. Vladivostok, 2005. 235 s. / Tropina T.L. Cybercrime: Concept, State, Criminal Law Measures of Struggle: Thesis for Master Degree in Law. Vladivostok, 2005. 235 p.

4 Lopatina T. M. Viktimologicheskaya profilaktika prestupleniy v sphere kompyuternoi informatsii. www.sovremennoepravo.ru / Lopatina T. M. Victimological Prevention of Crimes in the Field of Computer Information. www.sovremennoepravo.ru

5 Bagdeeva V.A. Problemy mezhdunarodnoi kiberprestupnosti // Aktualnyie problemy rossiyskogo prava. № 3, 2009. S. 564-572 / Bagdeyeva V. A. Problems of International Cybercrime // Actual Problems of Russian Law. No. 3, 2009. P. 564-572.

6 Mashlykin V. G., Konovalov A. M. Realiyi "informatsionnogo Apokalipsisa": kiberprestupnost, kiberterrorism, kiberoruzhiye. http://ieras.ru/111.htm / Mashlykin V. G., Konovalov A. M. Realities of an "Information Apocalypse": Cybercrime, Cyberterrorism, Cyber-Warfare. http://ieras.ru/111.htm

7 Zaporozhets A.V. Pedagogicheskaya profilaktika addiktivnogo povedeniya shkolnikov v sphere informatsionno-kommunikatsionnyih tekhnologiy: dissertatsiya kandidata pedagogicheskikh nauk. Chelyabinsk, 2010. 172 s. / Zaporozhets A.V. Pedagogical Prevention of Addictive Behavior of Pupils in the Field of Information and Communication Technology: Thesis for Master Degree in Pedagogy. Chelyabinsk, 2010. 172 p.

- the formation (creation) of information culture;
- the implementation of informational and cognitive needs of the students;
- the organization of socio-cultural interaction of students, parents and teachers;
- the scientific and methodological support of preventive work.

In his thesis D. Matviyenko[8] demonstrates close to A. Zaporozhets' point of view. He considers it to be possible to avoid crimes (offences) in the information space, if fostering the culture of information behavior, thinking and outlook among users. The author offers information education, personification, propaganda of the ideal forms of information behavior as ways (directions) of the formation of information culture.

Cybercrime threatens seriously to information safety of the person(s), state and society. In her thesis A. Sapozhnikova[9] suggests considering cooperation of the administrative bodies, enforcement structures and civil society ones, as well as opportunities for social participation and control as the most important means to confront these threats. The author rightly argues that threats to information safety can't be regarded as a problem to be solved by technical (technological) ways solely. Such means as the ideological "promotion" of the values of culture and civil society, imlementation of the social partnership strategies must play a part while protecting the person(s), state and society against cybercrime.

In the research work by L. Sudareva[10] the author exposes the following causes and conditions to transform a person into a cybercriminal:

- the low level of cultural and economic development of society;
- the low social status of the individual;
- the motivation to get material gain;
- professional skills to use information technologies.

It is necessary to note that the following processes ensure the prevention of cybercrime, on the one hand, and, on the other hand, belong to the competence of teachers and, therefore, can be executed by pedagogical ways. Among them are such factors as:

- increasing the cultural development level of a person;
- forming socially important motives of activity of a person;
- creating necessary conditions for successful socialization of an individual;
- teaching information technologies.

The research work by Ye. Zerkina[11] is devoted to the problem of pedagogical prevention of the students' deviant behavior in the information and communication technology field. It

8 Matvienko D. V. Kultura informatsionnogo povedeniya polzovateleiy Internet: philosophsko-kulturologicheskoe issledovaniye. Krasnodar. 2009. 187 s. / Matviyenko D. V. Culture of Information Behavior of the Internet User: Philosophical and Cultural Research. Krasnodar, 2009. 187 p.

9 Sapozhnikova A. S. Vzaimodeistviye gosudarstva i obshchestva v politike mezhdunarodnoi bezopasnosti RF: dissertatsiya kandidata politicheskikh nauk. M. 2009. 191 s. / Sapozhnikova A. S. Cooperation of State and Society in the Information Safety Policy of the Russian Federation: Thesis for Master Degree in Politics. M., 2009. 191 p.

10 Sudareva L.A. Pravovoye i informatsionnoye obespecheniye deyatelnosti organov vnutrennikh del po preduprezhdeniyu kompyuternykh prestuplenii: dissertatsiya kandidata juridicheskikh nauk. M., 2008. 250 s. / Sudareva L.A. Legal and Information Support of the Internal Affairs Bodies Activities to Prevent Computer-Related Crimes: Thesis for Master Degree in Law. M., 2008. 250 p.

11 Zerkina Ye. V. Podgotovka budushchikh uchitelei k preventsii deviantnogo povedeniya shkolnikov v sphere informatsionno-kommunikatsionnyih tekhnologiy: dissertatsiya kandidata pedagogicheskikh nauk. Magnitigorsk, 2007. 187 s. / Zerkina E. V. Training Future Teachers to the Prevention of Deviant Behavior of Pupils in the Field of Information and Communication Technology: Thesis for Master Degree in Pedagogy. Magnitogorsk, 2010. 187 p.

justifies such a means of prevention, as the project activity in the information space by using a variety of social services.

Many cybercrimes are committed based on the users' ignorance. So another pedagogical way of cybercrime prevention can be considered as teaching measures of self-defense to users[12] . Such teaching can be implemented through the efforts of public agencies, state educational institutions, within the public-state cooperation. A fundamentally important requirement to discuss teaching is to inform users about existing cyber-threats as much as possible.

800 students and experts in the field of information technology took part in the studies in 2008 and 2011[13] . They demonstrated a low level of the respondents' awareness on cybercrimes. On the basis of these data the author made a conclusion about necessity to involve mass media and public authorities to carry out educational work with the population and potential risk groups.

Summing up the short review of research works, some conclusions about the possibilities of prevention of cybercrime by pedagogical means can be made:

1. Prevention should be carried out in the cities, where there are many educational institutions to teach information technology to the young people as their future profession.

2. Pedagogical workers and psychologists of educational institutions as well as officers of the Internal Affairs bodies (juvenile inspectors, divisional inspectors) can be the subjects of socio-pedagogical control of the young people involvement in information technology. While computer science and its disciplines courses should be focused on teaching computer competence not so much, as developing information culture of the user[14].

3. In addition to teachers, psychologists and police officers the representatives of public authorities, the mass media, and all involved in economic and social life parties (such as banks, software manufacturers, providers of Internet services, mobile operators, etc.) can implement purposeful preventive work to inform the public about subjects, ways and means of cybercrimes commission and their consequences. While informing it would be correct to teach, first of all, the fundamentals of information safety of the person.

4. To implement this preventive work competently it is necessary to teach the appropriate personnel and to develop teaching materials for them containing textbooks for students, guidelines for subjects of the preventive work, instructions on information safety for the citizens.

5. Special preventive work must be planned and implemented with a specific segment of the youth: groups of the young people and teenagers attending classes in the clubs for programmers, the students of universities and colleges, mastering the IT profession. It is the respected teachers who must be the subjects of this preventive educational work to have a positive result.

6. To implement this preventive work it is also necessary at the state level to solve the issue to refuse to register that segment of mass media devoted to use information technology for antisocial purposes (including the Internet publications) that in detail inform their readers

12 Ponimaniye kiberprestupnosti: rukovodstvo dlya razvivajushchikhsya stran. Mezhdunarodnyi sojuz elektrosvyazi. Zheneva, 2009. 228 s. http://gipi.kg / Understanding Cybercrime: a Guide for Developing Countries. International Telecommunication Union. Geneva, 2009. 228 p. http://gipi.kg

13 Molodchaya E. N. Politika protivodeistviya kiberterrorizmu v sovremennoi Rossii: politologicheskiy aspect: dissertatsiya kandidata politicheskikh nauk. M. 2011. 188 s. / Molodchaya Ye. N. Policy to Counteract Cyber-Terrorism in Modern Russia: Political Aspect: Thesis for Master Degree in Politics. M., 2011. 188 p.

14 Khodyakova N.V. Informatsionnaya kultura lichnosti i protsess ejo formirovaniya. Volgograd, 2016. 107 s. / Khodyakova N.V. Information Culture of the Person and the Process of (its) Formation. Volgograd, 2016. 107 p.

(or users) about the algorithms of "hacking" systems of information protection and schemes of IT-fraud, analyze software vulnerabilities, ways to bring the computer-and-telecommunication equipment to malfunction, etc. On the contrary, the activity of such mass media is useful, that promotes a civilized approach to information technology and an observance of computer law regulations, inform about the successful IT-experts with the high level of information culture.

7. To prevent cybercrime it is necessary to develop information sites and institutions of the social partnership of different structures that can implement new forms and more effective methods to counteract computer-related crimes. In addition to mentioned-above measures, it is necessary to establish creative contests and competitions to develop socially important projects, demonstrating intellectual abilities of the risk group representatives (potential cybercriminals). Such preventive work can and should be stimulated by grants.

We pay your attention to the fact that the first steps in the field of the formation of information culture of the higher education establishments students in the Russian Federation has already been made. A new purpose of teaching computer science and information technology to the students and posrgraduate students – information culture of the person – has been described and substantiated by N. Gendina, Ye. Danilchuk, N. Khodyakova, etc. while using the scientific-pedagogical fundamentals. Structural-dynamic model of the formation of information culture of the person and optimal pedagogical methods and ways of teaching information technology have been developed. Convincing practical results have been received in the experimental educational institutions.

So, in the Volgograd Academy of the Internal Affairs Ministry of the Russian Federation for more than 15 years the post-graduate students have been taking courses in such humanitarian problems of informatization and computerization, as:

- exclusion of the traditional cultural values from the information space;
- the negative social consequences of computer errors;
- the negative affect of information technology on physical and mental health;
- dependence of the person's life and well-being on digital information related to him / her.
- cybercrime.

While taking these courses the post-graduate students develop their personal multimedia projects on various aspects of information culture ("Computer Ethics", "Computer Aesthetics", "Computer Law", "Computer Ergonomics", "Values of Information Society", "Man and Computer", etc.) and discuss them in the group. Doing mini-researches (an essay or an article) the post-graduate students take part in serious discussions with experts-pragmatists, defending their professional and personal points of view related to information culture of the person. Considering the fact that after graduation from the post-graduate courses their students join the teaching staff of the higher educational establishments of the Internal Affairs Ministry of Russia it can be stated that they will present their socially important views to cadets in the future.

However, not each educational organization has such experience. The formation of information culture has not been yet recognized as a strategic purpose of IT -education. Although the countries participating in the Bologna process agreed to teach information and communication competence to schoolchildren and students as necessary, however, its content is understood by teachers and education managers as utilitarian, beyond social, humanitarian and cultural context of information processes.

While not denying the importance of information and communication competence as the purpose of teaching computer science and information technology, we emphasize that it occupies an intermediate position in the triad: computer competence – information and communication competence and information culture. If computer competence and information and communication competence prove to be the tasks to be possible to solve while studying at school or higher educational establishment, information culture is a strategic purpose for a person to navigate his / her life defending cultural values in the information space and overcoming cyber threats to be faced with.

## REFERENCES:

1. Bagdeeva V.A. Problemy mezhdunarodnoi kiberprestupnosti // Aktualnyie problemy rossiyskogo prava. № 3, 2009. S. 564-572 / Bagdeyeva V. A. Problems of International Cybercrime // Actual Problems of Russian Law. No. 3, 2009. P. 564-572.
2. Geller A. V. Ugolovno-pravovyie i kriminologicheskiye aspekty obespecheniya zashchity electronnoi informatsii i Interneta: dissertatsiya kandidata juridicheskikh nauk. M., 2016. 219 s. / Heller A. V. Criminal Law and Criminological Aspects of the Protection of Electronic Information and the Internet: Thesis for Master Degree in Law. M., 2016. 219 p.
3. Evropeiskaya Konventsiya po kiberprestupleniyam (prestupleniyam v kiberprostranstve). Budapesht, 2001. http://mvd.gov.by / The European Convention on Cybercrime (Crimes in the Cyberspace). Budapest, 2001. http://mvd.gov.by
4. Zaporozhets A.V. Pedagogicheskaya profilaktika addiktivnogo povedeniya shkolnikov v sphere informatsionno-kommunikatsionnyih tekhnologiy: dissertatsiya kandidata pedagogicheskikh nauk. Chelyabinsk, 2010. 172 s. / Zaporozhets A.V. Pedagogical Prevention of Addictive Behavior of Pupils in the Field of Information and Communication Technology: Thesis for Master Degree in Pedagogy. Chelyabinsk, 2010. 172 p.
5. Zerkina Ye. V. Podgotovka budushchikh uchitelei k preventsii deviantnogo povedeniya shkolnikov v sphere informatsionno-kommunikatsionnyih tekhnologiy: dissertatsiya kandidata pedagogicheskikh nauk. Magnitigorsk, 2007. 187 s. / Zerkina E. V. Training Future Teachers to the Prevention of Deviant Behavior of Pupils in the Field of Information and Communication Technology: Thesis for Master Degree in Pedagogy. Magnitogorsk, 2010. 187 p.
6. Lopatina T. M. Viktimologicheskaya profilaktika prestupleniy v sphere kompyuternoi informatsii. www.sovremennoepravo.ru / Lopatina T. M. Victimological Prevention of Crimes in the Field of Computer Information. www.sovremennoepravo.ru
7. Matvienko D. V. Kultura informatsionnogo povedeniya polzovateleiy Internet: philosophsko-kulturologicheskoe issledovaniye. Krasnodar. 2009. 187 s. / Matviyenko D. V. Culture of Information Behavior of the Internet User: Philosophical and Cultural Research. Krasnodar, 2009. 187 p.
8. Mashlykin V. G., Konovalov A. M. Realiyi "informatsionnogo Apokalipsisa": kiberprestupnost, kiberterrorism, kiberoruzhiye. http://ieras.ru/111.htm / Mashlykin V. G., Konovalov A. M. Realities of an "Information Apocalypse": Cybercrime, Cyberterrorism, Cyber-Warfare. http://ieras.ru/111.htm
9. Molodchaya E. N. Politika protivodeistviya kiberterrorizmu v sovremennoi Rossii: politologicheskiy aspect: dissertatsiya kandidata politicheskikh nauk. M. 2011. 188 s. / Molod-

chaya Ye. N. Policy to Counteract Cyber-Terrorism in Modern Russia: Political Aspect: Thesis for Master Degree in Politics. M., 2011. 188 p.

10. Ponimaniye kiberprestupnosti: rukovodstvo dlya razvivajushchikhsya stran. Mezhdunarodnyi sojuz elektrosvyazi. Zheneva, 2009. 228 s. http://gipi.kg / Understanding Cybercrime: a Guide for Developing Countries. International Telecommunication Union. Geneva, 2009. 228 p. http://gipi.kg
11. Sapozhnikova A. S. Vzaimodeistviye gosudarstva i obshchestva v politike mezhdunarodnoi bezopasnosti RF: dissertatsiya kandidata politicheskikh nauk. M. 2009. 191 s. / Sapozhnikova A. S. Cooperation of State and Society in the Information Safety Policy of the Russian Federation: Thesis for Master Degree in Politics. M., 2009. 191 p.
12. Sudareva L.A. Pravovoye i informatsionnoye obespecheniye deyatelnosti organov vnutrennikh del po preduprezhdeniyu kompyuternykh prestuplenii: dissertatsiya kandidata juridicheskikh nauk. M., 2008. 250 s. / Sudareva L.A. Legal and Information Support of the Internal Affairs Bodies Activities to Prevent Computer-Related Crimes: Thesis for Master Degree in Law. M., 2008. 250 p.
13. Tropina T.L. Kiberprestupnost: ponyatiye, sostoyaniye, ugolovno-pravovyie mery borby: dissertatsiya kandidata juridicheskikh nauk. Vladivostok, 2005. 235 s. / Tropina T.L. Cybercrime: Concept, State, Criminal Law Measures of Struggle: Thesis for Master Degree in Law. Vladivostok, 2005. 235 p.
14. Khodyakova N.V. Informatsionnaya kultura lichnosti i protsess ejo formirovaniya. Volgograd, 2016. 107 s. / Khodyakova N.V. Information Culture of the Person and the Process of (its) Formation. Volgograd, 2016. 107 p.

# NEW CHALLENGES IN FIGHTING FINANCIAL CYBERCRIME

**Saša Živanović**
Cyber Crime Department, Ministry of Interior of the Republic of Serbia
*sasa.zivanovic@mup.gov.rs*
**Brankica M. Popović**
Academy of Criminalistic and Police Studies, Belgrade, Serbia
*brankica.popovic@kpa.edu.rs*

**Abstract:** Originated almost fifty years ago and widely utilized since 90's of the 20th century, the Internet as a global network has become a necessary tool in almost every aspect of human modern life. A wide range of diverse applications have emerged, including numerous e-commerce and e-banking services. Unfortunately, like most other achievements, the Internet has also a dark side that can be abused. Today we are witnessing that the Internet is often used for various types of fraud, the distribution of pedophile material and other forms of cybercrime. Material damage caused by the financial cybercrime at global level is measured in billions of US dollars. Features of the Internet, especially the ability to operate covertly and anonymously, often through the use of zero day vulnerability, are increasingly used by organized criminal groups in the performance of financial cybercrime. Their targeted (spear phishing) attacks in recent times are not directed only at multinational and large corporations, but also at small and medium enterprises (SMEs) and their computers serving primarily for e- banking and e-commerce applications. Moreover, a large share of today's financial cybercrime represents malware infections with the so-called ransomware which encodes virtually all user data on the computer, requiring ransom (often in crypto values) to reveal the corresponding key in order to decrypt the data. As a rule, beside ransomware infections, the victims realize that they are the targets of financial cybercrime after the completion of financial transactions from their business accounts. In the case of business e-mails compromised in the so-called 'Directors' scams', victims realize the deception only after several days that is when contacting the foreign partner, usually by a phone call. In this paper the phenomenon of financial cybercrime will be explained with the focus on the organization and methodology of organized criminal groups operation. Special emphasis is placed on explaining financial cybercrime attack vectors as well as proactive approach to counteract them.

**Key words:** Internet, fraud, financial cybercrime, ransomware

## INTRODUCTION

The phenomenon of financial cybercrime cannot be considered as a new one, but unlike the previous time, today it is considered as one that takes a dominant role in cyberspace, and occurs as a result of increasing presence and use of information and communication technologies (ICT).

Different factors motivate cybercriminals, either alone or through an organized criminal group, to comitt the criminal act of financial cybercrime, but the most important ones are:

the expansion of electronic commerce, frequent international financial transactions, the diversity of legal systems, the complexity of ICT networks, availability of automated tools for committing cybercrime acts (the so-called crimware[1] service), increased rates of zero-day vulnerabilities[2], spear phishing[3] attack that is now focused on small and medium-sized companies, etc. [1, 4]

The evidence base for how 'cyber' has contributed to financial (economic) crimes is incomplete and weak, both today and over time, since unlike cyber security vendor data, it depends on victims or others identifying and communicating their experience of an economic crime and also their idea about how it was done. Nevertheless, according to a document[4] published on 14 June 2016 by the US Federal Bureau of Investigation - Center for reporting cybercrime (FBI IC3), we can state that there is a dramatic increase in the *business e-mail compromise scams* (the so-called 'Directors' scam') which have caused business losses of about 3.1 billion US dollars, involving almost a hundred (100) countries in the world since 2013. Furthermore, in early 2015, the US Director of National Intelligence James R. Clapper[5] identified cybercrime as the greatest national security threat, ranked above the threats of terrorism and espionage, noting that an increasing number of countries in the world put the combat against cybercrime as a priority in its security.

## CONCEPT OF FINANCIAL CYBERCRIME

Although there are several definitions of a financial or economic cybercrime, among which the easiest one is mentioned in the report from the University of Cardiff called "Implications of Economic Cybercrime for Policing"[6] stating that 'it is simply a fraud through the use of the Internet", we would like to define financial cybercrime as "comitting a crime in a cyberspace in order to obtain data, goods and/or money (financial gain and theft of intellectual property)". This definition is a comparative compared to traditional economic and financial crimes, for example fraud in business operations by submitting forged documents, phishing and others, only that it is taking place in the electronic ambience the so-called cyber space consisting of computers, computer networks and the people that use them in the business environment.

Today, financial cybercrime can be understood as having two different forms:

- Criminal activities dependent on networked information and communications technology (ICT), largely via the internet, such as: unauthorized access to protected computers, computer networks and electronic data processing, computer fraud, creating and introducing computer viruses, damages of computer data and programs. The offending would not be possible without access to a computer network (mainly through the largest global network-Internet), and

- Criminal activities of traditional crimes such as fraud, extortion, robbery, that are enabled and facilitated by ICT, but are not dependent upon them, and therefore can exist in some non-cyber form.

1 http://searchsecurity.techtarget.com/definition/crimeware
2 'What is a Zero-Day Vulnerability?', Security News at pctools by Symantes, http://www.pctools.com/security-news/zero-day-vulnerability/
3 'What is Spear Phishing?', KasperskyLab, https://usa.kaspersky.com/resource-center/definitions/spear-phishing
4 https://www.ic3.gov/media/2016/160614.aspx
5 http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/
6 https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/research-2015/Economic-cybercrime-Summary-Report.pdf (pp.5)

The evolution of cybercrime (high-tech crime) leads to availability and sophistication of various malicious tools, where advertisement, application and even arrangements for criminal activity usually takes place in digital underground, the so-called darkweb[7] using a non-standard communication protocols and ports, making the investigation in such cyberspace very difficult. Digital underground is further increasing through a large number of forums focused on offering services, tools and information about the compromised payment cards, as well as the theft of money from the accounts of legal entities and individuals. The anonymity provided by darkweb favored the creation of organized criminal groups that unlike traditional organized crime groups work on partnerships.

Recruitment for such criminal groups is carried out sometimes in the form of offering a legitimate job, and the organization itself is clearly defined by the role of each group member, among which the most important are: the developers and progrmmers responsible for the creation or modification of an existing malicious software (malware), the tester responsible for malware testing, coders whose role is reflected on the repackaging of malware as it would not be recognized by the antivirus software, web designers responsible for creating phishing sites, persons who are responsible for the control, supervision and drawing money from the compromised accounts - called money mules[8]. The criminal group organizers have the task to provide the funds necessary for the creation of malicious tools which would be used for committing a crime. Large organized criminal groups are different from other criminal groups by the fact that their attacks are not directed only to financial institutions and online shopping, but are also focused on the attacks on small and medium-sized enterprises, with even better organization of raising stolen money by using the money laundering techniques. One such criminal group is 'Carbanak'[9] whose actions caused damage to financial institutions and corporate customers in the amount of nearly $ 1 billion US dollars [3].

According to the FBI IC3[10], among others, the following Internet crime schemes and trends are identified:

- *Auction Fraud* - involves fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site;

- *Counterfeit Cashier's Check* - targets individuals that use the Internet classified advertisements to sell merchandise by making them unaware that check they are depositing is fraudulent;

- *Credit Card Fraud* - the unauthorized use of a credit/debit card or card number to fraudulently obtain money or property is considered credit card fraud;

- *Debt Elimination* - schemes generally involve websites advertising a legal way to dispose of mortgage loans and credit card debts having extremely high risk of identity theft;

- *Parcel Courier Email Scheme* - involves the supposed use of various National and International level parcel providers such as DHL, UPS, FedEx etc., the victim is directly emailed by the subject(s) following online bidding on auction sites;

- *Escrow Services Fraud* - in an effort to persuade a wary Internet auction participant, the perpetrator will propose the use of a third-party escrow service to facilitate the exchange of money and merchandise. The victim is unaware the perpetrator has actually compromised a true escrow site and in actuality created one that closely resembles a legitimate escrow service;

7 'What is the Dark Web and Deep Web?', available at: http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-deep-web-3593569/
8 Money mule blog articles by Brian Krebs (https://krebsonsecurity.com/tag/money-mules/)
9 'Carbanak APT', KasperskyLab, available on: https://www.kaspersky.com/resource-center/threats/carbanak-apt
10 More on https://www.ic3.gov/crimeschemes.aspx

- *Identity Theft* - occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. This type of crime is a vehicle for perpetrating other types of fraud schemes;

- *Internet Extortion* - involves hacking into and controlling various industry databases promising to release control back to the company if funds are received. Similarly, the subject will threaten to compromise information about consumers in the industry database unless funds are received;

- *Lotteries* - this scheme deals with persons randomly contacting email addresses advising them they have been selected as the winner of an International lottery;

- *Nigerian Letter* - combines the threat of impersonation fraud with a variation of an advance fee scheme;

- *Pyramid* - investment scams in which investors are promised abnormally high profits on their investments;

- *Phishing/Spoofing*, *Spam* ... etc.

In before mentioned report from the University of Cardiff[11], it was recognized that in last decade data breaches and identity frauds have been rising steadily, and e-commerce fraud losses increased rapidly (especially after the rise of botnets).

## FINANCIAL CYBERCRIME ATTACK FRAMEWORK

An attack stage involves several phases where the first phase, the so-called passive attack, involves information gathering about the targeted company or financial institution and is essential in the development strategy of the next phase of an attack. A passive attack can be skipped in certain cases, for example when it is directed against users of a single electronic sales service, or users of a particular e-bank. In that case those users are directed to phishing sites, or they receive e-mails with relevant content in order to compromise data regarding their accounts and payment cards.

After a passive attack, the techniques of targeted phishing attacks (*spear phishing*) are performed, including sending electronic messages with malicious link or malicious programs attached in order to gain unauthorized access to the computer network. Simply clicking on malicious link/program leads to computer infection, but often the infection is automatically downloaded to the user's computer through a '*drive-by download*' attack or through web sites compromised with exploit kit that redirect users to another (malicious) website. This site contains a malicious code used to identify and exploit the user's computer vulnerabilities.

After penetration into the computer network cyber criminals will, using numerous malicious tools, secure their presence in the network in order to ensure this phase of the attack.

The next phase of attack involves the use of legal programs for remote management and hidden administration of the targeted computer (*remote desktop software*) such as *Teamviewer*, *Microsoft's RDC - Apple's own Remote Desktop*, *VNC - Virtual Network Computing* and others.

After the theft of usernames and passwords for electronic banking services, in the final stage of attack criminals perform money tranfer from the compromised accounts to, in advance opened, accounts of criminal group members (*money mules*) who raise money under the supervision and control of the other criminal group members [2,3].

11 https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/research-2015/Economic-cybercrime-Summary-Report.pdf

## EXAMPLES OF FINANCIAL CYBERCRIME ATTACK

In spite of the fact that crimes related to credit cards misuse are one of the most common crimes in financial cybercrime, we will pay special attention to other two types of crime, namely:

- *Business e-mail compromise scams* which, based on the research of cybercrime reputable company '*Statista Inc*'[12], contributed to the total damage of 246,230,000 USD in 2015, while according to the data from the Federal Bureau of Investigation USA - Center for reporting cybercrime (IC3) the damage from this kind of scam was over 3 billion US dollars globally[13]for the period from 2013 to 2106.

- *Ransomware,* which is considered a special case of the *Internet Extortion*.

## BUSINESS E-MAIL COMPROMISE SCAMS

*Business e-mail compromise scams*, which are also called *Directors' scams, Directorship fraud*, *CEO fraud* or *Man-in-the-Email*, is a sophisticated scam that targets companies mainly with foreign suppliers or customers. The scam is performed through the bank transfer, which is carried out by compromising legitimate business accounts through the techniques of social engineering, sending e-mails or unauthorized intrusions into the computer in order to make the unauthorized transfer of funds[14]. There are several schemes/scenario for the exercise of directors' scam among which the most common in the Republic of Serbia (multi-million damage in euro) is a scenario of changes in the foreign trade payment instructions - SWIFT[15] (Society for Worldwide Interbank Financial Telecommunication). After compromising a targeting (buyer or supplier) computer, the criminal group keeps track of the electronic communication between business partners. When a final agreement is made, the supplier sends the customer an invoice with payment instructions. At that time, that geniune message is intercepted and replaced with a new (fake) one containing payment instructions to previously opened accounts of criminal group members. That account can be opened in the foreign country, and if customer asks for the reason, the usuall explanation is that there are some problems with the old bank.

For the time being, this type of scam is the only one identified in fraudulent acts on the territory of the Republic of Serbia, but apart from it there are other scam schemes. During the attack aimed at large companies, the compromise of the financial director electronic account is performed resulting in the theft of his identity. Then fake e-mail, which looks like a legitimate message from CFO, is sent to another employee responsible for processing bank transfers containing the instructions for an immediate fund transfer to the previously opened account of a criminal group member.

If a company has a long-standing relationship with a supplier, a fake e-mail might have a form of a proposal for the advance purchase of goods before they rise in price suggesting that the buyer will have big savings if they promptly and urgently transfer the funds.

Another scam scheme implies that criminal groups, after compromising e-mail provider, send to clients/buyers fake warnings that there was a problem with their previous payments

12 https://www.statista.com/statistics/234987/victim-loss-cyber-crime-type/
13 https://www.ic3.gov/media/2016/160614.aspx
14 'Business E-Mail Compromise: Cyber-Enabled Financial Fraud on the Rise Globally', FBI News, 2017, available at: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise
15 https://www.swift.com/about-us/history

and that they have to make that payment again, directing them to another account that is owned by a criminal group.

The techniques of social engineering in directors' scams are crucial for the success of the fraud. Criminal groups are usually very innovative and apart from the common attack schemes, they are falsely represented as legal company representatives with different proposals (i.e joint investment or the purchase of the property), claiming that they have a lucrative information, and exerting pressure on the victim to act secretly and quickly in the transfer of funds due to the end of working hours of international financial institutions. Victims are usually contacted before the end of the working day or working week.

While some cases involve the use of malicious software, directors' scams generally rely solely on social engineering techniques, making their detection a difficult task. Some recent examples of fraud have shown that employees were cheated by e-mails that were masked as legitimate CEOs emails. This is achieved by the fact that criminals register a domain similar to his target, for example if the target e-mail is ime@firma.com criminals use a variation such as: ime@firma.net, ime@firna.com, ime@f1rma.com, changing small Latin letter l with number 1 (one), or replacing letter O with number 0 (zero) and the like.

The use of a spoofing email[16] tool in order to mask a fake email message that appears to be sent from a legitimate source for the purpose of identity theft is a frequently used technique in executing directors' scams. These tools are available and easily accessible on the Internet, such as: http://www.anonymailer.net, https://emkei.cz, http://www.sendanonymousemail.net etc.

Malicious tools used in directors' scams also indicate how easy it is for cyber criminals to launch such an attack. Their use allows criminal groups to have unauthorized access to victims' data, including passwords and bank account information, access to legitimate email with payment instructions and other personal data therefore removing any suspicion that fraudulent action is performed. Malware used in tis type of fraud can be easily purchased on the Internet at a good price. Some malware can be bought for as much as $ 50, and some are far cheaper or even free.

Incidents in 2014 showed common methods of attack that cyber criminals are using to steal information. In campaigns that used Predator Pain[17] and unlimited e-mails sent to victims, they contained malware (Keylogger) [18] that sent cyber criminals the victims' confidential information (user names, passwords, etc.). Another fraud campaign performed in March 2016 targeting 18 companies in the US, the Middle East and Asia, was made through a simple malware available on the Internet for $ 25.

In addition to large corporations and companies, the tendency of the last few years points to the fact that the victims of directors' scams are more and more small and medium-sized enterprises. A criminal group first identifies a person in a company authorized to transfer money, then it monitors and studies procedures that that person is using for conducting banking transfers in a particular business environment. Then an appropriate fraud scheme is conducted.

If a legal entity has become a victim of this type of fraud, it is very important to react quickly and take the procedures in the following order [5]:

- Contact the business bank with a request for revocation of money transfer due to a suspicion of fraud;

16 http://searchsecurity.techtarget.com/definition/email-spoofing
17 https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-predator-pain-and-limitless.pdf
18 http://www.ultimatekeylogger.com/free/

- Contact the financial institution on whose account funds are transferred with request for return or freezing of funds;

- Submit a criminal complaint to the prosecutor's office or the police administration in which following data are provided: a brief description of fraud, phone contacts with phone numbers (if available), date and time of the incident, e-mail address of fake messages with *message header/header fields*, content and attachments of electronic messages (invoices, payment instructions, etc.), name, account number, amount of transaction and location of the commercial bank, name, account number, amount of transaction and location of foreign bank to which money is sent, SWIFT number, and other data that are considered to be relevant for making a criminal complaint;

- All data stored in electronic form must be archived on an external memory unit (USB, CD/DVD, cloud storage, etc.);

- Do not delete electronic data related to scam from a computer and memory devices;

- As there is a likelihood of computer compromise, engage a professional who will safely check the computer and the computer network in order to identify and remove malicious software, taking into account the preservation and integrity of electronic evidence relevant to the criminal proceedings.

The best way to proactively deal with directors' scams is a multiple approach to defense against this type of targeted attacks through developing internal procedures and policies and familiarizing employees with this type of scam in order to be able to detect and recognize its schemes. Application of Two Factor Authentication (TFA), not only for corporate e-mail accounts but also for other communication channels before the transaction of funds has proven to be a reliable method to avoid this type of fraud. If possible, use digital signature or cryptographic tools and techniques to exchange electronic messages. When responding to the received e-mail, never use the '*Reply to sender*' function, instead use the function '*New*' or '*Forward*' and enter the e-mail address manually. Always check the newly-received e-mail not to mask a legitimate e-mail account. Configure an e-mail address with the level of importance setting (by using stars, flags ...) in order to emphasize and identify the legitimate electronic addresses with which you communicate. Beware of sudden changes in business practice and communication.

Companies that have implemented strong internal prevention techniques at all levels (especially to personnel who may be the initial victims of fishing attempts) have proved to be very successful in identifying and refusing attempts of directors' scams.

## RANSOMWARE

The expansion and evolution of malicious software in the last few years has been largely experienced by ransomware[19] through a number of campaigns conducted on the Internet [4]. Financial cybercrime proved to be very effective in generating revenue for cyber criminals using ransomware, and in addition has a huge impact on the business of the affected organizations. Almost every company or individual, anywhere in the world and in any industry, are all potential targets and can become the victim of ransomware.

There are a number of definitions of ransomware, but the most comprehensive is the one given through an act to amend Section 523 of the Penal Code relating to computer crimes in the USA state of California on the 27th of September 2016. Among other things, it defines ransomware as a 'computer contaminant or lock placed or introduced without authorization

19 Ransomware, TrendMicro, https://www.trendmicro.com/vinfo/us/security/definition/ransomware

into a computer, computer system, or computer network that restricts access by an authorized person to the computer, computer system, computer network, or any data therein under circumstances in which the person responsible for the placement or introduction of the ransomware demands payment of money or other consideration to remove the computer contaminant, restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock'.[20]

In today's world of financial cybercrime ransomware, especially *cryptographic* ransomware has crossed the path from a minor threat to a sophisticated multi-million criminal enterprise targeting both individuals and companies. It has existed in various forms for decades. The first known ransomware appeared in 1986, and in 1989 the one known as '*PC Cyborg*' was created by hacker Joseph Popp[21]. In May 2005, with the appearance of the first forms of cryptographic malware, the first ransomware extortion was noted, while in the middle of 2006 more sophisticated RSA encryption schemes with stronger key are intorduced, such as *Gpcode*[22], *TROJ.RANSOM.A*, *Archiveus*, *Krotten*, *Cryzip*, and *MayArchive*. The expansion of ransomware occured in 2011, when a ransomware worm appeared to imitate '*Windows Product Activation*' code, and infected a large number of computers in the world. By 2013 almost all attacks mainly targeted systems based on Windows ™ operating system through *Stamp.EK exploit kit*, but it also infiltrated into the Mac OS (Apple computers), making the damage of about 5 million USD in the last quarter of that year. Last few years, ransomware has been experiencing its true expansion through multiple variants on multiple platforms, causing great damage and targeting not only computers and servers, but also smartphones, mainly with the Android operating system. In February 2016, the Republic of Serbia was ranked 10$^{th}$ in the world with 840 infections in one hour with a ransomware tool called *Locky*[23].

There are five basic types of ransomware that also have their own subversion, namely:

- *Encryption Ransomware:* Encodes personal files and folders (documents, tables, images and video). Disputed files are deleted after they are encrypted and users mostly find a text file with a payment instruction in the same folder where now unavailable files existed. The problem is detected at a time when one tries to open any of these files. Some but not all types of encryption software show 'lock screen'.

- *Lock Screen Ransomware – WinLocker*: locks the computer screen and requires payment. Personal files are encrypted.

- *Master Boot Record (MBR) Ransomware: The Master Boot Record* (*MBR*) is a part of the computer hard disk that allows the operating system to boot. *MBR Ransomware* changes computers *MBR* in order to interrupt the normal startup process. Instead (of starting a computer), a ransom request is displayed on the screen with payment instructions (in the cryptocurrency).

- *Ransomware* encoding *web servers*: it targets *web* servers and ancodes all files on it. It exploits known vulnerabilities in CMS to place a ransomware on *web* servers.

- *Mobile device ransomware* (*Android*): Mobile devices (mostly with *Android* operating system) can be infected with ransomware through '*drive-by downloads*' function. They can also be infected through malicious applications masking themselves into popular services such as *Adobe Flash* or anti-malware tools.

Ransomware attack is usually delivered via e-mail messages that could be executable files, archives, or images. When an attachment from an e-mail is opened, the malware is installed

20 http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB1137
21 'The Strange History of Ransomware', https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b (accessed 01.02.2017)
22 http://www.spywaretechs.com/remove-gpcode-ransomware/
23 http://thehackernews.com/2016/02/locky-ransomware-decrypt.html

into the user's system (victim). Cyber criminals can also place malware on websites, and when a user visits this site he is unaware that the malware is installed in his system.

The infection is not immediately visible to the user. Malver runs silently in the background while the computer data are not completely encrypted. Then the dialog box opens and the user of the infected computer is informed that his files are encrypted. He is asked for a ransom (with the instructions for payment in the cryptocurrency) in order to obtain a key neccessary to unlock the encrypted files. By that time it is too late to save any of the data through known security measures. The cryptocurrency, most frequently the *Bitcoin*, has enabled a payout mechanism that encourages the success of this model. Payment mechanisms to which cyber criminals have previously relied are either extinguished or placed under the law, while *Bitcoin* does not have a regulatory mechanism such as the Central Bank and it is virtually impossible to track currents of the cryptocurrency. The biggest attack to date happened in May 2017 when ransomware variant *WannaCry/WCRY*, which originally spread via malicious Dropbox URLs embedded in spam began exploiting a recently patched vulnerability in the SMB Server[24].

As ransomware proved to be profitable in financial cybercrime, in future times it is expected that attacks will take place on more platforms based on all operating systems with the tendency of increasing ransom, particularly in situations when criminal groups know they have encrypted valuable information. The very fact that a large number of victims pay ransom stimulates criminal groups to deal with ransomware campaigns around the world.

However, if there is infection caused by a ransomware campaign, it is necessary to disconnect all devices, turn off all wireless features: *Wi-Fi*, *Bluetooth and NFC*. Next, it is necessary to determine the scale of the infection and to check if the infection occurred in the following places: mapped and shared folders from other computers, external hard drives, USB, all devices for network storage, *Cloud* data warehouse (*Google Drive, OneDrive*, etc.). When you determine with which type of ransomware infection you are compromised, try to find a possible decryptor[25] to unlock the encrypted files on the Internet. If you find a decryption tool, remove ransomware from your computer and all connected devices on the network, then locate your backup and check if all the files you need are valid, verify the integrity of the backup in order to determine if there are files that are corrupted or do not load. Make sure if there are earlier versions of files that are stored in the *cloud*. For new types of ransomware, you will not be able to check *Shadow*[26] copies. When you have checked all this, restore the files from the backup. If you do not find a decryption tool, make backups of encrypted files in order to decrypt it if a decryptor appears later in the future.

Regardless of the fact that ransomware campaigns pose a growing threat, ransomware protection involves several stages of defense, the first of which is adequate employee training through getting to know new threats and multi-layer protection in the existing computing environment through 'endpoint'[27] technology. Implement *antispam* and/or *antiphishing* tools and check weather the firewall is in function. Limit administrator privileges on employee computers to prevent the installation of unwanted software, regularly update operating systems and security antivirus software. In order to reduce potential damage from ransomware campaign, it is necessary to implement a *backup solution* (hardware, software or both). Test the integrity of physical backup files, as well as *ease-of-recovery* from *online* or software backups.

24 https://www.trendmicro.com/vinfo/us/security/definition/ransomware
25 i.e. https://www.nomoreransom.org/crypto-sheriff.php or https://success.trendmicro.com/solution/1114221 or many more
26 Volume Shadow Copy Service https://technet.microsoft.com/en-us/library/ee923636(v=ws.10).aspx
27 http://searchsecurity.techtarget.com/definition/endpoint-security-management

## CONCLUSION

Financial cybercrime is increasingly present because it is motivated by profits with minimal investment, and not by ideology or by some other factor. It will continue to pose a significant threat to the business and integrity of global financial institutions. Financial cybercrime cannot be completely eliminated, but procedures must be made in order to mitigate the risks of such incidents. Modification, and the proliferation of malicious software and the use of illegal networks designed to steal data and money will be increasingly present. Timely introduction to and protection from new threats is a key factor in the proactive act of fighting financial cybercrime, and the only adequate response is found to be a public-private partnership, with the mandatory presence of academic institutions with the government sector.

## REFERENCES

1. Belcher Pat & Geftic Seth. (2016). Crimeware-as-a-Service Goes Mainstream, available at: https://www.invincea.com/2016/09/crimeware-as-a-service-goes-mainstream/ (accessed 20.03.2017)
2. DeSantis Matthew, Dougherty Chad, McDowell Mindi. (2011). Understanding and Protecting Yourself against Money Mule Schemes, Carnegie Mellon University. Produced for US-CERT, available at: https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf (accessed 30.03.2017)
3. GReAT-Kaspersky Lab's Global Research & Analysis Team. (2015). Carbanak APT: The Great Bank Robbery. available at: https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf (accessed 28.03.2017)
4. Ramos Pablo. (2016). Crimeware: Malware and massive campaigns around the world, available at: https://www.welivesecurity.com/2016/06/08/crimeware-malware-massive-campaigns-around-world/ (accessed 25.03.2017)
5. Setera Kristen. (2016). FBI Warns of Dramatic Increase in Business E-Mail Compromise Scams, FBI Boston, available at: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-compromise-scams (accessed 30.03.2017)

# DIGITAL LIBRARY FROM A DOMAIN OF CRIMINALISTICS AS A FOUNDATION FOR A FORENSIC TEXT ANALYSIS

**Dalibor Vorkapić**[1]
University of Belgrade – Faculty of Mining and Geology
**Aleksandra Tomašević**
University of Belgrade – Faculty of Mining and Geology
**Miljana Mladenović, PhD**
eVox Solutions
**Ranka Stanković, PhD**
University of Belgrade – Faculty of Mining and Geology
**Nikola Vulović**
University of Belgrade – Faculty of Mining and Geology

**Abstract:** This paper presents a model that provides harvesting, preparation, metadata description, management and exploitation including full text search over documents from a domain of criminalistics written in Serbian language. Proposed approach is applied in a web portal that collects various texts derived from journals of the Academy of Criminalistics and Police Studies, the Criminal Code of Serbia, the "Tara" and "Reiss" conferences, and from some of PhD dissertations related to this field of research. After text processing, a corpus containing over 5,500 pages of plain text is created and prepared for publication as an online resource for full text search using Omeka, an open source content management system for on line digital library development. Search capabilities, both full text and metadata search are customized and improved by query expansion via web service relying on the Serbian morphological dictionary and the Serbian WordNet semantic network for providing morphological and semantic text search expansion. The paper outlines possibilities for further use and analysis on a digital library as a corpus, annotation, tagging, document classification and clustering, as well as sentiment analysis with the first results in that direction.

**Keywords:** Omeka, WordNet, full text search, morphological and semantic text search, query expansion.

## INTRODUCTION

A digital library as a special library with a focused collection of digital objects stored as electronic documents can vary in size and scope, and can be maintained by individuals, organizations or institutions. The digital content may be stored locally, or accessed remotely via computer networks. An electronic library is a type of information retrieval system.For this research experiment, the texts from the field of criminology were collected, comprising the articles from journals of the Academy of Criminalistics and Police Studies, the Criminal Code of Serbia, the "Tara" and "Reiss" conferences, and from several PhD dissertations related to

1 dalibor.vorkapic@rgf.bg.ac.rs

this field of research. The textthat is not in Serbian language was removed.Tables, figures, references and links, were removed as well, which is usual preparation for corpus processing. After this preparation, thetext collection contained 5,500 pages of plain text, in A4 format, which was used for further text analysis and processing. As a web publishing platform and a content management system (CMS)for digital objects management Omeka[2]was selected. It is developed by the Centre for History and New Media (CHNM) at George Mason University specially for scholarly content, with anemphasis on digital collections and exhibits. While Omeka may not be as readily customizable as other platforms designed for the widespread use, such as WordPress, Omeka has been used by many academic and cultural institutions, mainly because of its built-in features for cataloguing and presenting digital collections. The content developmentin Omeka is complemented by an extensive list of descriptive metadata fields that are incompliance with Dublin Core, thestandard used by libraries, museums and archives. This additional layer helps in establishing proper source attribution, standards for description and organization of digital resources as important aspects of scholarly work in the classroom settings but often overlooked in general blogging platforms.

For the digital library presented in this paper, Omeka is installed on operating system Ubuntu 15.10 in a virtual machine. This virtual machine uses 8GB of RAM and 127GB of memory which is dynamically allocated on the storage and one virtual Xeon processor that runs at 2.6GHz. There are several preconditions forinstalling Omeka:

- Operating systems on which Omeka can work are: Fedora, OpenSUSE and Ubuntu
- It requires a HTTP server, but the recommended one is Apache
- Database management system is MySQL server, version 5 or later
- It requires PHP version 5.3.2 or later.

The Omeka platformis published underGNU licence[3] (General Public), while basic installation, documentation, plug-ins and best-practice examples are freely available athttps://omeka.org. The customisation is user friendly and enables parameters adjustments,including: database name, authentication details, and interface language. For Serbian,the localisation is available and easy to implement with changing in*/application/config*just*locale* = “”to*locale* = *“sr_RS”*.

The Digital library that will be presented in this paper is available athttp://master-kpa.rgf.rs/ for search and browse public use and editing management authorized use. The digital library documentcollection is accessiblethrough user friendly applicationthat is organised in several categories: Journal for Criminalistics and Law, Archibald Reiss, Doctoral Dissertation, and other (final process). Further classification is possible, so categories can contain subcategories, to achieve better organisation of digital objects. For each category or subcategory, it is possible to define a specific collection that will display the entire content of the collection. Apart from navigation and browsing of content, simple and advanced search are available.The administrator panel enables installing and customizing the appearanceof add-ins that are essential for full system functioning, so the platform could adequately respond to the requests. There are four user roles:*super-user*that can do all tasks in Omeka digital library,*admin*for users administration tasks, but withoutaccess to the settings panel, the *contributor*role for editor and *researcher*users for authorized accessing to digital objects.

2 https://omeka.org/
3 https://www.gnu.org/licenses/gpl-3.0.en.html

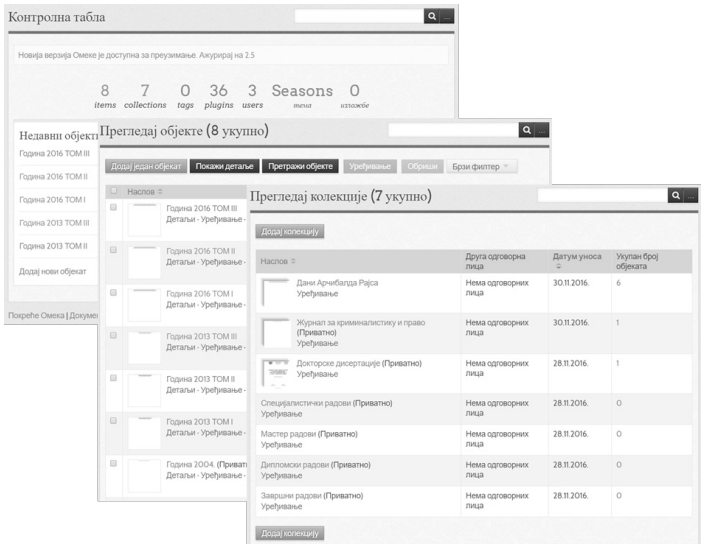



*Figure 1.Control panel, on which administrator regulates the Digital Library*

## FORENSIC LINGUISTICS

The linguistic study of forensic texts is a part of the field of Natural Language Processing, which includes text type classification and syntax and semantic analysis of texts written in a natural language. Various texts are subject of the study: Acts of Parliament (or other law-making body), private wills, court judgements and summonses and the statutes of the bodies such as States and government departments, cross-examination, evidence presentation, judge's decisions, police cautions, police testimonies in court, summing up to a jury, interview techniques, the questioning process in court and police interviews, etc. Generally speaking, any text or item of spoken language can potentially be a forensic text when it is used in a legal or criminal context.[4]

An important part of the forensic texts study is threat communication. Threat is an important feature in a ransom demand. Ransom demands are examined to identify between genuine and false threats. An example of the ransom note analysis is the case of the Lindbergh kidnapping. From the first sentence, the kidnapper makes the claim that the child is in good hands, but to make such a claim, the note would have to be written before the perpetrator enters the premises. Therefore, the claim is false (at the time of writing) since the kidnapper had not even encountered the child when he wrote the note.[5] Kidnappers may write statements that later end up being true, such as "your child is being held in a private location" being written ahead of time.

Here are some facts about suicide letters: a suicide note is typically brief, concise and highly propositional with a degree of evasiveness. A credible suicide letter must make a definite unequivocal proposition in a situational context. The proposition of genuine suicide is

4 John Olsson (2008). Forensic Linguistics, Second Edition. London: Continuum ISBN 978-0-8264-6109-4
5 Falzini, Mark W. (9 September 2008). "The Ransom Notes: An Analysis of Their Content & "Signature""

thematic, directed to the addressee (or addressees) and relevant to the relationship between them. Suicide notes generally have sentences alluding to the act of killing oneself, or the method of suicide that was undertaken.[6] The contents of a suicide note could be intended to make the addressee suffer or to feel guilt. Genuine suicide letters are short, typically less than 300 words in length. Extraneous or irrelevant material is often excluded from the text.

The next forensic text type is death row statements. They either admit the crime, leaving the witness with an impression of honesty and forthrightness, or deny the crime, leaving the witness with an impression of innocence. They may also denounce witnesses as dishonest, critique law enforcement as corrupt to portray innocence or seek an element of revenge in their last moments. Death row statements are within the heavily institutionalized setting of death row prisons. The Forensic Linguistics Institute holds a corpus of these documents and is conducting research on them. And the last but not the least important is social media. Social media statements are often context specific, and their interpretation can be highly subjective. Forensic application of a selection of stylistic and stylometric techniques in a simulated authorship attribution case involving texts has been done in relation to Facebook.[7] Analysis of social media postings can reveal whether they are illegal (e.g. sexist) or unethical (e.g. intended to harm) or whether they are not (e.g. simply provocative).[8]

## SOFTWARE SOLUTIONS MODEL

The human language processing group (HLT group) at the University of Belgrade is engaged in a task of producing various language resources,[9] both corpora and lexiconsfor many years now. Given the fact that these resources have been developed for many years, they have been conceived within different frameworksand the technological point of view. Although the HLT group made every reasonable effort to keep the resources as coherent and as standardized as possible, a certain level of heterogeneity was inevitable. Hence, due to the growth of the volume of resources as well as their different usage, there was a need for developing a setof tools that would facilitate the maintenance and exploitation in different domains and scenarios. Embarking on this task, the HLT group has produced a workstation for language resources, labelled LeXimir and set of web services Vebran, which greatly enhances the potentials of manipulating each particular resource as well as several resources simultaneously.[10]

To keep development and use of the applications and resources at the same time without frequent conversions, the strategy for the development was to support original formats used in another software tools for language resourcesprocessing (Unitex, WorNet, LeXimir, Vebran). Another important decision was totry re-using the available software, avoid devel-

6 John Olsson (2004). An Introduction to Language Crime and the Law. London: Continuum International Publishing Group

7 C.S. Michell (2013). Investigating the use of forensic stylistic and stylometric techniques in the analysis of authorship on a publicly accessible social networking site (Facebook) (MA in Linguistics thesis). University of South Africa

8 C. Hardaker (2015). The ethics of online aggression: Where does "virtual" end, and "reality" begin? BAAL Conference on the Ethics of Online Research Methods. Cardiff

9 CvetanaKrstev, Duško Vitas, "Corpus and Lexicon - Mutual Incompleteness", in Proceedings of the Corpus Linguistics Conference, 14-17 July 2005, Birmingham, eds. PernillaDanielsson and MartijnWagenmakers, ISSN 1747-9398, http://www.corpus.bham.ac.uk/PCLC/, 2005

10 Cvetana Krstev, Ranka Stanković, Duško Vitas, Ivan Obradović, "The Usage of Various Lexical Resources and Tools to Improve the Performance of Web Search Engines", in Proceedings of the Sixth Interantional Conference on Language Resources and Evaluation (LREC'08), Marrakech, Morocco, 28-30 May 2008, European Language Resources Association (ELRA), 2008

opingthe existing functions, butfocus on the necessary functions that did not exist and then integrate them with other tools.

There are diverse ways to integrate the existing and new systems into a hybrid tool. Every method has good and bad characteristics and because of that it cannot be used in every situation. Problemsexist and the best way to solve them is to use different methods. The motivation for creating hybrid systems can be to improve methods, to solve problem complexity with multiple tasks and resolve multifunctionality. Improving the method can be achieved by integrating different methods to overcome specific limitations and disadvantages, combining the method with poor specifications with another method with different specifications.For problems with multiple tasks, or subtasks, which cannot be solved with one method, hybrid systems are being created to solve all subtasks with appropriate method.Realisation of multifunctionality is motivated by the need to create hybrid systems within a single architecture for solving problems in different ways. These systems functionally emulate a variety of methods.

The RESTfull Web services based on Unitex routines are used for the implementation of morphological analysis and output generation relying onelectronic dictionaries. For queryexpansion morphological and semantic vocabulariesare combined, because synonymous terms are taken from WordNet[11] and terminological databases. The hybrid search engine has replaced the system that supports only simple,keyword based queries, with the morphologically and semantically expandedquery.

## METADATA

The metadata area core for the development of digital libraries, as the structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use or managean information resource. These data are the key to ensure that resources will be secured and to continue to be accessible in future. Metadata is often called data about data or information about information.[12] There are several different types of metadata: descriptive – that describe a resource purpose, such as discovery and identification of objects that includes basic elements: title, author, publisher, location, date, language, a unique identifier, description, keywords, subject headings, abstract, etc.; structural – describe types, versions and links between digital objects (e.g. connect the original document and all its versions, whereby include information about versions and the information about the latest change in them, etc.); administrative – contain information on the rights of access to the digital object in accordance with copyright and intellectual property protection, the source, size and type of files on access to the source, the size and display format, and using them to actively monitor the number of users who visit and use certain content.[13] Web platform Omeka uses Dublin Core as a standard for displaying metadata. The Dublin Core includes a set of elements to describe a wide range of sources in the network and aims to: simplicity in the creation and maintenance so that each user could make a set of descriptive statements understandable semantics to facilitate searches across the global network to all who are in need of information; localization: originally implemented in English, but there are versions that are written for many other languages (Serbian, Russian,

11 Miljana Mladenović, Jelena Mitrović, Cvetana Krstev, "Developing and Maintaining a WordNet: Procedures and Tools", In The Proceedings of Seventh Global WordNet Conference 2014, eds. Heili Orav, Christiane Fellbaume, Piek Vossan, University of Tartu, Tartu, Estonia, January 25-29, 2014, pp. 55-62, 2014, ISBN 978–9949–32–492–7

12 HODGE, G., 2001. Metadata made simpler, Niso Press

13 TRTOVAC, A. S., 2016. Deskriptori metapodataka i sadržaja u pronalaženju informacija u digitalnim bibliotekama. Univerzitet u Beogradu-Filološki fakultet.

Chinese, Finnish, Norwegian, Japanese, etc.).[14]Dublin Core consists of 15 basic elements: title, subject, description, type, source, relation, coverage, creator, publisher, contributor, rights, date, format, identifier and language. Most often these elements are sufficient to describe the digital object.Web platform Omeka has an extension (or plugin) Dublin Core Extended, that represents the extended list of the basic set of elements. It includes the following elements: Abstract, Access Rights, Accrual Method, Accrual Periodicity, Accrual Policy, Alternative Title, Audience, Date Available, Bibliographic Citation, Conforms To, Date Created, Date Accepted, Date Copyrighted, Date Submitted, Audience Education Level, Extent, Has Format, Has Part, Has Version, Instructional Method, Is Format Of, Is Part Of, Is Referenced By, Is Replaced By, Is Required By, Date Issued, Is Version Of, License, Mediator, Medium, Date Modified, Provenance, References, Replaces, Requires, Rights Holder, Spatial Coverage, Table Of Contents, Temporal Coverage, Date Valid, DC-RDFoutput format.

## USE CASE DIAGRAM

Use case diagram on the left describessearch possibilitiesoffered to the user together with different responsibilities for lexicographer, terminologist and for linguists. Terminologist is generally using search on lemma and synonyms, while linguist is more interested in search by linguistic patterns and syntactic graphs. Figure 2 on the right shows a diagram of a use case forcorpus preparation that includes: collection of articles, lexical processing resources, describing text with metadata, analysis of unknown words, complement morphological dictionaries, addition to terminology database, transliteration, correction of broken words, correction of optical character recognition errors.

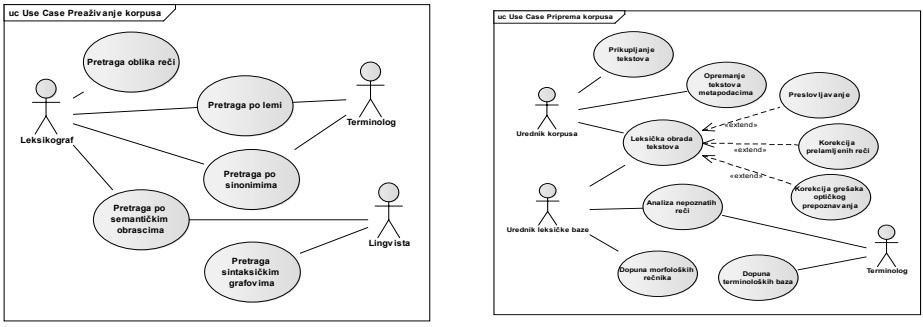



*Figure 2. Use case diagrams: exploitation (left), preparation (right)*

## APPLICATIONS FORLINGUISTIC RESOURCES

The linguistics and lexical resources used for query expansion and text analysis are depicted in Figure 3 on the left, while on the rightthere are main application components of the language support system. Main lexical resources include morphological dictionaries for Serbian language,[15] Serbian and English WordNets, terminological databases: Termi, GeolISSTerm, RudOnto and Librarian dictionary. Apart from the grammars in the form finite state autom-

14 MILENKOVIĆ, M., 2003. Dublin Core Metadata Initiative (DCMI). Review of the National Center for Digitization, 70-79

15 Cvetana Krstev. Processing of Serbian – Automata, Text and Electronic Dictionaries, Faculty of philology, Belgrade, 2008

ata and transducers, the system is using rules for inflection of multiword units. Digital librariesUnitex corpora[16] and CQP web corpora are the most importantamong textual resources. Linguistic support is implemented via REST web service Vebran that interacts from one side with lexical and linguistic resources and from the other with Omeka KPA digital library.

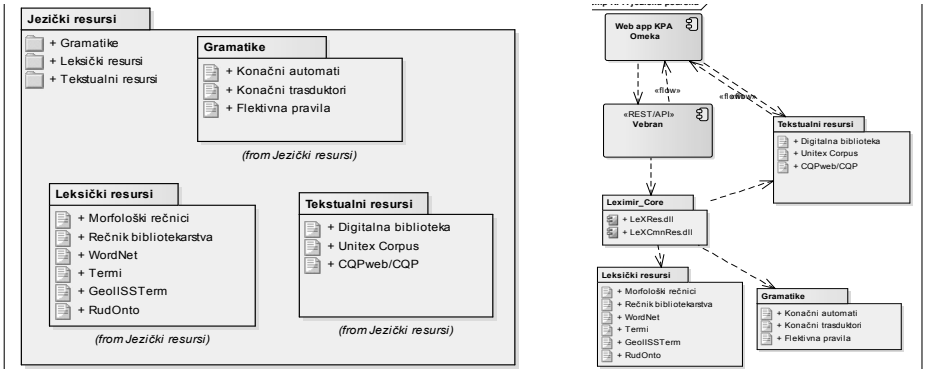



*Figure 3. Linguistic resources applications*

## DYNAMIC MODEL QUERY EXPANSIONS

The dynamic aspect of the application is presented in the interaction diagram with a model of query expansionshowing messages sent between objects or class instances as a series of sequential steps over time. They are used to describe the workflow, message transmission and different elements cooperation of the system to achieve a result. Figure 3 shows the interaction of the user and system components in case of semantic query expansion,[17] which mayinclude morphological expansion. The class *WNManager* for the WordNet resources management provides a semanticexpansion of a query that includes introducing literals from the selected synsets. Expansion with additional relations (hyponymy-hypernym) introduces also literals from the synsets which are connected by the relation of hypernym. Multilingual expansion is implemented using two wordnets and their inter-lingual index. The method differs from the previous only in the possibility of extending the query literals in the other language which can be reached via a synchronized synsets.

16 Duško Vitas, Cvetana Krstev, Ivan Obradović, Ljubomir Popović, Gordana Pavlović-Lažetić", An Processing Serbian Written Texts: An Overview of Resources and Basic Tools ", in Workshop on Balkan Language Resources and Tools, 21 Novembar 2003, Thessaloniki, Greece, eds, S. Piperidis and V. Karkaletsis, pp. 97-104, 2003

17 Cvetana Krstev, Ranka Stanković, Duško Vitas, Ivan Obradović, "The Usage of Various Lexical Resources and Tools to Improve the Performance of Web Search Engines", in Proceedings of the Sixth Interantional Conference on Language Resources and Evaluation (LREC'08), Marrakech, Morocco, 28-30 May 2008, European Language Resources Association (ELRA), 2008

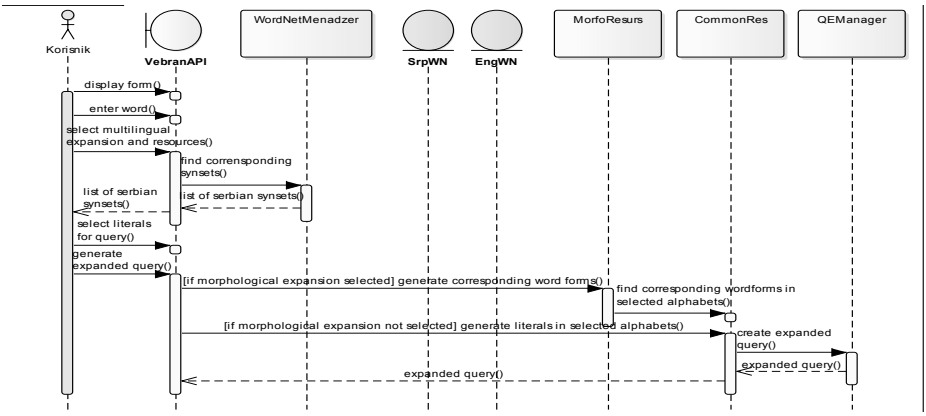



*Figure 4. Sequence diagram of a multilingual query expansions*

The search option is on the operator page. There are two ways of search, Narrowed search that includes the search on specified fields, collections and kinds, user who added a resource and the geographic address. This search method searches only on the basis of the given word, without changing the form of words. Extended search includes morphological and semantic search. Morphological search includes search of all inflected forms of specified word that are retrieved from SrpMD (Serbian morphological dictionary). For nouns, grammatical forms include case andnumber for example for *kuća* (Eng.*house*)*kuće, kućama, kući,*etc. for adjective additionally comparison, for verbs person, times,etc. Semantic search involves the expansion of the query by searching semantic network Serbian WordNet.[18] This semantic network is based on the concepts among which there are semantic relations. With the simplesearch with keyword *napad*(Eng.*attack*), the system will findonly exact matchof the word *napad*, while with the extended search for the same word the system will search also for the words: *agresija, agresijama, agresije, …, akcija, akcijama, akcije,…, inicijativa, inicijativama, inicijative, …, napad, napada, napade, …, nasrtaj, nasrtaja, nasrtaje,…, , navala, navalama, navale, …, агресија, агресијама, агресије, …, акција, акцијама, акције, …, иницијатива, иницијативама, иницијативе, … , напад, напада, нападе,…, насртај, насртаја, насртаје,…, навала, навалама, навале, …,* that means all synonyms, both alphabets (Cyrillic and Latin) and all inflected forms.

If we want to focus on word *napad* only, but analyse different contexts of occurrences, more sophisticated query can be requested. Simple query that extracts all inflected forms of lemma "napad" (eng.*attack*) would be written in angular brackets "<" and ">" e.g. <*napad*>. Another possibility is to use a part of speech marker to retrieve any word in inflected form for specified part of speech. For example, template <N> would match all nouns, while <N+Hum> would match all nouns related to human beings. Also, it is possible to concatenate query expressions to retrieve more complex patterns.The following expression: <*A*><*napad*><*PREP*><*N+Hum*>is an example of morphological and semantic expression search in-Unitex system. This query is retrieving any inflective form of lemma *napad* (*attack*), preceded by an adjective (<A>) and followed by a preposition and a noun (<N>) that is human (depicted by the semantic mark +Hum), retrieving output concordances like:

18 I. Obradović, R. Stanković, "Wordnet Development Using a Multifunctional Tool". Proceedings of the International Workshop Computer Aided Language Processing (CALP) '2007, Borovets, Bulgaria, C. Orasan, S. Kuebler (eds.), pp. 25-32, September 2007.

| |
|---|
| se označavamestonakome se javljaju čestinapadinažrtve škole, kada je pitanjuimovinski |
| išljajno ubistvo, kidnapovanje ili neki drugi napad na lica ili slobodu međunarodno zaštićenog |
| samo kada je to neophodno da se spreči fizički napad na službeno lice, drugog maloletnika ili |
| me, posle ukazivanja na podatke o broju fizičkih napada na policajce u SAD-u u razdoblju −. go |
| unima sa navijačima protivničkih ekipa; fizičkim napadima na građane, igrače, službena lica i p |
| oružja i pretnjom njegove upotrebe ili fizičkim napadom na žrtvu. Od oružja se najčešće kor |
| svaki oblik fizičkog zlostavljanja ili fizičkog napada na dijete kojim se izaziva ili se može |
| eno krivično delo iz člana a KZRS, zbog fizičkog napada na sudiju udaranjem pesnicom ruke u pre |
| i zovu se krivična dela.{S} Mnogi napadi na pojedinca predstavljali su krivično del |
| pomenuto, očekivan od ljudi osuđenih za najteže napade na pripadnike organa reda, Ali, s dr |
| ikom pokušaja krivičnog dela, dolazi do neposrednog napada od strane učinioca na društvene odno |
| nu ili kolektivnu samoodbranu u slučaju oružanog napada protiv člana Ujedinjenih nacija, dok Sa |
| iz tri naša kaznena zavoda.{S} Rizik ponovljenog napada na pripadnike policije Sa puno osnov |
| dgovor na pitanja prvo: da li se radi o ponovljenom napadu na službena lica, u drugom slučaju d |
| UMESTO ZAKLjUČKA Mali broj istraživanja posvećenih napadima na policajce uslovio je potrebu da |
| jive maštovitosti, teorija koja podvodi preventivni napad na suverenu državu pod izgovorom tero |
| ativne baze za izvršavanje sistematskih razbojničkih napada na putnike i trgovce. (T. Taranovsk |
| rorizma koji se sastoji u samoubilačkim terorističkim napadima na ljude i imovinu, svesnim žrt |
| rezultata kriminološkog istraživanja o teškim napadima na policajce u Srbiji koje je sproveden |
| odologija kriminološkog istraživanja o teškim napadima na policajce u Srbiji, koje je sproved |
| anja poslova, smatramo da ubuduće svaki teži napada na službena lica zahteva potpunu analizu ko |
| adicijom, data dva ilustrativna primera ubilačkih napada na policajce, koji mogu poslužiti kao |
| Kada se radi o dobu dana, sve podatke o vremenu napada na policajce podelili smo u vremenske p |

The Serbian morphological dictionaries cover large lexica, but each special domain has characteristic words that occur in ordinary textsoccasionally, but frequently in domain specific texts. That is the case with presented collection. Among unrecognized tokens were the following terms:

*psihoaktivni, podstrekavati, situacijski, narkokartel, kriminalnopolitički, izvršilaštvo, zakonopisac, procesnopravni, geoprostorni, protiv vazduhoplovni, delikvencija,…* (Eng. *psychoactive, incite, site, cartel, criminal and political, complicity, legislator, procedural, geospatial, antiaircraft, delinquency,…*).

These words are examples of word candidates for enrichment of morphological dictionary.Their addition will enhance the search performance and criminalistics text analysis.In this research, the analysis included extraction of multi-word units using LeXimir[19]that system retrieved as most frequent:

*nasilje u porodici žurnal za kriminalistiku*, *izvršenje krivičnog dela*, *policijski službenik*, *policijska akademija*, *pravno lice*, *ljudsko pravo*, *pranje novca*, *radnja izvršenja, država članica, trgovina ljudima,* (Eng. *domestic violence, journal of criminology, committing an offense, police officer, police academy, legal person, human right, money laundering, action execution, member states, trafficking*).

## SENTIMENT ANALYSIS AS THE NEXT STEP IN A STUDY OF FORENSIC TEXTS

The semantic network Serbian WordNet(SWN) is a lexico-semantic resource that has been developed based on the idea of the Princeton WordNet (PWN), a mental lexicon that helps

19 Ranka Stanković, Cvetana Krstev, Ivan Obradović, Biljana Lazić, and Aleksandra Trtovac, "Rule-based Automatic Multi-word Term Extraction and Lemmatization", Proceedings of the 10th International Conference on Language Resources and Evaluation, LREC 2016, Portorož, Slovenia, 23--28 May 2016, 2016, eds. Nicoletta Calzolari et al., ISBN 978-2-9517408-9-1

scientists working on psycholinguistic projects. SWN is a set of more than 22.000 concepts called synsets, where a concept is represented by the set of synonym word forms that have the same or similar meaning. Synsets respect the syntactic categories such as noun, verb, adjective, and adverb and can be interconnected by semantic relations, and word forms by lexical relations.Synonymy is WordNet's basic relation, because WordNet uses sets of synonyms (word forms with similar meaning) to represent a concept. Antonymy (opposing-name) is a symmetric relation between two word forms with opposite meaning. Hyponymy (sub-name) and its inverse, hypernymy (super-name), are transitive relations between synsets and they organize the meanings of concepts into a hierarchical structure. Meronymy (part-name) and its inverse, holonymy (whole-name) distinguish component parts. Troponymy (manner-name) is for verbs what hyponymy is for nouns.For the purpose of enriching SWN with the data concerning sentiment measurement, SentiWordNet, a lexical resource for opinion mining based on the Princeton WordNet, is used.[20] It assigns three sentiment scores: positivity, negativity and objectivity to each PWN synset, but in SWN two SentiWordNet sentiment scores (positive and negative) are used for each SWN synset. A sentiment lexicon is produced using word forms defined in SWN that have positive or negative sentiment scores. This kind of lexicon is applied in sentiment polarity classification tasks on Serbian texts, achieving 97.1% accuracy over cross-validated datasets and 84.9% and 79,1% over different test datasets.[21] In that terms, SWN can be used in query expansion to give semantic meaning to terms that are looked for. For example, in Figure 5 it is shown that SWN synsets defining notions "*terorističkinapad*"(*terrorist attack*) and "*upad*" (*intrusion*) have negative sentiment polarity scores (0.75 and 0.125) respectively, which makes possible to classify the texts containing these terms as "forensic texts".

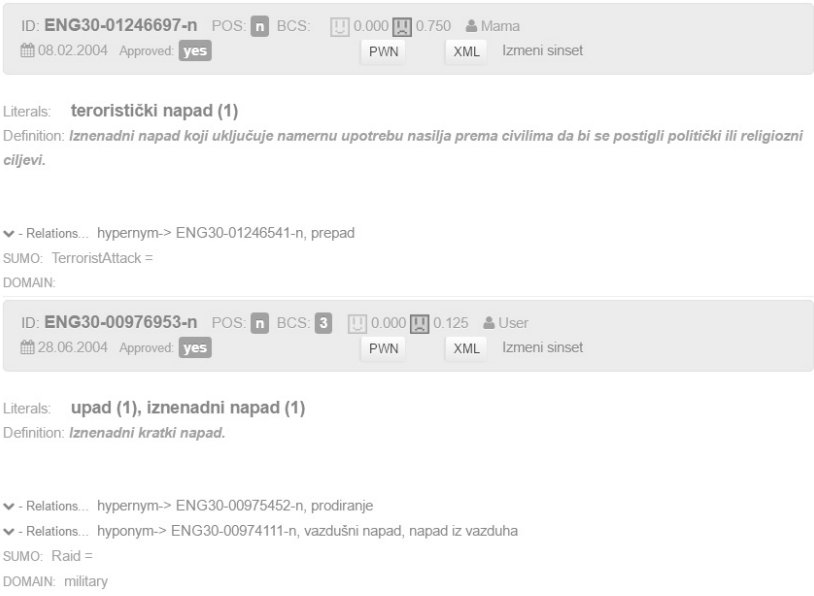



*Figure 5. WordNer interface*

20 Mladenović, M., & Mitrović, J. (2014). Semantic Networks for Serbian: New Functionalities of Developing and Maintaining a WordNet Tool. In G. Pavlović Lažetić, C. Krstev, I. Obradović & D. Vitas Natural Language Processing for Serbian – Resources and Application, 1-11. Matematički fakultet, Beograd.
21 Mladenović, M., Mitrović, J., Krstev, C., & Vitas, D. (2015). Hybrid Sentiment Analysis Framework For A Morphologically Rich Language. Journal of Intelligent Information Systems, Volume 46, Issue 3, pp 599–620

## CONCLUSION

The paper presented the digital library from criminalistics domain available at http://master-kpa.rgf.rs/, as a documentcollection organised in several categories: Journal of Criminalistics and Law, Archibald Reiss, Doctoral Dissertation, and other (final process). Various methods for improvement of keyword based simple search is demonstrated on the texts prepared for text analysis and terminology extraction. Implementation details of Omeka, including add-in customisation, integration with Vebran, LeXimir and Unitex is discussed and presented in a few examples. Having in mind that the metadata are a core for the development of digital libraries, that explains, locates, or otherwise makes it easier to retrieve, to use or to manage an information resource, metadata classification and management of metadata is elaborated. The paper concludes with Sentiment Analysis as the next step in a study of forensic texts.

## REFERENCES

1. Falzini, M W. "The Ransom Notes: An Analysis of Their Content & "Signature""
2. Hardaker, C. The ethics of online aggression: Where does "virtual" end, and "reality" begin? BAAL Conference on The Ethics of Online Research Methods. Cardiff, 2015
3. HODGE, G., 2001. Metadata made simpler, Niso Press, 2008.
4. Krstev, C. Processing of Serbian – Automata, Text and Electronic Dictionaries, Faculty of philology, Belgrade, 2008.
5. Krstev, C., Stanković, R., Vitas, D., Obradović, I. "The Usage of Various Lexical Resources and Tools to Improve the Performance of Web Search Engines", in Proceedings of the Sixth International Conference on Language Resources and Evaluation (LREC'08), Marrakech, Morocco, 28-30 May 2008, European Language Resources Association (ELRA), 2008
6. Krstev, C., Vitas D. "Corpus and Lexicon - Mutual Incompleteness", in Proceedings of the Corpus Linguistics Conference, 14-17 July 2005, Birmingham, eds. PernillaDanielsson and MartijnWagenmakers, ISSN 1747-9398, http://www.corpus.bham.ac.uk/PCLC/, 2005.
7. Michell, C.S. Investigating the use of forensic stylistic and stylometric techniques in the analysis of authorship on a publicly accessible social networking site (Facebook) (MA in Linguistics thesis). University of South Africa, 2013
8. Milenković, M. Dublin Core Metadata Initiative (DCMI). Review of the National Center for Digitization, 70-79. 2008
9. Mladenović, M., Mitrović, J. Semantic Networks for Serbian: New Functionalities of Developing and Maintaining a WordNet Tool. In G. PavlovićLažetić, C. Krstev, I. Obradović& D. Vitas Natural Language Processing for Serbian – Resources and Application, 1-11. Matematičkifakultet, Beograd. 2014
10. Mladenović, M.,Mitrović, J.,Krstev, C. "Developing and Maintaining a WordNet: Procedures and Tools", In The Proceedings of Seventh Global WordNet Conference 2014, eds. HeiliOrav, Christiane Fellbaume, PiekVossan, University of Tartu, Tartu, Estonia, January 25-29, 2014, pp. 55-62, 2014, ISBN 978–9949–32–492–7, 2014
11. Mladenović, M., Mitrović, J., Krstev, C., Vitas, D. Hybrid Sentiment Analysis Framework For A Morphologically Rich Language. Journal of Intelligent Information Systems, Volume 46, Issue 3, pp 599–620, 2015

12. Obradović, I.,Stanković,R. "Wordnet Development Using a Multifunctional Tool". Proceedings of the International Workshop Computer Aided Language Processing (CALP) '2007, Borovets, Bulgaria, C. Orasan, S. Kuebler (eds.), pp. 25-32, September 2007.
13. Olsson, J. An Introduction to Language Crime and the Law. London: Continuum International Publishing Group, 2004
14. Olsson, J. Forensic Linguistics, Second Edition. London: Continuum ISBN 978-0-8264-6109-4
15. Stanković, R.,Krstev, C.,Obradović, I.,Lazić, B., Trtovac, A. "Rule-based Automatic Multiword Term Extraction and Lemmatization", Proceedings of the 10th International Conference on Language Resources and Evaluation, LREC 2016, Portorož, Slovenia, 23--28 May 2016, eds. Nicoletta Calzolari et al., ISBN 978-2-9517408-9-1, 2014
16. Stanković, R.,Krstev, C.,Obradović, I.,Lazić, B., Trtovac, A. "Rule-based Automatic Multiword Term Extraction and Lemmatization", Proceedings of the 10th International Conference on Language Resources and Evaluation, LREC 2016, Portorož, Slovenia, 23--28 May 2016, eds. Nicoletta Calzolari et al., ISBN 978-2-9517408-9-1, 2016
17. Trtovac, A.Deskriptorimetapodatakaisadržaja u pronalaženjuinformacija u digitalnimbibliotekama, PhD Thesis. Univerzitet u Beogradu-Filološkifakultet, 2016
18. Vitas, D.,Krstev, C.,Obradović, I., Popović, Lj., Pavlović-Lažetić, G."An Processing Serbian Written Texts: An Overview of Resources and Basic Tools ", in Workshop on Balkan Language Resources and Tools, 21 Novembar 2003, Thessaloniki, Greece, eds, S. Piperidis and V. Karkaletsis, pp. 97-104, 2003.
19. https://omeka.org/
20. https://www.gnu.org/licenses/gpl-3.0.en.html

# THEORETICAL RESEARCH OF INFORMATION AND ITS PROPERTIES IN THE EXERCISE OF INFORMATION AND ANALYTICAL WORK

**Lepiokhin Alexander**,
PhD in law, Head of law informatics department of the
Academy of the Ministry of Interior of the Republic of Belarus
Academy of the Ministry of Interior of the Republic of Belarus,
prav_informatika@mail.ru

**Abstract:** This article is a summary of the provisions on the problem of "information" as a category, starting with the works of ancient Greek philosophers, the works of thinkers of the Middle Ages and modern times. The author has considered certain provisions of the founders of the information theory and cybernetics. A categorical approach was proposed to the definition of 'information' in relation to the information-analytical work. An analysis of the subject area of this category has reviewed 'information' through a system of its properties.

**Keywords:** information and analytical work, information, properties of the information, theory of information, cybernetics.

## INTRODUCTION

The development of society at the present stage, and especially in its last decade, is characterized by rapid development and widespread use of information technology, and therefore, there are serious changes in the structure and social relations in society, the geopolitical system of the world, the economy, methods and ways of governance, gradually, a new socio-psychological aspect of man, for which information is one of the core values and needs for existence. In this regard, consideration of different approaches to the 'information' category in the context of the implementation of its content characteristics in the information-analytical work of law enforcement appears a promising area of scientific research.

The category of 'information' can be used in different contexts - scientific, philosophical (among other categories) and ordinary. It is obvious that in view of the considered problem it is interesting to research this category from scientific positions, as well as both qualitative and quantitative characteristics of information. The notion of 'information' has a Latin linguistic roots (*informatio* - clarification statement) and semantically refers to measure the distribution of matter and energy in space and time, a measure of the changes that accompany all the processes occurring in the world.[1]

1 A modern dictionary of foreign words. - Moscow: "The Russian Language", 2001. – 763 p.; The term "information"/Material from the free encyclopedia Wikipedia [Electronic resource]. - Access mode: https://en.wikipedia.org/wiki/Information - Access date: 15/02/2017.

## HISTORICAL OVERVIEW OF THE CATEGORY

Despite a long history of the category of 'information', which starts in the papers of ancient philosophers (Plato - the use of the term 'cybernetics' as management in a general sense, Aristotle – doctrine of the logic, Pythagoras - the foundations of mathematics and geometry, Democritus - the doctrine of atoms and the mathematical researches, and other ancient researchers as well (see for more detail[2]) significant paying attention to this category was in the works of medieval philosophers (Peter Abelard, John Duns Scotus, Raymund Lull – the representatives of scholasticism, etc.), Renaissance (Giordano Bruno, Jean Bodin, Galileo Galilei, Michel de Montaigne, etc.) and Modern Times (Pascal Francis Bacon, Thomas Hobbes, René Descartes, and others),[3] but until the mid-20th century the category of 'information' was the ordinary meaning and is synonymous with the concepts of 'message' or 'data'.

Active development of technologies and technical means of information processing and the generation of cybernetic science predetermined the formation of new scientific trends and theories of studying this category, which ultimately led to the emergence of the 'information theory' as a section of applied mathematics that studies information, its properties and data transmission systems. Claude Shannon's work "Mathematical Theory of Communication",[4] which contains ideas related to the limits of possibilities of data transmission systems, is considered to be the classical beginning of the study of this concept (as a mathematical category), since it is believed that the emergence of information theory is conditioned by the need for another theory - the theory of communication. The development of scientific search and comprehension of this category was received in the works of the founder of cybernetics Norbert Wiener "Cybernetics and Society" and "Cybernetics, or control and communication in the animal and machine",[5] in which one of the first definitions of 'information' was formulated in the context of cyber science. "Information is the designation of the content obtained from the outside world in the process of our adaptation to it and the adaptation of our feelings to it".[6]

From the epistemological positions of the theory of management, the definition of information through its content in the context of information-analytical work is filled with a certain meaning, since this activity is not only informational in nature but is concretized in the analysis of the content of the received information signals. Accordingly, the provisions formulated by N. Viner in the part of the disclosure of the category 'information' have an important methodological significance for the formation of the theory of information and analytical support of administrative activity, conditioned by the hermeneutic nature of the sphere in question. Moreover, these approaches will allow us to define the properties and formulate the requirements for information as a central category of information and analytical activity.

It should be noted that the research and use of the concept of 'information' is characteristic of many branches of science – mathematics, computer science, cybernetics, jurisprudence, medicine and other spheres of scientific knowledge. Questions of nature and material foundations of information among the domestic (in the sense of the states of the post-Soviet space) scientists were raised in the works of A. Ursul "Nature of Information", "Reflection and Infor-

2 Ancient philosophy: Encyclopedic dictionary. - M., 2008. – 896 p.
3 Gritsanov, A. The Newest Philosophical Dictionary. - Minsk: Skakun, 1999. - 896 p.; Gubsky, E., Korableva, G., Lutchenko, V. Philosophical Encyclopedic Dictionary. - Moscow: Infra-M, 2005. - 576 p.
4 Shannon, K. Works on information theory and cybernetics. - Moscow: IL, 1963. - 830 p., Pp. 243-322.
5 Winner, N. Cybernetics or control and communication in an animal and a machine. - Moscow: Soviet radio, 1968. - 325 p.
6 Winner, N. Cybernetics and Society. Moscow: Izd-vo inostr. Lit-ry. Moscow, 1958 [Electronic resource]. - Access mode: http://filosof.historic.ru/books/item/f00/s00/z0000816/st000.shtml - Date of access: 01/02/2017.

mation".[7] In these works, the problems of information were raised, as forms of the existence of matter, like mass and energy, as well as its reflection as properties of matter.

The analysis showed that the basis for such a study is in the cybernetic processes of interaction of the mapping objects. And, as rightly noted by A. Ursul: "In the concept of interaction, it is already stated not simply that all objects are changing, but that one object changes precisely because another object acts on it, and this latter in turn changes under the influence of the first".[8] Accordingly, this message allows naturally to raise questions about the nature and essence of information in the context of carrying out information and analytical work (IAW), the properties (information) of interacting objects, the mechanism and amount of information displayed, whether the display contains information for the conduct of IAW and a number of others. Essential and categorical questions of information were also raised in the works of Soviet academician V. Glushkov,[9] in which he pointed out that "information exists, because there are material bodies and heterogeneities created by them". Disclosing the definition of the category 'information' V. Glushkov noted that "on the one hand, information is a collection of possible information that circulates in the country and in society, including in the technical systems created by man. On the other hand, he considered information as "a measure of heterogeneity in the distribution of energy or matter in space and time".[10]

In general, it should be noted that in the works of cybernetics scientists of the Soviet period (A. Lyapunov, A. Berg, V. Moiseev and others), there was a desire to disclose not only the quantitative and statistical side of information, but its semantic aspect, epistemological nature and its content. Since the solution of management tasks, and especially in the social environment, this involves studying the qualitative characteristics and properties of information, and in the future its quantitative evaluation (i.e. if we briefly conclude - the numerical characteristics of the phenomenon are important for analysis and prediction, but the primary task is to identify this learning parameters).

The modern stage of studying the category 'information' is characterized, on the one hand, by the emergence and consolidation of the normative definition in the relevant laws,[11] and on the other - active study of this concept in relation to various branches of scientific knowledge. Thus, according to the Law of the Republic of Belarus[12] information is understood as data about persons, objects, facts, events, phenomena and processes, regardless of the form of their

7 Ursul, A.D. Reflection and information. M. 1973 [Electronic resource]. - Access mode: http://informaticslib.ru/books/item/f00/s00/z0000007/ /st001.shtml - Date of access: 05.02.2017; Ursul, A.D. Nature of information: philosophical essay / AD Ursul; Chelyab. State. Acad. Culture and arts; Scientific and educational. Center "Information Society"; Ros. State. Trade and economy. Un-t; Center issled. Glob. Processes and sustainable development. - 2 nd ed. - Chelyabinsk, 2010. - 231 p.

8 Ursul, A.D. Reflection and information. M. 1973 [Electronic resource]. - Access mode: http://informaticslib.ru/books/item/f00/s00/z0000007/ /st001.shtml - Date of access: 05.02.2017

9 Glushkov, V.M. Fundamentals of paperless computer science. - Moscow: Science. -1982. - 552 p.; Glushkov, V.M. Introduction to cybernetics. - Kiev: Publishing House of the Academy of Sciences of the Ukrainian SSR, 1964 – 342 p.; Kapitonova, Yu.V., Letichevsky, A.A. Paradigms and ideas of academician VM Glushkov. - Kiev: Naukova Dumka, 2003. - 456 p.

10 Glushkov, V.M. Introduction to cybernetics. - Kiev: Publishing House of the Academy of Sciences of the Ukrainian SSR, 1964 – 342 p

11 Information, information and information protection [Electronic resource]: Law of the Republic of Belarus No. 455-3 of 10.11.2008 (as amended on 04.01.2014) / access from the legal system "ConsultantPlus". - Date of access: 02/02/2017; About information, information technologies and information protection [Electronic resource]: Federal Law No. 149-FZ of July 27, 2006 (as amended on July 13, 2015) / access from the legal system "Consultant Plus". - Date of access: 02/02/2017.

12 Information, information and information protection [Electronic resource]: Law of the Republic of Belarus No. 455-3 of 10.11.2008 (as amended on 04.01.2014) / access from the legal system "ConsultantPlus". - Date of access: 02/02/2017

presentation. A similar definition is contained in Russian legislation,[13] according to which information is understood as information (messages, data) regardless of the form of their presentation. Obviously, these definitions have a fairly general meaning, but, on the whole, reflect the semantic nature of information, defining it through a legal construction: "information is data about ...".

Without going into serious discussion about the definition of the category 'information' at the present stage, since not the definition itself is the subject of this study, but it is of definite scientific and practical interest to reveal the properties of information and its functional purpose in relation to information and analytical work. In this connection, let us formulate the following definition: information is data about qualitative and quantitative characteristics of an object (phenomenon, event, process). It should be noted that we deliberately pointed to such a category as data obtained as a result of the use of computer-readable (computer) data in the analysis of objects, phenomena, events, processes. At the same time, we do not identify them (information and data), given their different nature.

## PROPERTY OF INFORMATION

Having defined the concept of 'information', we will concentrate our attention on revealing the properties of information (its qualitative and quantitative characteristics) that are of significant importance in carrying out information and analytical work. It should be noted that some properties are fixed in the above laws "On Information ...", in which some properties are indicated directly corresponding to the article that discloses the basic concepts of the law – "confidentiality of information – a requirement that a person who has access to certain information do not transmit such information to third parties without the consent of its owner". Such properties of information as the reliability of information and the timeliness of its provision are determined by the Russian legislator as the principles of information. And speaking about the security of information as one of its properties, in the relevant law there is a separate article defining the goals, content, responsibilities and requirements for information protection.[14]

In the Belarusian law regulating the relevant legal relations, the following information properties are defined as: "access to information - the possibility of obtaining information and using it", "information protection - a set of legal, organizational and technical measures aimed at ensuring confidentiality, integrity, authenticity, accessibility and safety of information". In this definition, we focus on the direction of measures to protect information to ensure its properties – confidentiality, integrity, authenticity, accessibility and security. At the same time, in the law under consideration only the first of the given properties of information is disclosed - its confidentiality, which means the requirement not to allow the dissemination and (or) provision of information without the consent of its holder or other grounds stipulated by the legislative acts of the Republic of Belarus.[15] The rest of the information properties indicated in the law do not have a clear legislative fixation and are either blanketed in nature (their meaning can be given not only in legislative acts, but also state and international stan-

13 About information, information technologies and information protection [Electronic resource]: Federal Law No. 149-FZ of July 27, 2006 (as amended on July 13, 2015) / access from the legal system "Consultant Plus". - Date of access: 02/02/2017.

14 About information, information technologies and information protection [Electronic resource]: Federal Law No. 149-FZ of July 27, 2006 (as amended on July 13, 2015) / access from the legal system "Consultant Plus". - Date of access: 02/02/2017.

15 Information, information and information protection [Electronic resource]: Law of the Republic of Belarus No. 455-3 of 10.11.2008 (as amended on 04.01.2014) / access from the legal system "Consultant-Plus". - Date of access: 02/02/2017

dards in the field of information technology and information protection) or do not have a regulatory fixing, granting freedom for scientific research in this field.

It is obvious that the available both normative and semantic gaps in the definition of the system of information properties necessitate the activation of scientific research and solution of the indicated problem. Without the task of reviewing the properties of information in general, let us focus our efforts on the formation of such a system of information properties (qualitative and quantitative characteristics) in the context of carrying out information and analytical work. At the same time, we pay attention to the fact that qualitative characteristics, as a rule, are subjective in nature of the analyst (that is, the method of expert evaluations is based on them), and some of them can be formalized and accordingly processed using numerical methods.

The most important property of information in the context of increasing information flows is its *relevance* - the ability and opportunity to respond to questions posed by the information and analytical work entity and to remove information uncertainty (entropy) with respect to the object of information and analytical activity. Since the amount of information generated in the society constantly increases, it is important for the subject to rank incoming (processed) information for its relevance to the phenomenon under investigation, and generally shift the emphasis of information and analytical activity to the information component in favour of its analytical component. In close connection with the relevance of information is the following property information.

*Sufficiency of information* - involves the receipt, processing and use of the amount of information necessary to solve the problems facing the information and analytical work entity, and accordingly, the transfer of this amount of information in the form of an analytical document for the person making the decision (PMD). In information theory, the quantitative characteristics of information have been thoroughly studied. In this case, 1 bit is taken as a unit of information (the entropy of which is reduced to two values - no or yes, "0" and "1"). Classically, the quantitative characteristic of information of equiprobable events is determined by the following formula of R. Hartley in 1928:[16]

$$I = \log_2 N$$

It should be noted that initially the base of the logarithm was not of fundamental importance, since it characterized a unit of uncertainty. But, taking into account the emergence and development of information theory and the adopted binary system of calculus (having two states), the unit of uncertainty is called a binary unit or bit and represents the uncertainty of the choice of two equiprobable events – "0" and "1". At the same time, for non-equiprobable events the formula of K. Shannon [6] is used:

$$I = -\sum_n p_n \log_2 p_n$$

where, n - possible states, p - probability function of the n-th event, that it is true.

It should be noted in general utilitarian nature of the theory of information, in terms of determining the amount of information, communication channels, and encoding and decoding of the signal due to the development of technology and the need for the data and develop the main provisions for this particular application. At the same time, these provisions regarding the quantitative characterization of information can also be used for information and an-

16 Hartley, R.V.L. Transmission of information. - Bell System Technical Journal - 7. - 1928. Translation: Hartley RVL. Transmission of information. // Theory of information and its applications. - Fizmatgiz, 1959 – 232 p.

alytical work. Examples of such use are given in the work,[17] where the entropy of equiprobable variants of development is determined according to the Hartley formula and the practical task of search for a criminal by obtaining additional information about him and narrowing the circle of suspects from 1 000 000 people (by the condition - the number of residents of the city) to 23 people suspected of committing a crime. Thus, the acquisition of information is associated with a decrease in the variety of options or uncertainty (entropy) of the event.

The next property of information that is of key importance for the information and analytical work is *its reliability*, which implies the correspondence of its incoming message to the original message (signal). It should be noted the integral character of the considered property of information in the context of information and analytical work, which includes both quantitative and qualitative (estimated) characteristics of the message. If we propose to formalize the practical task of choosing a managerial decision for a decision maker on the basis of reliability of information based on the availability of three sources of the same information with a reliability of 30% and one source of other information with a reliability of 90%, then obviously without using a mathematical apparatus this task is not the right decision.

Undoubtedly, every message besides useful information pertaining to the event under study has information that does not have potential usefulness. It is about the so-called *information noise*, i.e. information not representing values for the subject of information and analytical activities. But, in the context of information and analytical work, there is an interest in "*tonality" (emotional colouring*) of such information noise. For example, if during the information and analytical work we consider reports published on news information resources for a certain period - $\Delta t$, then it is possible to reveal the general tonality formed by the information resource in the media (information) space of the state (from negative attitude to information messages to strictly positive). Of course, the evaluation of the tonality will be subjective and poorly formalized, based mostly on expert assessments of the relevant subjects, nevertheless the general information background created by the information resource will be clear, due to information noise as well.

No less important property of information is its *efficiency or timeliness*, which involves obtaining (creating) information at the appropriate time, which is especially important in the framework of information and analytical work at the operational-tactical level, characterized by dynamic changes in the environmental conditions and the conditions of the system. In general, within the framework of the information and analytical work, $\Delta t$, i.e. the period from the moment of information creation - $t_1$, before its processing, analysis and use - $t_2$, should tend to $\Delta t \to 0$. Obviously, the considered situation is idealistic, nevertheless, as we believe, the reduction of $\Delta t$ will increase the efficiency of information and analytical work.

Speaking about the *availability of information*, it should be noted, given the increase in information flows and, in fact, the formation of large information arrays of information, that this property of information becomes particularly important. Since the notion of information accessibility (with respect to information resources and systems) presupposes such a property of information to be available at an acceptable time (communication with information operability) upon request from an authorized entity.[18] In the context of the information and analytical work, it is necessary to pay attention to some key points within this information property. The first is the availability (availability) of information, i.e. the channels of communication between the information source and the information and analytical work entity should be

17 Information technology in the management of internal affairs: a textbook / ed. Doct. Tech. Sciences, Professor I. V. Goroshko. - Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, 2015. – p.5-6.

18 State standard STB 34.101.35-2011 "Information technology. Methods and means of security. Objects of informatization. Protection Profile Class B3."

taken into account and, secondly, the possibility of using it for solving problems within the framework of the information and analytical work.

The issues of information and analytical support lie in close connection with the protection of information, in this connection, such a property as *information security* is undoubtedly of scientific and practical interest. At the same time, the characteristic of this property includes a set of measures aimed at preventing unauthorized access, as well as ensuring confidentiality, integrity and accessibility of information - the properties of information specified in the relevant law.[14] We believe that the very nature of information and analytical activities, the sources of information used, the technologies for implementation, and, most importantly, the results obtained (until the decision of the decision maker, decisions on their publicity) should not be public. Since in the implementation of the information and analytical work the subject of analysis is often a specific citizen, his personal data and various secrets (privacy, medical, adoption, etc.), the publicity of such information, as well as the results of analysis, can have negative consequences (including legal ones) for the subject of information and analytical work, as well as the citizen himself (the object of analysis). In this regard, the security of information in the context of the information and analytical work becomes particularly important.

*Additivity of information* (complementarity), which is especially important in the IAR, as a complex property of information, emphasizes its synergetic nature. The specified property assumes complementarity of information received from one or various sources of information. At the basis of this property is the law of information additivity, according to which the amount of information $I(x_1, x_2,)$, necessary to establish $(x_1, x_2)$, is equal to the sum of the quantities $Ix_1$ and $Ix_2$, required for independent establishment of elements $x_1, x_2$:

$$I(x_1, x_2) = Ix_1 + Ix_2$$

In other words, the amount of information contained in the message about the event that several independent events occurred is equal to the sum of the amounts of information contained in the messages about individual events. Thus, the information volume of the aggregate event consists of information volumes, the events included in it. These provisions are essential in the organization and conduct of information and analytical work, taking into account its content and the number of different sources of information.

## CONCLUSION

Thus, having considered some provisions on the concept and content of such a category as 'information', it seems possible to draw the following conclusion. Information for the purposes of information and analytical work is understood as information (data) on the qualitative and quantitative characteristics of an object (phenomenon, event, process) of information and analytical activities.

The content of this category in the information and analytical work can be disclosed through a system of information properties including:

- relevance of information;
- sufficiency of information;
- reliability of information;
- timeliness of information;
- accessibility of information;
- security of information;
- additivity of information.

## REFERENCES

1. A modern dictionary of foreign words. - Moscow: "The Russian Language", 2001. – 763 p.
2. About information, information technologies and information protection [Electronic resource]: Federal Law No. 149-FZ of July 27, 2006 (as amended on July 13, 2015) / access from the legal system "Consultant Plus". - Date of access: 02/02/2017.
3. Ancient philosophy: Encyclopaedic dictionary. - M., 2008. – 896 p.
4. Gritsanov, A. The Newest Philosophical Dictionary. - Minsk: Skakun, 1999. - 896 p.
5. Gubsky, E., Korableva, G., Lutchenko, V. Philosophical Encyclopaedic Dictionary. - Moscow: Infra-M, 2005. - 576 p.
6. Glushkov, V.M. Fundamentals of paperless computer science. - Moscow: Science. -1982. - 552 p.
7. Glushkov, V.M. Introduction to cybernetics. - Kiev: Publishing House of the Academy of Sciences of the Ukrainian SSR, 1964 – 342 p.
8. Hartley, R.V.L. Transmission of information. - Bell System Technical Journal - 7. - 1928. Translation: Hartley RVL. Transmission of information. // Theory of information and its applications. - Fizmatgiz, 1959 – 232 p.
9. Information, information and information protection [Electronic resource]: Law of the Republic of Belarus No. 455-З of 10.11.2008 (as amended on 04.01.2014) / access from the legal system "ConsultantPlus". - Date of access: 02/02/2017.
10. Information technology in the management of internal affairs: a textbook / ed. Doct. Tech. Sciences, Professor I.V.Goroshko. - Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, 2015. - 156 p.
11. Kapitonova, Yu.V., Letichevsky, A.A. Paradigms and ideas of academician VM Glushkov. - Kiev: Naukova Dumka, 2003. - 456 p.
12. Shannon, K. Works on information theory and cybernetics. - Moscow: IL, 1963. - 830 p., Pp. 243-322.
13. State standard STB 34.101.35-2011 "Information technology. Methods and means of security. Objects of informatization. Protection Profile Class B3."
14. The term "information" // Material from the free encyclopedia Wikipedia [Electronic resource]. - Access mode: https://en.wikipedia.org/wiki/Information - Access date: 15/02/2017.
15. Ursul, A.D. Reflection and information. M. 1973 [Electronic resource]. - Access mode: http://informaticslib.ru/books/item/f00/s00/z0000007/ /st001.shtml - Date of access: 05.02.2017.
16. Ursul, A.D. Nature of information: philosophical essay / AD Ursul; Chelyab. State. Acad. Culture and arts; Scientific and educational. Center "Information Society"; Ros. State. Trade and economy. Un-t; Center issled. Glob. Processes and sustainable development. - 2 nd ed. - Chelyabinsk, 2010. - 231 p.
17. Winner, N. Cybernetics and Society. Moscow: Izd-vo inostr. Lit-ry. Moscow, 1958 [Electronic resource]. - Access mode: http://filosof.historic.ru/books/item/f00/s00/z0000816/st000.shtml - Date of access: 01/02/2017.
18. Winner, N. Cybernetics or control and communication in an animal and a machine. - Moscow: Soviet radio, 1968. - 325 p.

# CYBERCRIME, AS WELL AS INTERNATIONAL CYBER THREATS AND THEIR SOLUTIONS

**Bulai Iurie**
Doctor of Law, Associate Professor
Department of Criminal Procedure and Criminalistics
Academy "Stefan cel Mare"
Ministry of Internal Affairs of the Republic of Moldova
**Bulai Rodica**
Master in IT, University Lecturer
Department of Special Investigation Activity
and Information Security
Academy "Stefan cel Mare"
Ministry of Internal Affairs of the Republic of Moldova

**Abstract:** The authors approach the problem of cyber–threat in this very article. Nowadays the cyber-crime, cyber-terrorism and cyber warfare are real phenomena and their danger has exceeded the national level (of a single country) constituting threats to safety and security at the regional and international levels. The essence of these phenomena as well as some counteract visions represent the subject of study developed in this article.

**Keywords:** cybercrime, cyber terrorism, cyber warfare, cyber threats, cyber security, cooperation strategy.

## INTRODUCTION

The world lives in the era when information technologies and cyber world have become an integral part of society and of each individual separately. Cyber world represents a tremendous opportunity to simplify and improve the whole vital activity of humanity.

The rapid development of information technologies and informatisation of the society has led to the appearance of new types of crime and threats such as cybercrime, cyber terrorism, and cyber warfare.

## CYBERCRIME

To prevent cybercrimes one needs to understand this phenomenon. In the literature and practical activities the terms are found such as "computer crime", "kiberbanditizm", "cybercrime", etc.

Thus the definition of "cybercrime" is more multilateral than "computer crime", and more optimally reflects the nature of this phenomenon.

According to Zecurion Analytics, the damage to companies from data leaks in 2015 has risen from $18 billion to $29 billion. This is the biggest loss in the history of statistics. This is

a disaster typical of the vast majority of countries. The initiatives or objective reasons, according to which the number of incidents could be reduced are simply missing now. Moreover, the statistics of incidents indicates that the percentage of leaks increased by using complex schemes, including social engineering elements, implemented insiders and various information transfer channels. This means that the security services of companies will have to confront the serious challenges that differ from the typical schemes worked out by impostors in the past years. More often, the cyber-criminals use several attack vectors simultaneously, which allows identifying vulnerabilities in each separate direction, use and combining the detected holes, causing maximum damage.[1]

Each phenomenon or appearance develops, cybercrime is not an exception and the new real threats in the virtual space such as cyber-terrorism, network-centric warfare (NCW) and cyber warfare (CW) - are concepts becoming reality in the 21st century.

## CYBER-TERRORISM

**Computer Terrorism (Cyber terrorism**) — the use of computer and telecommunication technologies (first of all, the Internet) for terrorist purposes.

The term was proposed in the 1980s by Barry Collin, the senior researcher of the Institute of Security and Intelligence, who used it in the context of the trend towards the transition of terrorism from the physical to virtual world, the increasing intersection and coalescence of these worlds.[2]

A characteristic feature of cyber-terrorism and its difference from cybercrime is its scale, intensity, openness and consequences. Cyber-terrorism is a serious threat to mankind, comparable to the weapons of mass destruction. The same threat could come either from terrorist or extremist organizations, including some special services standing behind them, which seek to implement the geopolitical ambitions of their leaders.

Thus, according to some scientists, cyber terrorism is a more dangerous type of terrorism than the biological or chemical terrorism, as it can threaten millions of people because of computer vulnerability of military computers from hackers, etc.[3]

Researchers Matthew Devost, Brian Houghton and Neil Pollard define the information terrorism (a variant of which is the cyber terrorism) as: 1. Connecting the criminal use of information systems by means of fraud or abuse and physical violence, specific to terrorism; 2. The deliberate abuse of digital information systems, networks or these systems components or networks, which contribute to the implementation of terrorist operations or acts.[4]

1 Zecurion Analytics: companies' damage from data leaks for the year increased by 63% http://www.cio.ru/news/568//22.03.2017//18.38
2 *Collin B.* The Future of Cyberterrorism // decision Crime & Justice International Journal. — 1997. — Vol. 13. — Release 2.).
3 Mocanu Raluca-Ioana – 68 apud P. Griset, S. Mahan – Terrorism in Perspective, Ed. Sage Publication, Thousand Oaks, London, New Delhi, 2003, p. 158
4 Thomas T.L., "Deterrence of asymmetric terrorist threats facing the society in the information age" // "The world community against the globalization of crime and terrorism. Materials of the International Conference", Moscow, 2002, p. 165.

# NETWORK-CENTRIC WARFARE (NCW) AND CYBER WARFARE (CW)

The phenomenon of network-centric warfare (NCW) and cyber warfare (CW) are concepts becoming reality in the 21st century. In the operational art and tactics in the past decades fundamental changes have occurred that require from states a radical revision of the old military doctrines and critical reassessment of the entire spectrum of military art. In fact, today we are talking about a new military art, when the previous assessments, experience and knowledge require a radical revision or even rejection of earlier views.[5]

The concept of "information operations" was implemented by the US Army during the Gulf War (2003) being taken then by other NATO member states. In the USA doctrine, informational operations are shown as being "the integrated engagement of electronic warfare, computer network operations, psychological warfare, acts of deception/disinformation, protection operations in coordination with capabilities designed to support or those which have to collaborate for influencing, subverting, vitiation or controlling the human decision systems or automated of the opponent or his decision processes along with the protection the systems and its own processes".[6]

Since the third period of globalization and the transition from an industrial to information era affect mainly the developing countries, information is the most effective weapon. And since the prevailing type of human behaviour in the information age is network behaviour, the network-centric war fits the best. According to the Pentagon doctrine, the core of such a war is at the intersection of the social, physical, information and cognitive domains. If the information is still connected with a certain infrastructure, then the cognitive sphere is the least material of all four areas, because it exists in the human consciousness.

In an ideal form, the actors of a network war represent networks of small diverse types of associations, resembling cells. They are dispersed, but interrelated. The network must be amorphous, without a heart and head, although not all nodes of the network should be equivalent to each other. The best battle tactics in the direct and figurative sense is swarming. Like a swarm of bees, the groups of individuals united by a common idea synchronously begin to attack the target, be it a state or a transnational corporation. Superior in strength and potential of their opponents' goal, nevertheless, is forced to react to every smallest "bite", and if the attackers have a certain technique and are experienced in conflict, then the outcome is almost a foregone conclusion. In other words, against one **Goliath** goes into battle not one **David**, but many.

The Network-centric warfare threat (NCW) and cyber warfare (CW) were acknowledged of the developed countries that have created and developed and in some cases already used cyber-military structures/units**.**

The United States, China, United Kingdom, South Korea and Russia entered the top five states with the most developed special units in the area of cybersecurity for military and intelligence purposes.

This is stated in the report of the company Zecurion Analytics, which deals with the protection of data from leaks. The leader of the rating is the USA with the number of cyber troops in 9,000 people, Washington allocates 7 billion dollars for their financing. For comparison, Russia spends about 300 million dollars for these purposes, having at its disposal one thousand specialists. In its turn, China became the leader in the list of the number of cyber troops – 20,000 people. The smallest unit is in France - 800 people. Great Britain 450 $ - 2,000; South

5 http://eurasian-defence.ru/ (Date viewed: 10/04/2016).
6 Manea Valentin The information warfare and cyberspace p. 266, source: http://www.nos.iem.ro/bitstream/handle/123456789// Date viewed la 04.04.2017

Korea 400 $ - 700, Germany 250 $ - 1000, France 220 $ - 800, North Korea 200 $ - 4,000, Israel 150 $ - 1,000.[7]

The danger of cyber threats is recognized at all social levels. Thus in the European Union the IFIP Congress was held, which contains the results of the work that cannot be missed and presents the investigations on the virtual identity.[8] Thus a social survey on security has been conducted throughout Europe. The survey was carried out on more than 27,000 Europeans and can be regarded as a model survey.

So if the upper insecurity lines, the lack of a sense of security still widely dominate, the youth unemployment rate (80%), violence caused by drugs and alcohol (74%) and access to health care for the poor (69%), then, for the first time the fear risk, the concern that national Internet infrastructures may be exposed to impact/threat or become a source of viruses (39%) exceeds the fear of becoming a victim of a terrorist attack (38%).[9]

Due to various reasons, it becomes more difficult to separate the military and cyber security of a state of the region from other states, which will inevitably lead to regional military-political integration. The threat to the state could come and as a reason for the attack could serve the fact that it belongs to another military unit, economic and political union, as a result of the political-diplomatic conflict, and so on. The trend of building blocks and military-political alliances, and finding the state in the sphere of influence of the military or economic-political alliances represents a natural political and economic pattern.

The real existence of cyber-terrorism, network-centric warfare (NCW) and cyber warfare (CW) require from the states a radical revision of the old doctrines of cybersecurity and critical reassessment of the whole spectrum of areas - information systems that support the activities of critical infrastructure (fuel and energy complex, energy-distributing network system control and management of land, sea and air traffic in particular) if defeated by software tools can pose a threat to national and international security.

State authorities and local governments often are even more affected by cybercriminals and cyber-terrorists, cyber-attacks organizing espionage, data theft from the public or private strategic information systems and/or hindering their normal work. As an example, one of the first such cyber warfare occurred in April 2007, when in connection with the decision of the Estonian government to move the monument to the Liberator Soldier, the sites of state structures of the country suffered from the organized attacks. Extremely painful became this impact due to the presence in Estonia of a developed system, the so-called e-government, to which so actively seek to move not only European, but also the leading Asian countries.[10]

We believe that the best result in the fight against cyber threats is the development of cooperation at the national and regional international level. Moreover, the main actors in the development of this process must be the countries that have an impact, both at the regional and international level, such as the US, Russia, China and the European Union, etc. Unfortunately, in this direction there exist problems.

In this situation, the following examples are eloquent. The US and China leadership has undertaken a number of initiatives for the development of cooperation in this direction. In

7 The countries with the highest expenditures for cyber war are named published Korrespondent.net, January 10, 2017, 11:44, http://korrespondent.net/world date viewed 03/28/2017

8 M. Friedwald et al., "Privacy and Security Perceptions of European Citizens: A Test of the Trade-Off Model", pp. 39-53.

9 https://cybersecuritytrends.ro/category/ (No. 5) virtual library published on the 12/05/2016, date of review: 04/10/2016

10 Galushkin A. A**.** On the issue of cyberterrorism and cybercrime // Bulletin of the Peoples' Friendship University of Russia. Series: Juridical sciences. 2014. №2. URL: http://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-i-kiberprestupnosti (date of view: 04.10.2016). Scientific library of CyberLeninka: http://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-i-kiberprestupnost

particular, during the visit of the USA State Secretary John Kerry in Beijing, China, a working group on cyber security has been created, which established a mechanism for dialogue on cyber-security, which was one of the first US attempts to improve relations with China on the background of the data disclosed by Edward Snowden on the ongoing cyber espionage from America against China since 2009.

Unfortunately, the collaboration within the working group was suspended after the US accusations of commercial espionage against China. Messages appeared last year, when the US announced an attempt by five Chinese military officials to steal commercial secrets using the latest technologies. In their turn, China accused the US of cyber espionage which became known in May 2014. Investigation of the US spying in the Internet space has revealed that China has been the main objective during the conduct of the United States of illegal operations. The officials from the Chinese administration said that most of the attacks are carried out from the territory of the USA; Chinese experts estimated, in 2012, the number of attacks was more than 34 thousand.[11]

So in this area as in any other, the attempts to find opponents and allies have always been and will be; so the US military believes that the present form of government in Russia and the high level of corruption allow to carry out sufficiently effective cyber-attacks at both the internal and foreign enemies, including the United States.

Russia is a more serious cyber threat than China, says David Smith, director of the non-profit Potomac Institute Cyber Center, dealing with issues of cyber security. He expressed his opinion in an article published in the August issue of the electronic journal Defense Dossier, published by the American Foreign Policy Council.[12]

As you can see from the presented examples, the situation is far from rosy, and the threat of cyberspace, regardless of whom it comes from, cyber criminals, cyber-terrorists, centralized strategic cyber aggression (hereinafter CA) is one of the most important national security strategy of any state for the implementation of which there should be developed and implemented strategic directions and a set of measures to ensure them - analytical, legal, institutional, technological, to be undertaken at three levels: national, regional, international.

Since the incidents in cyberspace have already gone beyond the brink of ordinary crimes, the use of the definition of "cyber" with the word "war" is not on the level of "if", but on "when" and "how".[13]

Action and cooperation in every field starts with legislation (national level) and the agreements, conventions, etc. (and international level) in any field on terms acceptable to all the principles and rules.

Here are the examples of national legislations in the field of cyber security: the United States (18th United States Code, Chapter 47, Article 1029 and 1030),[14] the Russian Federation (Federal Law from December 28, 2010 Nr 390-FL "On security" and from June 28, 2014 N 172-FL "On the strategic planning in the Russian Federation"),[15] China (last Cybersecurity Act, approved on

11 Markova A.V., China and the USA in the Internet space in the context of ensuring cybersecurity // Historical, philosophical, political and legal sciences, cultural studies and art criticism. Questions of theory and practice. 2014. No. 12-3 (50). URL: http://cyberleninka.ru/article/n/otnosheniya-knr-i-ssha-v-internet-prostranstve-v-kontekste-obespecheniya-kiberbezopasnosti (date of view: 04.10.2016).

12 In the United States, Russia was named the main cyber-urosis /// http: //www.spo23.ru/cyber_war_in_russia// (date of view: 09.02.2017) .// 14.36 More: http://internet.cnews.ru

13 The merger of cyber and national security Military training should include the defense of computer networks. Ilmar Tamm, Director of the Advanced Center for NATO Cooperation on the Issues of Cyber Defense in Estonia) www.marschallcenter.org///30.01.2017

14 David Icove, Karl Seger, and William Von Storch Computer Crime a Crimenfighter-s Handbook O reily Association, inc- ISBN 1-56592-086 c.104

15 https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html//// date view 03.02.2017// 13.35

November 7, 2016 by the Chinese authorities, will come into force in June),[16] and the European Union (see the report to the European Parliament, Council, the European Committee for the economy and social aspects, and the Regional Committee of the European Union Strategy for Cybersecurity (Brussels 7.2.2013 JOIN (2013)),[17] etc. Realizing the reality of the threat, countries, in addition to their own laws, developed national strategies (envisaging prevention and confrontation of CT), efforts have been directed both at the international and regional level for generating and ratification of agreements, contracts in this sector. There are various agreements, legal acts, regulating the safety of the global cyberspace, among the first is the Budapest Convention of 2001 and other.

Among them, Tallinn Guide on international law applicable to the introduction of cyber war (Original: Tallinn Manual on the International Law Applicable to *Cyber Warfare*) - a document developed by an international group of experts at the request of the Centre of Excellence NATO joint cyber defence (*original published by the publishing house Cambridge University Press, 2013*). This manual provides that States have the right to apply various countermeasures against illegal cyber operations. Thus, the very countermeasures can be deemed illegal, but not in the case of response action (in this case, their use is justified). The state that has been the victim of an "armed attack" in cyberspace, which caused loss of a human life or other serious damage, has the right to respond with force in cyberspace and the physical world. This very thesis quite often leads to disputes and discussions, but in our view, there is nothing supernatural in it (providing clear identification of the aggressor). It is evident that the cyber aggression poses a threat and can trigger different effects in severity, but in this case, no matter how serious the consequences of cyber aggression, it cannot be compared with the consequences that can occur in case of military actions.

Over the previous years, a certain amount of experience in preventing violations in the Internet was accumulated. As part of the legal regulation at the general level, it is necessary to say about the possibilities of establishing relations concerning the functioning of the global network, namely the introduction of certain prohibitive, protective and incentive measures to reduce the socially-negative phenomena/threats in their spreading. Today in the world most countries have national legislation pertaining to the use of the global information space. First of all, proposals are being made to develop legal and organizational mechanisms for using the Internet.

In our opinion, one of the aspects of solving the problem addressed would be the prophylaxis and the evaluation of how to manage the virtual world. Nowadays, there are different methods to approach the way of legal management and regulation of the virtual world with various accents. So, studying various approaches to solving this problem, we can note several main points of view.

In the opinion of V. A. Nomokonov, legal regulation of the Internet occurs in five main areas: "protection of personal data and privacy on the web; regulation of electronic commerce and other transactions, ensuring their security; protection of intellectual property; the fight against the illegal content of information and illegal conduct on the Web; legal regulation of Internet communications".[18]

The representatives of the first approach, represented by the United States, rely on self-regulation of the global network and non-interference in its processes. First of all, it is expressed in the self-determination of the content of the sites. Another US argument is that even with all the will to regulate the information contained in the Internet, on a global scale, it is unthink-

16 digital.report///03.02.2017 date view 14.00.
17 www. europar.europa.eu /// date view 02.02.2017//в 12.15./
18 Nomokonov V.A. Actual problems of fighting cybercrime // Collection of proceedings of the international conference "Information Technologies and Security". Issue 3. - Kiev: National Academy of Sciences of Ukraine, 2003. - P. 104 - 110.

able because of its enormous volume.[19] Also, the United States, which retains technological and military leadership, has adopted at the highest level a number of directives and official documents regulating political and military activities in cyberspace. Among them stand out, the "Review of cybernetic policy"[20], "International Strategy on Cyberspace"[21] and "Strategy of the Ministry of Defense on actions in cyberspace 2011".[22] Along with this, during the presidency of B. Obama, the United States began to pay a special attention to the international and treaty aspects of this problem. Washington's activities in cyber war and cyber security led to the fact that international interest in this issue has increased dramatically.

The topic of information security was also developed at the international level within the framework of the UN. One of the principles began in December 1998 by the General Assembly (GA) which adopted by consensus (without voting) the resolution "Advances in the field of information and telecommunications in the context of international security" (document A/RES/53/70).[23]

The USA adheres to the idea of "active cyber defense". It was embodied in the Article 19 of The strategic concept of the NATO alliance (adopted in 2010 at the Lisbon summit), which identifies the main challenges and threats, where it is spoken about the need to build the capacity to detect, prevent and protect against cyber-attacks.

At the same time, the US emphasizes the need to promote private sector initiatives in the field of high technology to implement its own regulatory mechanisms, pointing out the need for government intervention if self-regulation measures are not sufficiently effective.[24] The US pursues a state policy in the field of personal information protection on the Internet, copyright protection of software and hardware developers of computer systems and their networks, combating monopoly in the information sphere, protecting consumer rights and citizens' rights to information.[25]

The countries of Western Europe hold a different point of view, proposing to combine the self-regulation of the global network with the impact on it by legislative methods. In Western Europe, it is believed that the spread of negative phenomena on the Internet can prevent effective use of its potential.[26] The optimal solution in this situation is the creation of model legal norms for all the countries. An example of such cooperation is the 2001 Council of Europe Convention on Cybercrime. Many developing countries are also concerned about the current situation. A significant group of countries of the so-called "Group of 20" (Brazil, South Africa, India and others) takes practically the same position on the legal regulation of the Internet,

19 Melyukhin I.S. Regulirovanie Interneta. / Informatsionnoe obshchestvo: istoki, problemy, tendentsii razvitiya. M., 1999. – S. 148-156./ Meliukhin IS Regulation of the Internet. Information society: origins, problems, development trends. M., 1999. - P. 148-156

20 Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington, D.C., May 29, 2009) // The White House website. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_ Review_final.pdf.

21 International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / SEAL of the President of the United States. Washington D.C., 2011. May. 26 p.

22 Department of Defense Strategy for Operating in Cyberspace / Department of Defense United States of America. Washington D.C., 2011. July. 14 p.

23 The updated draft of this resolution was adopted by consensus in December 1999, but it did not contain any fundamental changes.

24 Kozlov VE, Chernenko IT, Perspective directions of improving the legislation of the Republic of Belarus in countering computer crime / Center for Computer Crime Research. [Electronic resource]. - 05/05/2004. - URL: http://www.crime-research.ru/articles/Kozlov/ (reference date: 05.25.2009)

25 Chemerinsky K.V. Illegal organization and (or) carrying out of gambling: separate problems of the criminal liability // the International scientific edition Modern fundamental and applied researches. - 2014. - No. 3 (14). - P. 110-114.

26 Bachilo I.L. Kopylov V.A. Are there any grounds for creating the branch "Information Law" // Information Society. 1999. No. 6. - P. 49-50

offering simply "to manage the Internet globally" under the auspices of an intergovernmental organization within the UN, of the same International Telecommunication Union.

So in the opinion of A. A. Komarov, the Internet management issues include the widest range of issues, including combating spam, illegal content, but this position is actually reduced to the establishment of censorship on the Internet. Establishing censorship on the Internet, in the opinion of many, even of democratic countries, is not an attempt on the personal rights of citizens. Today, within the framework of the national legislation of individual states, more stringent measures are being taken to combat crime in the sphere of high technologies. The Japanese National Police Office (NPA) initiated the establishment of a national cybercrime centre in conjunction with the Tokyo City Police Department and other major police departments in the prefectures. In the context of globalization, legislators from different countries are calling to more decisive measures in combating violations on the Internet. The introduction of preventive measures in various countries leads to a gradual strengthening of control by law enforcement agencies over the activities of individuals in the "World Wide Web". The most radical position in this respect is occupied by the PRC. In order to establish order in the use of the Internet, the Government of China established censorship, extending to the entire national segment of the global network. The Chinese authorities have developed a system of blocking sites containing signs of extremism, terrorism and separatism. In order to prevent the spread of extremism, China's law enforcement agencies confiscate the servers that host such materials. In front of the providers is set the task to monitor the content of sites on their servers.[27]

Unfortunately, interaction within the framework of "common spaces" presupposes for some countries today not so much interstate cooperation in their development as competition for the principles of their division, and an increase in their number generates new forms of interstate or even transnational conflicts, reviving the theories of "hard power" and geopolitical competition. From the analysis of the negotiation process, it is easy to conclude that there is a significant discrepancy in the approaches to ensuring cybersecurity.

Criminals/cyber opponents know the different subtleties and accents that are launched by each state, using the discrepancy between policies and the lack of a harmonized legal approach, they use these gaps to launch and carry out cyberattacks of different genres and degrees of danger. Based on the above, in our opinion, the following steps should be taken.

## AT THE NATIONAL LEVEL, TO TAKE THE FOLLOWING MEASURES:

- Act and participate in the development of the international strategy to combat cyber threats and the creation of common international legal mechanisms to regulate the virtual space;

- To develop a draft of the National Strategy for Cyber Security Concept of the state, which should be based on the principles and laws of other government documents that would consider its implementation at various national levels and areas:

- General purpose and direction of the Strategy of cybersecurity is to provide a virtual security of the individual, the organization and the state by defining the system of priorities, principles and measures in the field of internal and external policies in which should be

27 Komarov A. A., The problem of the legal regulation of the Internet in order to suppress offenses committed against minors. // Security questions. - 2015. - No. 4. - P.28-48. DOI: 10.7256 / 2409-7543.2015.4.17103. URL: http://e-notabene.ru/nb/article_17103.html

reflected: all the components of cyberspace under which they are protected from the greatest possible number of threats and impacts of unwanted effects;

- By specific/private directions of strategies it should determine the standards of cooperation of subjects of the information society - the individual, organizations and the state - in the field of cyber security; norms for compliance the balance between the establishment of liability for non-compliance CS, on the one hand, and the introduction of excessive restrictions - on the other; CS priority risks according to the probability of realization of cyber threats and the size of the negative consequences of CS incidents; updating of means and methods to ensure cyber security in order to confront the changing cyber threats.

- Develop and implement a multi-layered institutional cyber security system, which would include:

- **Scientific-analytical level:** - which would have studied cyber security risks according to the probability of the cyber threats implementation and sizes of negative consequences; updated the means and methods of ensuring cybersecurity. This is one of the most important tasks. Since the problem is in the complexity of the classification of threats emanating from the territory of the state, and directly from it. As a result of this trend, it is necessary to emphasize the need for all states to adopt measures for the identification of cyber threats, as well as the early detection, prevention, protection and minimization of consequences.

- **Executing level**: which would carry out coordination in two directions, the internal (between national bodies responsible for the identification of cyber threats and confrontation) and external, carrying out the coordination between national institutions and similar foreign regional/international institutions.

- Increase the capacities in the field of information and abilities in confrontation electronic attacks. It is necessary to strengthen the measures of internal political character, to promote the development of the technological component of cyber security to preserve the balance of power and the preparation of a counterweight to other probabilistic "enemies" in the field of cyber security.

- Perform, implement, and realize the regional and international cooperation in the field of cyber security, monitoring the activities of criminal and terrorist groups and individual hackers operating in cyber space.

- Act and participate actively for the development of international cooperation in the region and the structures aimed at identifying the cyber threats, early detection, prevention, protection and minimization of consequences.

**On the international level:** – develop and implement an international agreement in the field of prevention and investigation of cyber aggression;

Create an international body with regional and national representative offices. This body should be the equivalent of the United Nations Organization (UNO) in cyberspace Cyber UNO (CUNO) there must be several structures, for example: scientific-analytical level, performing functions that should be the same as those at the national level we have mentioned above. Executing level may be – in our opinion, on the international, regional and national levels. The regional level will allow in the case of cyber aggression, to join the opposition in time, national level will allow on par with the national representatives, to include in the investigation regional and international representatives (CUNO). We also believe that CUNO activities should be carried out by 12 administrators chosen annually from the members of the CUNO, in contrast to the UNO there should be no privileged members, with the right to veto or permanent ones.

In the case of cyber aggression, CUNO will create a commission for investigation of international, regional, national representatives. The commission's conclusions with the appropriate evidence will be sent to the international court. The guilty will suffer the penalty of sanctions and fines, to compensate the damage.[28]

## CONCLUSION

Yes, the present world is very mobile, it is inconceivable without the cyberspace and information technologies, and these areas are vulnerable, responding to evil with even greater evil we generate chaos. The key to solving the problem is poise objectivity, negotiations and agreements in which all would participate and respect the taken decisions.

We believe that participation in the conference of eminent experts from different countries will enhance the scientific level of the scientific forum and the conclusions and recommendations developed by them will serve to strengthen countries' security and combating cyber aggression around the world.

## REFERENCES:

1. Bachilo I.L., Kopylov V.A., Are there any grounds for creating the branch "Information Law" // Information Society. - 1999. - No. 6. - P. 49-50
2. Bulai Iu., Bulai R., Patraşo A., Netcentric / Cyber war – Real threats of safety of the contemporary world Materials of the international scientific and practical conference entitled Theoretical and Practical Problems of Information Security held at Minsc, Belorusia 18 May 2017
3. Collin B**.** The Future of Cyberterrorism // Crime & Justice International Journal. — 1997. — Vol. 13. — Release 2**.).**
4. Chemerinsky K.V., Illegal organization and (or) carrying out of gambling: separate problems of the criminal liability // the International scientific edition Modern fundamental and applied researches. - 2014. - No. 3 (14). - P. 110-114
5. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington, D.C., May 29, 2009) // The White House website. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_ Review_final.pdf.
6. David Icove, Karl Seger, and William Von Storch Computer Crime a Crime Fighter's Handbook O Reily Association, Inc- ISBN 1-56592-086 c.104
7. Department of Defense Strategy for Operating in Cyberspace / Department of Defense United States of America. Washington D.C., 2011. July. 14 p.
8. Galushkin A.A. On the issue of cyberterrorism and cybercrime // Bulletin of the Peoples' Friendship University of Russia. Series: Juridical sciences. 2014. №2. URL: http://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-i-kiberprestupnosti (date of view: 04.10.2016). Scientific library of CyberLeninka: http://cyberleninka.ru/article/n/k-voprosu-o-kiberterrorizme-i-kiberprestupnosti

28 Bulai Iu., Bulai R., Patraşo A. Netcentric / Cyber war – Real threats of safety of the contemporary world, Materials of the international scientific and practical conference entitled Theoretical and Practical Problems of Information Security held at Minsc, Belorusia 18 May 2017

9. Kozlov V.E., Chernenko I.T., Perspective directions of improving the legislation of the Republic of Belarus in countering computer crime / Center for Computer Crime Research. [Electronic resource]. - 05/05/2004. - URL: http://www.crime-research.ru/articles/Kozlov/ (reference date: 05.25.2009)
10. Komarov A.A., The problem of the legal regulation of the Internet in order to suppress offenses committed against minors. // Security questions. - 2015. - No. 4. - P.28-48. DOI: 10.7256 / 2409-7543.2015.4.17103. URL: http://e-notabene.ru/nb/article_17103.html
11. Manea Valentin The information warfare and cyberspace p. 266 http://www.nos.iem.ro/bitstream/handle/123456789// Date viewed la 04.04.2017
12. Mocanu Raluca-Ioana – 68 apud P. Griset, S. Mahan – Terrorism in Perspective, Ed. Sage Publication, Thousand Oaks, London, New Delhi, 2003, pag. 158
13. Markova A.V., China and the USA in the Internet space in the context of ensuring cybersecurity // Historical, philosophical, political and legal sciences, cultural studies and art criticism. Questions of theory and practice. 2014. No. 12-3 (50). URL: http://cyberleninka.ru/article/n/otnosheniya-knr-i-ssha-v-internet-prostranstve-v-kontekste-obespecheniya-kiberbezopasnosti (date of view: 04.10.2016).
14. Meliukhin I.S., Regulation of the Internet. Information society: origins, problems, development trends. M., 1999. - P. 148-156.
15. Nomokonov V. A., Actual problems of fighting cybercrime // Collection of proceedings of the international conference "Information Technologies and Security". Issue 3. - Kiev: National Academy of Sciences of Ukraine, 2003. - P. 104 - 110.
16. Ilmar Tamm, The merger of cyber and national security Military training should include the defense of computer networks. Ilmar Tamm, Director of the Advanced Center for NATO Cooperation on the Issues of Cyber Defense in Estonia) www.marschallcenter.org///30.01.2017
17. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / SEAL of the President of the United States. Washington D.C., 2011. May. 26 p.
18. Thomas T.L., "Deterrence of asymmetric terrorist threats facing the society in the information age" // "The world community against the globalization of crime and terrorism. Materials of the International Conference", Moscow, 2002, p. 165
19. Zecurion Analytics: companies' damage from data leaks for the year increased by 63% http://www.cio.ru/news/568//22.03.2017//18.38
20. http://eurasian-defence.ru/ (Date viewed: 10/04/2016).
21. The countries with the highest expenditures for cyber war are named published Korrespondent.net, January 10, 2017, 11:44, http://korrespondent.net/world date viewed 03/28/2017
22. https://cybersecuritytrends.ro/category/ (No. 5) virtual library published on the 12/05/2016, date of review: 04/10/2016
23. In the United States, Russia was named the main cyber-urosis /// http: //www.spo23.ru/cyber_war_in_russia// (date of view: 09.02.2017) .// 14.36 More: http://internet.cnews.ru
24. https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html//// date view 03.02.2017// 13.35
25. digital.report///03.02.2017 date view 14.00.
26. www. europar.europa.eu /// date view 02.02.2017//в 12.15

# VULNERABILITY TESTING USING METASPLOIT FRAMEWORK

**Mladen Živković**
*Kromberg & Schubert Serbia doo Kruševac, mladen.zhivkovich@gmail.com*
**Petar Čisar**
*Academy for Criminalistic and Police Studies, Serbia, petar.cisar@kpa.edu.rs*
**Imre Rudas**
*Obuda University, Hungary, rudas@uni-obuda.hu*

**Abstract:** This paper presents several important aspects of the application of tools and techniques within the Kali Linux operating system to test the vulnerability of computer system, with two main objectives - proactive information protection and ethical hacking. The complexity of the system vulnerability estimation highlights the need of performing the penetration test using a number of tools and techniques, as well as the necessary knowledge and skills, which is covered by the Kali Linux operating system. The paper also presents the practical application of advanced exploit tools of Kali Linux called Metasploit Framework (MSF), which is designed to investigate and determine the target and exploit realized attacks. MSF is an efficient and flexible development platform, which has reached a stage where it can successfully carry out the testing of the security status of computer and network systems, as a result of continuous development and improvement of the Kali Linux tools. One such example is the Meterpreter payload within the Metasploit tool, whose functionalities are explained in more detail in the paper. In addition, it was pointed out that MSF holds the possibility of extending the implementation of the outputs from other tools such as Nmap. Necessary examinations and tests were conducted in a virtual network environment, incorporating more hosts with different operating systems and levels of protection. As a complete platform to explore the system security, proactive protection and active digital forensic investigation in function of ethical hacking, Metasploit allows end users to customize the framework to their needs.

**Keywords:** ethical hacking, vulnerability, penetration testing, Kali Linux, Metasploit, Meterpreter.

## INTRODUCTION

The Metasploit Framework (MSF) is a penetration testing toolkit, exploit development platform and research tool. The framework includes a lot of pre-verified exploits and auxiliary modules for a handy penetration test. Different payloads, encoders, handlers, etc. are also a part of Metasploit which can be mixed up to work on any penetration testing kind of work.

In addition, Metasploit also serves as a platform for payload development (code execution after a successful launch of exploits), payload encoder (payload encryption, which makes data undetermined, so that detection system (Intrusion Detection Systems - IDS) and the system for protection against intrusion (Intrusion Protection Systems - IPS) do not recognize and block exploit), but also contains a variety of other tools. Metasploit also allows avoiding anti-forensic tools (Forensic Avoidance Tools), as well as other IDS techniques.

The architecture of MSF is divided into three major categories - libraries, interfaces and modules.

The interface (Console, CLI, Web, GUI) basically provides the beginning of operational activity of any type of module (Exploits, Payloads, Auxiliaries, Encoders, NOPs). Each of these modules has its own specific function in the process of testing:[1]

- *Exploit* is the 'proof-of-concept' of code developed to exploit certain vulnerabilities of the target system. The body or structure of Exploit can be divided into different components.

- *Payload* is a malicious code that is standalone or part of Exploit designed to launch arbitrary commands on the system.

- *Auxiliaries* is a set of tools designed to scan, do eavesdropping (sniffing), take the electronic signature, as well as other tasks for the security assessment.

- *Encoders* provide the possibility to avoid the detection of the virus, firewall, IDS/IPS and other similar protection mechanisms against malware by payload encryption during the operation of system testing on a breakthrough.

- *NOP* (No Operation or No Operation Performed) is a set of language instructions that is often added to the shellcode, whose only function is to consistently cover payload space.

## USING METASPLOIT FOR VULNERABILITY TESTING

The use of Metasploit for vulnerability testing will be presented through a series of screen situations.

The first four figures give a visually representation of how the tool is launched. Users find the graphical user interface named Armitage of great help. The first task after successful launching is the identification of the existing networks (Network Scan).

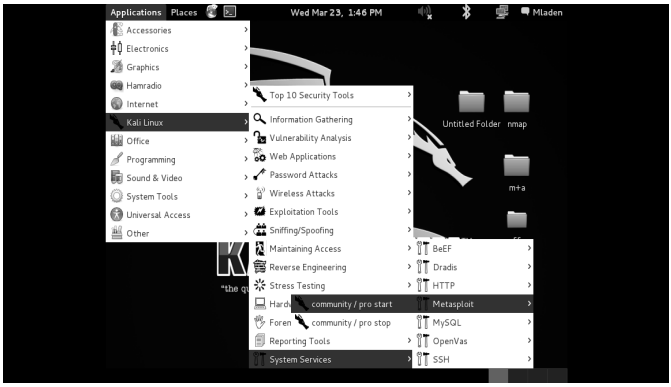



*Figure 1. Launch of Metasploit Tool*

1 Gojko Grubor, Aleksandra Pešić: Testiranje na proboj u funkciji proaktivne forenzike i zaštite informacija, Međunarodni naučni skup Sinergija, 2012

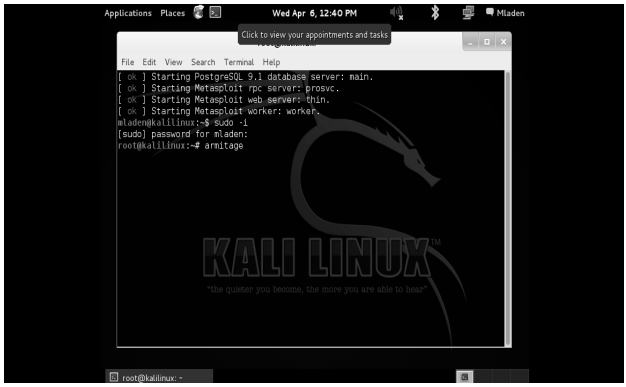



*Figure 2. Launching Armitage (GUI for Metasploit)*

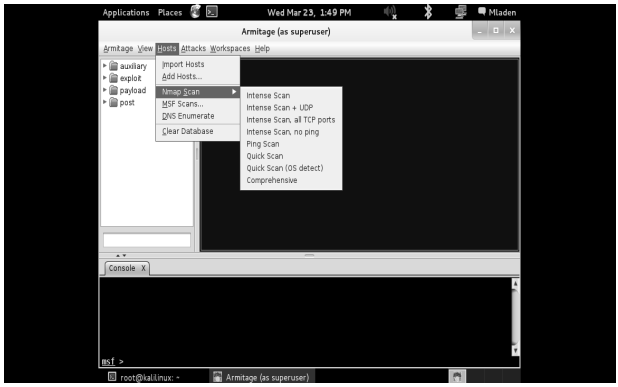



*Figure 3. Network Scan*

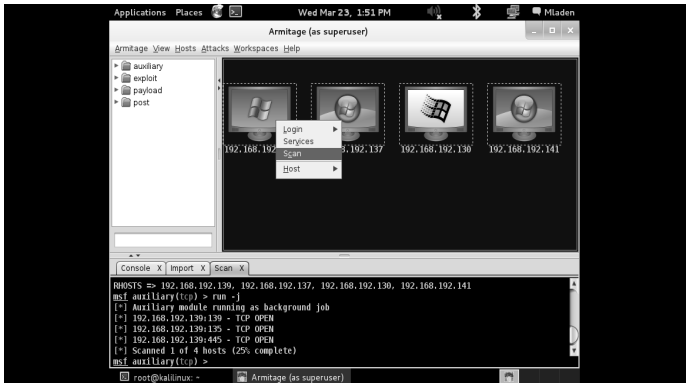



*Figure 4. Launching Metasploit Scan*

The aim is to test which attacks the target computer is vulnerable to. The process is initiated by marking the computer that is to be explored, then the tab Attack / Find Attacks is activated, which is located in the main menu.

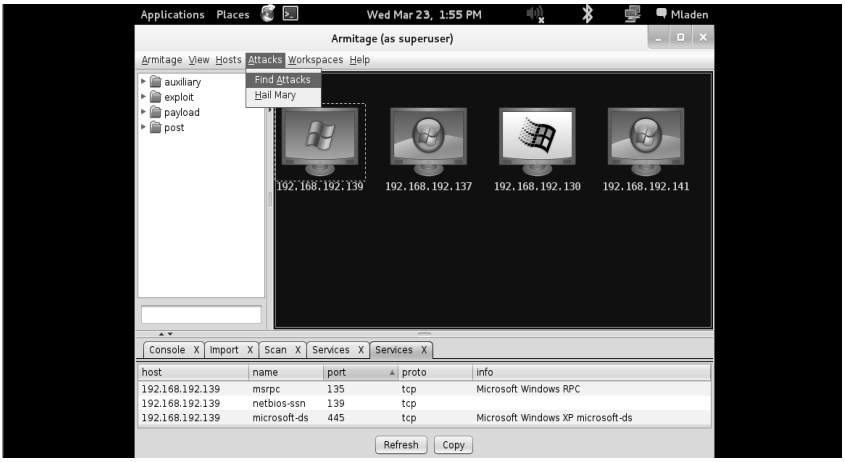



*Figure 5. Vulnerability Testing - 1*

As shown in Figure 5, the scan is launched in order to identify all attacks to which the computer with the IP address 192.168.192.139 is vulnerable. After a brief scan, a right click on a given computer in the drop-down menu opens a tab named *attack* in which it is possible to further test whether the observed computer is vulnerable to some of the attacks from a given group.


*Figure 6. Vulnerability Testing - 2*

In the tab below the graphical view of computer called *Check Exploits* is shown, where it can be noticed that the computer with the IP address 192.168.192.139 is vulnerable to an attack called *ms08-067-netapi*.

The opened ports on a specific computer determine which attacks can be performed on it.


*Figure 7. Launching an attack*

After launching an attack, there is a submenu with the detailed descriptions of the attacks that have been chosen, as well as additional settings.

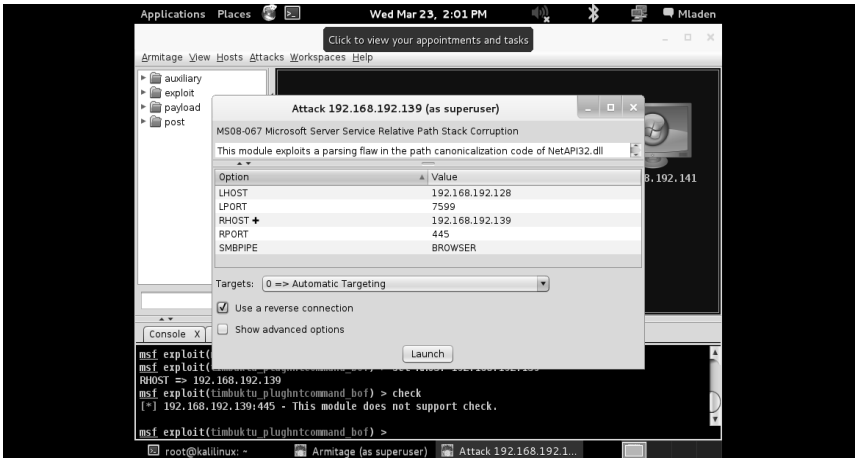



*Figure 8. Setting of an attack*

By clicking on the Launch button, the user then starts the given attack.

After a brief scan, the attacked computer changes the view into the Armitage interface, which indicates that the computer has been compromised and the access to the system is free.

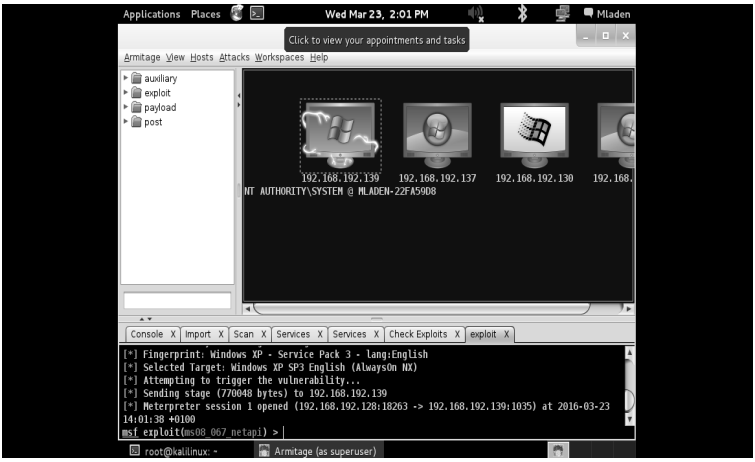



*Figure 9. Taking control over examined computer*

A right-click on the compromised computer generates the option Meterpreter 1 and clicking on it gives additional options that actually show what can be done to the analyzed computer.

One of the very important features of Metasploit is its tool-arsenal for post-exploitation activities. Meterpreter has been developed within Metasploit so as to make this task faster and easier.

Meterpreter (which stands for 'Meta-Interpreter') is an advanced, stealthy, multiple and dynamically extensible payload acting by injecting the 'reflective DLL' into the target memory. Scripts and accessories can be dynamically loaded at run time, to extend the exploitation activities. This includes the privilege escalation, export system task (dumping system accounts), reading keyboard rate (keylogging), and continuous maintenance of the backdoor (persistent backdoor service), enabling remote access (enabling remote desktop) and many other malicious operations. Moreover, the whole communication of the Meterpreter shell is encrypted by default.[2]

In addition, Meterpreter allows developers to write their own plug-ins in the form of a DLL file that can be uploaded and executed on the remote system. The real advantage of Meterpreter is that it works on the principle of self-injection in vulnerable processes on a remote system, during exploitation. All commands that pass through Meterpreter are also executed in the context of the current processes. In this way, Meterpreter is able to avoid detection by anti-virus or basic forensic investigation.[3]

2 Lee Allen, Tedi Heriyanto, Shakeel Ali: Kali Linux - Assuring Security by Penetration Testing, Packt Publishing Ltd, 2014.
3 Gojko Grubor, Aleksandra Pešić: Testiranje na proboj u funkciji proaktivne forenzike i zaštite informacija, Međunarodni naučni skup Sinergija, 2012.

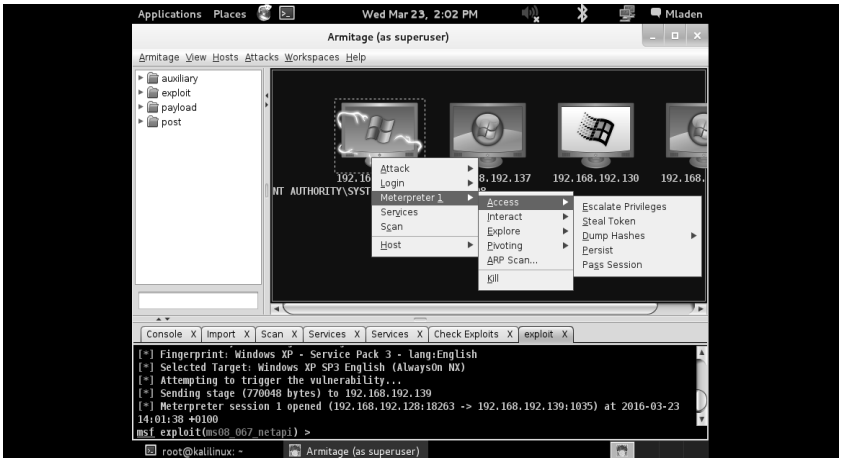



*Figure 10. Meterpreter Options - 1*

Some of the interesting attacks that Meterpreter allows include Dump Hashes from the submenu Access through which all the user names and passwords of a computer can be reached.


*Figure 11. Meterpreter Options - 2*

Following this the Desktop (VNC) from the submenu Interact, through which it can be seen what the compromised computer's user is currently working on.

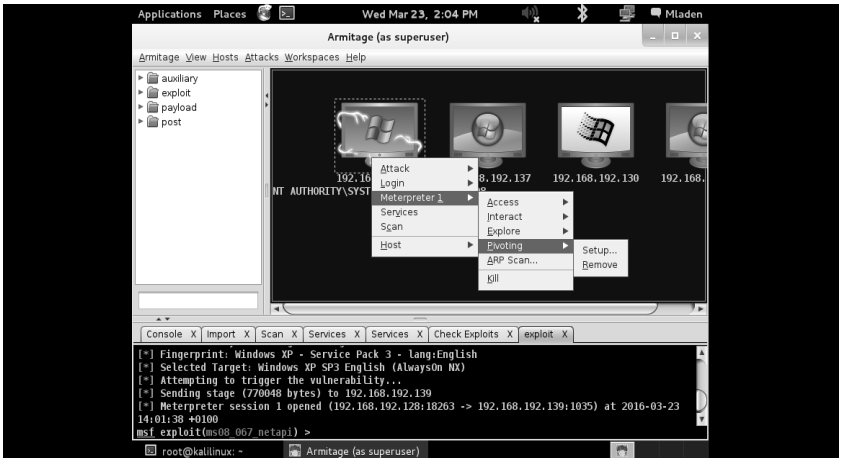



*Figure 12. Meterpreter Options - 3*

*Pivoting* is one of the common options used by 'blackhat' hackers; its purpose is that, when someone attacks a computer, further attacks on other computers are also carried out over that computer. This option allows one to create a primary computer from which all attacks are executed, further, to hide and prevent detection, i.e. if someone tries to determine where the attack came from, it will not reach the primary computer, and instead, the computer is taken as a pivot.

*Arp scan* is used to locate other active hosts on the network.

*Kill* serves for closing Meterpreter options.

One of that deserve more attention is 'Explore'. There are options such as *Browse Files* for the examination of the compromised computer's files, *Show Processes* which allows the reviewing of the processes that are active on the computer, as well as the option *Webcam Shot* which, if the attacked computer has a camera, can activate it remotely and see who is in front of the computer without the user's knowledge, and lastly, the option *Screenshot*, which gives access to the compromised computer's display screen.

After launching the Screenshot option, the screenshot of the attacked computer appears in the lower part of the screen (Figure 13), which is then stored in the folder created at the beginning and where one can gain the whole preview of the attacked computer start screen.


*Figure 13. Preview of attack result*

## CONCLUSION

As shown in this paper, the main feature of the Metasploit Framework is to simplify the process of exploitation itself. Various modules, such as Meterpreter that are directly injected into the process to run exploit on the system, as an auxiliary tool for avoiding IDS and the detection by the user is very powerful.

In examining the possibilities for intrusion, the focus is more on the collection and exploitation of information and less on the phase after the exploitation itself. At this stage most of the damage is already done, but it is precisely at this stage that Meterpreter becomes highly useful. Meterpreter tries to avoid HIDS (Host Intrusion Detection Systems), injecting its code into the already initiated process and enabling an attacker to use new coding and launching scripts, which corrupts the platform for further attacks. The Metasploit Framework has a support for databases so it can interact with a huge variety of databases, such as Postgres or SQLite.[4]

Although it is impossible to make a completely secure and protected system, due to the rapid progress of information and protection technology, the great problem of exploiting vulnerabilities in all areas of computing can be solved with a greater degree of success. This paper discussed several key aspects of the application of tools and techniques of the Kali Linux system for testing the vulnerability of the system on intrusion, with two main objectives: proactive information protection and ethical hacking. The overview of the research methods of vulnerabilities highlights the need for the process of testing the system on an intrusion requires a number of tools and techniques, as well as the necessary knowledge and kills for assessing vulnerability, which is all included within the Kali Linux operating system. Online repositories are of great benefit where there are a large number of publicly available studies and researches on vulnerabilities and exploit codes, as well as testing systems with Kali Linux tools.

This paper presents a practical application of advanced exploit tools of Kali Linux called the Metasploit Framework, which are designed to investigate, to determine the target and

4 Gojko Grubor, Aleksandra Pešić: Testiranje na proboj u funkciji proaktivne forenzike i zaštite informacija, Međunarodni naučni skup Sinergija, 2012

exploit realized attack. An insight into the development of exploits is given by analyzing each step of exploit code from MSF, which provides a deeper understanding of the basic structure and strategy of planning attack and exploitation.

MSF, a powerful and flexible development platform, has reached the stage where it can test the security status of computer and network systems, due to the continuous development and improvement of Kali Linux tools. As it has been highlighted, Metasploit has the capability of widening and implementation of outputs from other tools such, as Nmap for instance.

As a complete platform to explore the system security and proactive protection and active digital forensic investigation in function of ethical hacking, Metasploit allows end users to customize the framework to their needs.

The automation of Metasploit is much more than the simple launch of exploits through a wide variety of networks and target computers. It is actually the automation of what happens after the successful exploitation of vulnerabilities. Given that vulnerability scanners do not actually take control of the host, it is not possible to do anything after the exploitation, such as adding users (for security reasons) or even downloading and installing security patches on the vulnerability that allows the control of the host.

Proactive protection of information and proactive testing system on intrusions are the best ways of defense, as they require the regular updating of system software with security patches, strengthening the system protection with new mechanisms, and a security training of employees for solving detected configuration vulnerabilities, hardware and human factors. In this way, the risk of malicious attacks and exploit vulnerabilities in the system are greatly reduced. In addition, deeper understanding of operating systems and applications can improve the writing of better, safer codes, which is of great importance for information security and business organizations. This is the main aim of ethical hacking and ethical hackers.

## LITERATURE

1. Monica Agarwal, Abhinav Singh: Metasploit Penetration Testing Cookbook, Packt Publishing Ltd, 2013.
2. Lee Allen, Tedi Heriyanto, Shakeel Ali: Kali Linux - Assuring Security by Penetration Testing, Packt Publishing Ltd, 2014.
3. Robert W. Beggs: Mastering Kali Linux for Advanced Penetration Testing, Packt Publishing Ltd, 2014.
4. James Broad, Andrew Bindner: Hacking with Kali, Elsevier, 2014.
5. Gojko Grubor, Aleksandra Pešić: Testiranje na proboj u funkciji proaktivne forenzike i zaštite informacija, Međunarodni naučni skup Sinergija, 2012
6. David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni: Metasploit – The Penetration Tester's Guide, No Starch Press, San Francisco, 2011.
7. Armitage Tutorial – Cyber Attack Management for Metasploit, http://www.fastandeasyhacking.com/manual
8. Kali Linux Tutorials – Metasploit Framework, http://kalilinuxtutorials.com/metasploit-framework/
9. Metasploit, https://www.metasploit.com/
10. Official Kali Linux Documentation eBook, http://docs.kali.org/pdf/kali-book-en.pdf

# SECURITY ASSESSMENT OF UNIVERSITY WEBSITES IN SERBIA BY USING AUTOMATED BLACK BOX TESTING

**Petar Milić**[1]
University of Niš, Faculty of Electronic Engineering, Niš
**Kristijan Kuk,**
University of Criminalistic and Police Studies, Belgrade
**Jelena Mišić**
Department of Informatics and Computing,
**Stefan Kartunov**
Technical University of Gabrovo, Faculty of Mechanical and Precision Engineering, Gabrovo, Bulgaria

**Abstract:** University websites have a large number of users with variety of services offered to them. These websites bring vulnerabilities of different types depending on the technology used for web site building and infrastructure where they are deployed. Some of these websites are built by using Content Management Systems (CMS) due to their flexibility, structure of information and easy maintaining as the most common way to make services and data available on the Internet. In this paper the authors will analyze vulnerabilities of CMS (Content Management Systems) used for building university websites in Serbia, as a popular technology used for that purpose. Such CMS systems are Wordpress, Drupal and Joomla. Websites will be randomly selected and analyzed by using automated black box testing in order to detect which vulnerabilities are mostly represented. With application of this type of tests, the authors will try to identify how vulnerable are server side and client side of CMS systems and give recommendations about handling the possible security issues. Moreover, they will give comparative analysis of detected security issues in these CMS systems.

**Keywords:** website security, black box testing, vulnerability, CMS security.

## INTRODUCTION

University websites deployed on the Internet are mostly developed with aim to provide information to its users (regardless whether they are students or teachers), to facilitate communication between teachers and users and to serve as teacher resource centers with broad scope of options, integrating in thus WWW activities and learning process. These websites (faculty, college, department, laboratory, etc.) have a large audience which needs to be satisfied in terms of their need and expectations. Moreover, these sites represent technology-based learning environments and first point of entrance of future students in world of higher education websites. Generally speaking, these websites can be constructed via different approaches. One approach is development of the website starting from raw code programming and designing, while another implies usage of CMS (Content Management System) systems which contain predefined themes, functions, categories and many other features. The advantage of CMS

1 milicpetar86@gmail.com.

systems is easy maintaining which doesn't require programming knowledge in order to edit something on the website and where any person who is familiar with IT technologies can be an author and editor of the website. CMS systems contributed to the growth of the Internet due to their popularity, thus becoming a standard in building websites.

Nevertheless, any new change in the field of IT technologies and consequently Web, unfortunately leads to attraction of attention of attackers especially due to its popularity. According to the Internet World Stats, 2016, and as of June 2016, the number of current Internet users is 3.68 billion which is estimated to be equal to 50.1% of the world population. Due to these facts, it becomes clear why attackers are attracted to web application and websites. Reasonably, any web application available on the Internet is exposed to the attacks and potentially has some vulnerability. They are exploited by attackers in order to gain access to system or network or to cause loss and harm. Vulnerabilities in web application can be caused by improper implementation of web application and technology behind it, inadequate security of Web server and back-end database and also by lack of privacy policies. Thus the task of securing web applications is the one of the main concerns in their exploitation. According to the OWASP (Open Web Applications Security Project) Top Ten[2], the most common web application security risks identified recently on the web were given in Table 1.

**Table 1.** *OWASP Top Ten Vulnerability 2013*

| Ranking | Vulnerability |
|---|---|
| A1 | Injection |
| A2 | Broken Authentication and Session Management |
| A3 | Cross-Site Scripting (XSS) |
| A4 | Insecure Direct Object References |
| A5 | Security Misconfiguration |
| A6 | Sensitive Data Exposure |
| A7 | Missing Function Level Access Control |
| A8 | Cross-Site Request Forgery (CSRF) |
| A9 | Using Components with Known Vulnerabilities |
| A10 | Unvalidated Redirects and Forwards |

In this paper the authors will try to identify security vulnerabilities related to the CMS systems as one of the main categories of web applications with special focus on university websites constructed by them. By manual search of university websites in Serbia, it has been identified that following four websites of the University of Belgrade were constructed by CMS systems: Faculty of Economy – WordPress, Faculty of Philology – Wordpress, Faculty of Security Studies – Joomla, Faculty of Philosophy – Drupal, while four web sites of the University of Pristina temporary seated in Kosovska Mitrovica are constructed in following manner: University website – Joomla, Faculty of Art – Joomla, Center for Career Development – Drupal and ERASMUS+ project DBBT – Wordpress. The analysis will be conducted via automated black box testing. Automated tools for searching for vulnerabilities were chosen because of time consuming manual code analysis and resource limitations. CMS systems which will be outlined in this paper are Wordpress, Joomla and Drupal, as most popular. A comparison of obtained results and detected security issues will also be given.

2 Project The Open Web Application Security. (2013). Retrieved 2016, from The Ten Most Critical Web Application: https://www.owasp.org/index.php/Top_Ten.

## RELATED WORK

Erlingsson, Benjamin and Yinglian[3] propose MET (Mutation-Event Transforms) mechanism in order to enforce web application security policies from server side to client side. Security policies are specified via METs on server side of web application for direct enforcement at the client. By monitoring client behaviour and checking each web page modification METs achieve web page conformation with security policies. Similar, Antón, Earp and Reese[4] previously found that privacy policies are very useful in ensuring security of web applications by addressing common goals for a given web application. They developed taxonomy which broadly classifies privacy goals as either privacy protection or privacy vulnerabilities, with aim to help developers to evaluate application trust by aiding in the examination of its policies, requirements and practices.

The most prevalent security incidents related to the web application are XSS (Cross Site Scripting) and SQL injection attacks. These attacks come due to the fact that valuable data passes through the web application that uses databases[5]. Improper validation and handling of user input leads to the insertion of malicious code by attacker which can grant access to sensitive information and moreover, cause loss of data. According to the analysis of these two types of vulnerabilities by Fonseca & Vieira[6], it can be concluded that XSS attacks have large distribution in 11 observed fault types caused by them. This is in line with statement of Fonseca, Vieira & Madeira[7], who say that XSS and SQL injection attacks on web applications are most used approach by attackers who have moved their focus from network attacks. Security mechanisms such as firewalls, encryption, intrusion detection and role-based access control, protect network, but they cannot refuse attacks that target web application. Web applications are subjected to these attacks mostly due to the faults in developed software. Moreover, these faults are the result of faulty application logic. By observing normal behaviour of a web application in relation to its code, eventual violations can be identified[8]. These authors used dynamic execution to extract program invariants in combination with model checking to identify specification violations. In that manner, some logic flaws of web application related to the security-sensitive functionality can be detected.

Huang, Yu, Hang, Tsai, Lee, & Kuo[9], have proposed an approach where web application code is analyzed statically inline with ensuring runtime protection of vulnerable code increasing thus security of web application without user intervention. This approach fixes potentially vulnerable sections of code while it is not running, preventing any danger of loss of data and

3 Erlingsson, U., Benjamin, L. V., & Yinglian, X. (2007). End-to-End Web Application Security. San Diego, USA: In Proceedings of the Workshop on Hot Topics in Operating Systems.

4 Antón, A. I., Earp, J. B., & Reese, A. (2002). Analyzing website privacy requirements using a privacy goal taxonomy. In Proceedings of the IEEE Joint International Requirements Engineering Conference (pp. 23–31). Essen, Germany: IEEE.

5 Milić, P., Kuk, K., Civelek, T., Popović, B., & Kartunov, S. (2016). The Importance of Secure Access to E-government Services. In Proceedings of the International Conference "Archibald Reiss Days" (pp. 307–316). Belgrade, Serbia: Academy of Criminalistic and Police Studies.

6 Fonseca, J., & Vieira, M. (2008). Mapping software faults with web security vulnerabilities. In Proceedings of the IEEE International Conference on Dependable Systems and Networks (pp. 257–266). Anchorage, Alaska, USA: IEEE.

7 Fonseca, J., Vieira, M., & Madeira, H. (2007). Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks. In Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing (pp. 365–372). Melbourne, Australia: IEEE.

8 Felmetsger, V., Cavedon, L., Kruegel, C., & Vigna, G. (2010). Toward Automated Detection of Logic Vulnerabilities in Web Applications. In Proceedings of the 19th USENIX Security Symposium (pp. 143–160). Washington, DC, USA: USENIX.

9 Huang, Y.-W., Yu, F., Hang, C., Tsai, C.-H., Lee, D. T., & Kuo, S.-Y. (2004). Securing Web Application Code by Static Analysis and Runtime Protection. In Proceedings of the 13th international conference on World Wide Web (pp. 40-52). New York, NY, USA: ACM.

trying to guarantee soundness. Nevertheless, it must be pointed out that there are vulnerabilities which cannot be statically verified, such as dangling pointer, memory leak, buffer overflow, etc. Utilization of static code analysis method can be combined in a complementary fashion with monitoring approach, where web application execution is monitored and can be stopped for further execution if attack occurs, i.e. vulnerability is exploited.

Recent study on occurrence of vulnerabilities in CMS systems conducted by Yang, Kim, Y. Lim & Lim H[10] showed that high level of vulnerabilities was found in Wordpress, even 77.6%. They state this is caused by the overwhelming amount of usage of this CMS systems for building web applications and its poor security performance. Moreover, there is a relation between popularity of specific CMS system and its vulnerability, which shows that as CMS is more popular it is likely to be more vulnerable. Other CMS systems such as Joomla, Drupal and Magento are less vulnerable. Jerković, Vranešić & Dadić[11] identified that easy remote identification of CMS system, poor programming practicies while creating plugins, lack of oversight while submitting plugins, poor inspection of potential security issues with plugins and lack of autoupdate of CMS system are general security problems related to them.

## ANALYSIS OF SECURITY OF UNIVERSITY WEBSITES BASED ON CMS

Often, successful attack represents brute-force search conducted by using special convention for file naming, where hidden files are located on standard locations, especially in CMS systems. Attackers mostly create access points for themselves (sometimes called "backdoors") in the database, code, directories and other locations. If attacker breaks into the website, he/she will typically try to access the *wp-config.php* file (for Wordpress), because this file contains important information about site database, security keys, etc. Getting access to this information would allow attacker to change anything in the database, such as for example creation of user accounts, upload of files and taking control of the site. The three most likely affected files for Joomla CMS are: root's *index.php*, the template *index.php* and *.htaccess* file. A common attack is simply to modify the *index.php* or any code file in the Drupal site such as a template file. Also, some files are not part of known Drupal codebase, e.g. modules/system.

Table 2 provides some of the most common files attacked by hackers in some of the more popular Content Management Systems. These files are a good place to start looking for any malicious code. The aim of this paper is to analyze security of different CMS systems used for building websites of universities, faculties and other higher education institution websites in Serbia with special focus on the Wordpress, Joomla and Drupal. By conducting automatic black box testing the authors will try to identify vulnerabilities in these systems and to assess their security level. A comparison of similar vulnerabilities will be given in order to get information on how these systems are dealing with security risks. Common security risks identified in Table 1 in Introduction section is going to be analyzed. As CMS systems are popular technology for building websites, and keeping in mind identified target group for analysis and assessment, the research is justified.

10 Yang, Y., Kim, Y., Lim, Y., & Lim, H. (2016). A Comparison of Open-Source CMS and Analysis of Security Vulnerability. INTERNATIONAL JOURNAL OF COMPUTERS , 10, 82–86.

11 Jerković, H., Vranešić, P., & Dadić, S. (2016). Securing web content and services in open source content management systems. In Proceedings of the 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1644–1649). Opatija, Croatia: IEEE.

Beside analysis of CMS systems, automatic tool that was used will also give us information about web server configuration errors that may have security implications on implemented CMS system. Furthermore, it should detect whether there are IDS (Intrusion Detection System) and how it deals with large amount of requests and responses.

**Table 2.** *Common vulnerable files in CMS*

| *CMS* | *Files attacked by hackers* |
|---|---|
| ***Wordpress*** | wp-load.php, wp-config.php, functions.php and /wp-content/plugins/plugin.php. |
| | wp-content/wp-cache-config.php and wp-content/advanced-cache.php or wp-content/plugins/wp-super-cache/. |
| ***Joomla*** | includes/defines.php and /configuration.php and the homepage index.php |
| | index2.php, changelog.php, LICENSES.php, gdform.php, framework.php, and credits.php |
| ***Drupal*** | index.php, configuration.php, sites/default/modules/panels/plugins/styles/default.inc |

Automatic black box testing will be achieved via OWASP ZAP[12], which has various analyzing features. OWASP ZAP is a Java-based tool for testing web application security. It is an easy-to-use tool because of its intuitive GUI, and it is used by beginners as well as professionals. Kali Linux OS has built-in OWASP ZAP tool. This tool has an easy-to-use integrated penetration testing option for finding vulnerabilities in web applications, where one of them is path traversal attack. The path traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. An attacker may manipulate a URL in such a way that the website will execute or reveal the contents of arbitrary files anywhere on the web server. OWASP ZAP Scanning Report gives detailed description about potentially vulnerable URL addresses and parameters.


**Figure 1.** *Framework for path traversal attack technique.*

12 OWASP Zed. (2016). Retrieved 2017, from OWASP Zed Attack Proxy (ZAP): http://www.zaproxy.org/.

## RESULTS AND DISCUSSION

In this section, the results that have been performed as described in previous section along with major findings will be presented. The analysis was done in actual websites powered by CMS systems. The results of the analysis classified by risk category are given in Table 3 which shows number of vulnerabilities identified at each risk category. Below is Table 4 that shows categorization of identified vulnerabilities.

**Table 4.** *Categorization of vulnerabilities*

| | ***Joomla*** | ***Wordpress*** | ***Drupal*** |
|---|---|---|---|
| ***High*** | 19 | 4 | 1 |
| ***Medium*** | 23 | 62 | 22 |
| ***Low*** | 130 | 191 | 80 |
| ***Informational*** | 30 | 25 | 21 |

**Table 3.** *Category analysis results*

| | Vulnerabilities |
|---|---|
| High | SQL Injection,<br>Remote OS Command Injection,<br>Path Traversal,<br>Cross-Site Request Forgery (CSRF),<br>Cross-Site Scripting (XSS),<br>Unencrypted password form |
| Medium | X-Frame-Options Header Not Set,<br>Directory Browsing,<br>Clickjacking |
| Low | Cookie No HttpOnly Flag,<br>Cross-Domain JavaScript Source File Inclusion,<br>Web Browser XSS Protection Not Enabled,<br>X-Content-Type-Options Header Missing,<br>Password Autocomplete in Browser |
| Informational | Disclosed e-mail address,<br>Found Robots.txt,<br>Insecure Cookies,<br>Private IP address disclosure,<br>CVS/SVN user disclosure,<br>Found an HTML object |

As we can observe in Table 3., Joomla has more security issues than Wordpress and Drupal in high risk level category. In relation to the Joomla and Wordpress, Drupal shows better overall results. The highest number of vulnerabilities was found in Wordpress. This finding is in accordance with current research in literature, which report that Drupal shows less security vulnerabilities than the competition (Jerković, Vranešić, & Dadić, 2016; Yang, Kim, Lim, & Lim, 2016) and due to the fact that Wordpress is the most popular CMS. Figure 2 presents percentage of vulnerabilities per CMS found in each category, while Figure 3. shows total percentage of vulnerabilities per category.

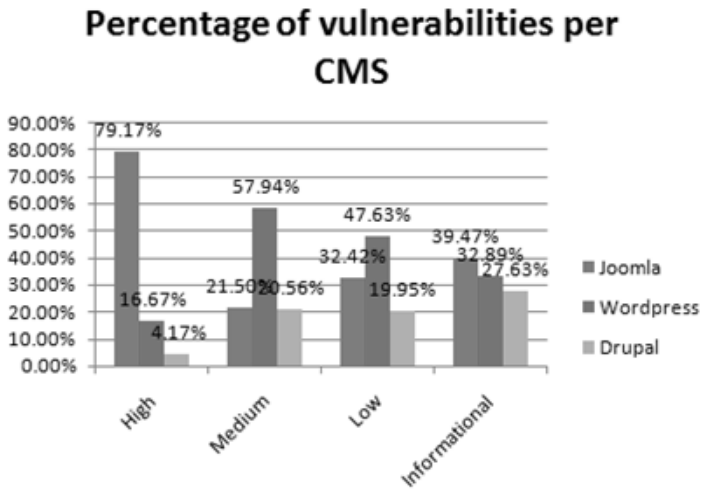



**Figure 2.** *Percentage of vulnerabilities per CMS in each category*

If we look at the percentage distribution of vulnerabilities found in each of the categories we have identified through tool OWASP ZAP which is given on Figure 3., it can be observed that only 4% of the total vulnerabilities were classified as high risk. In percentages, the highest number of found vulnerabilities found belongs to the low risk category, 66%. Some type of vulnerabilities which belongs to this category are: "Security Misconfiguration", "Cross-Domain JavaScript Source File Inclusion" and "Password AutoComplete" in Browsers.

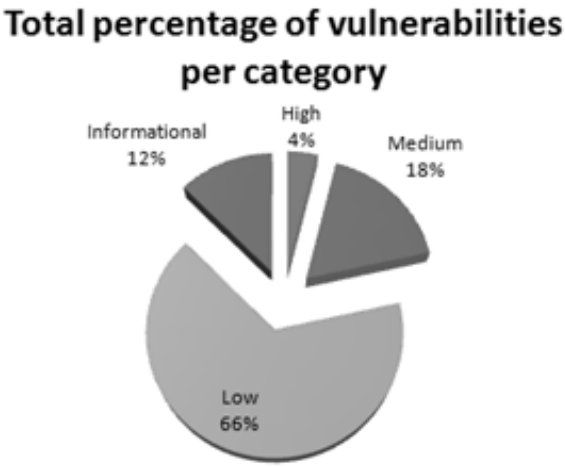



***Figure 3.*** *Total percentage of vulnerabilities per category*

Classification of vulnerabilities by OWASP Top Ten 2013 is given on Table 5. Slash in this table indicates that our tool didn't found vulnerabilities which belong to these categories. The presented values shows that Drupal has better results than Joomla and Wordpress. We

must point out, that given values for vulnerability "Cross-Site Scripting (XSS)" represents summary of this and vulnerability marked as "Web Browser XSS Protection Not Enabled" (refer to Table 4.) for which we believe that are quite similar and that represents two involved sides (server side and client side). Similar is for "Sensitive Data Exposure", where are putted values for "Directory Browsing" and "Insecure Cookies". Furthermore, "Security Misconfiguration" includes values of "X-Frame-Options Header Not Set", "Cookie No HttpOnly Flag" and "X-Content-Type-Options Header Missing".

Security Misconfiguration vulnerability is the most widespread form of the vulnerability that we discovered in our tests (Figure 4).

**Table 5.** *Vulnerability classification by OWASP Top Ten 2013.*

| | ***Joomla*** | ***Wordpress*** | ***Drupal*** |
|---|---|---|---|
| ***Injection*** | 2 | 1 | 0 |
| Broken Authentication and Session Management | / | / | / |
| Cross-Site Scripting (XSS) | 51 | 40 | 20 |
| Insecure Direct Object References | 12 | 30 | 12 |
| Security Misconfiguration | 81 | 82 | 41 |
| Sensitive Data Exposure | 69 | 43 | 40 |
| Missing Function Level Access Control | 39 | 39 | 0 |
| Cross-Site Request Forgery (CSRF) | 3 | 1 | 0 |
| Using Components with Known Vulnerabilities | / | / | / |
| Unvalidated Redirects and Forwards | / | / | / |

This can be due to the insufficient attention which should be devoted to the proper implementation of web environment in which CMS systems are executed. However, improper configuration and implementation of security issues in the CMS systems can also lead to a number of other problems making CMS vulnerable. In relation to this vulnerability, Sensitive Data Exposure vulnerability also has high values. It can be concluded that to some extent these two vulnerabilities are related, bearing in mind that the exposure of sensitive data commonly occurs due to improper handling of these data and configuration of environment and CMS.

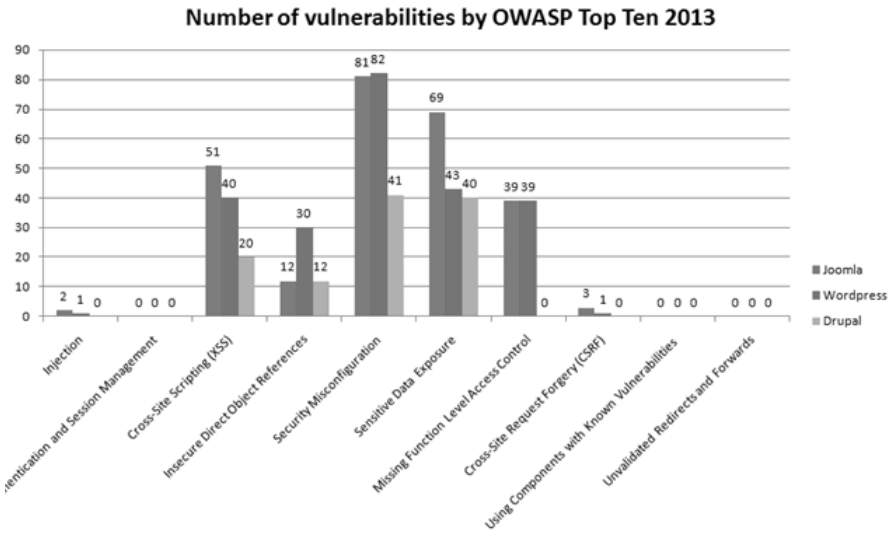



**Figure 4.** *Total percentage of vulnerabilities per category*

## CONCLUSION

In this paper we have analyzed current situation of security and vulnerabilities which can be found in popular CMS systems such as Joomla, Wordpress and Drupal. These types of web applications are often used for building educational websites because they enable easy creation and maintaining of content. As these categories have a large audience and rank on Web search, it is quite understandable and expected that they will attract attention of attackers. The analysis has identified vulnerabilities which were put in different categories depending on the risk level they have, which is done automatically via the tool used for detection of vulnerabilities. Results given in previous section show that small number of vulnerabilities were marked as high risk, while at the opposite side large number of vulnerabilities were marked as low risk.

For the purpose of minimization of the risk and prevention of attack, CMS systems need to be updated regularly along with web server, where client communication with the server should also be achieved via secured channels by using encryption as well as role-based access to control different parts of the website. Keeping in mind that use of CMS system is continuously increasing and that share of each CMS system may vary, one must not lose sight of the fact of raising the conscience about security in those systems. OWASP list of most common vulnerabilities can help in identification of new vulnerabilities which can affect CMS systems, but CWE[13], CVE[14] and CVSS[15] lists can be of great help in applying appropriate security patches in CMSS systems.

Further research in this area may lead to the identification of similar vulnerabilities that may be discovered in web applications and their grouping into a single category. For example,

13 CWE. (2017). Retrieved 2017, from Common Weakness Enumeration: https://cwe.mitre.org/.
14 CVE. (2017). Retrieved 2017, from Common Vulnerabilities and Exposures: https://cve.mitre.org/.
15 CVSS. (2017). Retrieved 2017, from Common Vulnerability Scoring System: https://www.first.org/cvss.

the "Cross-Site Scripting (XSS)" and "Web Browser XSS Protection Not Enabled" are vulnerabilities that can be grouped into a single category. Analysis of applications through these categories can give one new and more general view on this area.

## LITERATURE


1. Antón, A. I., Earp, J. B., & Reese, A. (2002). Analyzing website privacy requirements using a privacy goal taxonomy. *In Proceedings of the IEEE Joint International Requirements Engineering Conference* (pp. 23-31). Essen, Germany: IEEE.
2. *CVE*. (2017). Retrieved 2017, from Common Vulnerabilities and Exposures: https://cve.mitre.org/.
3. *CVSS*. (2017). Retrieved 2017, from Common Vulnerability Scoring System: https://www.first.org/cvss.
4. *CWE*. (2017). Retrieved 2017, from Common Weakness Enumeration: https://cwe.mitre.org/.
5. Erlingsson, U., Benjamin, L. V., & Yinglian, X. (2007). *End-to-End Web Application Security.* San Diego, USA: In Proceedings of the Workshop on Hot Topics in Operating Systems.
6. Felmetsger, V., Cavedon, L., Kruegel, C., & Vigna, G. (2010). Toward Automated Detection of Logic Vulnerabilities in Web Applications. *In Proceedings of the 19th USENIX Security Symposium* (pp. 143-160). Washington, DC, USA: USENIX.
7. Fonseca, J., & Vieira, M. (2008). Mapping software faults with web security vulnerabilities. *In Proceedings of the IEEE International Conference on Dependable Systems and Networks* (pp. 257-266). Anchorage, Alaska, USA: IEEE.
8. Fonseca, J., Vieira, M., & Madeira, H. (2007). Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks. *In Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing* (pp. 365-372). Melbourne, Australia: IEEE.
9. Huang, Y.-W., Yu, F., Hang, C., Tsai, C.-H., Lee, D. T., & Kuo, S.-Y. (2004). Securing Web Application Code by Static Analysis and Runtime Protection. *In Proceedings of the 13th international conference on World Wide Web* (pp. 40-52). New York, NY, USA: ACM.
10. Internet World Stats, U. a. (2016). Retrieved from World Internet Usage and Population Statistics: http://www.internetworldstats.com/stats.htm
11. Jerković, H., Vranešić, P., & Dadić, S. (2016). Securing web content and services in open source content management systems. *In Proceedings of the 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1644-1649). Opatija, Croatia: IEEE.
12. Milić, P., Kuk, K., Civelek, T., Popović, B., & Kartunov, S. (2016). The Importance of Secure Access to E-government Services. *In Proceedings of the International Conference "Archibald Reiss Days"* (pp. 307-3016). Belgrade, Serbia: Academy of Criminalistic and Police Studies.
13. *OWASP Zed*. (2016). Retrieved 2017, from OWASP Zed Attack Proxy (ZAP): http://www.zaproxy.org/
14. Project The Open Web Application Security. (2013). Retrieved 2016, from The Ten Most Critical Web Application: https://www.owasp.org/index.php/Top_Ten
15. Yang, Y., Kim, Y., Lim, Y., & Lim, H. (2016). A Comparison of Open-Source CMS and Analysis of Security Vulnerability. *INTERNATIONAL JOURNAL OF COMPUTERS, 10*, 82-86.

# CRIMINOLOGICAL AND CRIMINALISTIC CHARACTERISTICS OF COMPUTER CRIME IN THE REPUBLIC OF MACEDONIA

**Associate Professor Svetlana Nikoloska, PhD**
Faculty of Security – Skopje
svetlana.nikoloska@uklo.edu.mk

**Abstract:** The latest developments in the information technologies, beside the opportunities, involve a certain amount of weaknesses involving elements of abuse of such technologies and providing connection by means of computer systems and networking. The scope of abuse ranges from a sort of technical misconduct or abuse of insignificant size to wrongdoings entailing large consequences that cause a variety of damages and involve elements of crime. The crimes perpetrated via information technologies and involving abuse of computer systems and networks can be of national and international character. In the direction of detecting, disclosing, proving and preventing this type of crime, appropriate tactics, techniques and methods should be sought for the purpose of restraining computer crime, which is on the other hand quite different from the classical or economic crimes, in terms of instruments of execution, of object of criminal attack and conducting the criminal investigation in order to achieve relevant proofs, acceptable to the judicial authorities and the overall criminal procedure. Since the adoption of the first Criminal Code of the Republic of Macedonia in 1996, the recommendations deriving from international legal acts in the direction of incriminating typical computer crimes and crimes that can be executed in a classical manner, but including information technology and abuse of computer systems and networks, have been continuously implemented. Macedonian criminalist practice notifies a number of kinds and forms of computer crime in the last years, which represents a stimulus for investigating criminological and criminalist characteristics of computer crimes. This is also the subject of this paper, particularly paying attention to the scope, the structure and the dynamics of the reported, accused and sentenced perpetrators of computer crimes, and to the criminalist analysis of the most frequently perpetrated crimes, supported by several examples. This paper covers a period of five years (2011-2015 inclusive) that followed after the introduction of reforms to the Macedonian penal code of March 2010.

**Keywords:** computer crime, criminological characteristics, criminalist characteristics, criminalist practice, perpetrators.

## INTRODUCTION

In the history of the mankind, there is no other technological invention with a wider range of application or of greater influence on the changes in human living as is the case with the invention of computer. The changes caused by the information technology, which are genuinely obvious, can be viewed in the area of collecting, storing, processing and presenting of infor-

mation, turning the information into a strategic resource, which in the post-industrial era can be proved as valuable and influential as it was the capital in the industrial era. Thanks to this, the modern information and communication systems if used in an appropriate manner, can increase the efficiency of a really large number of activities.[1] The increased efficiency and the improved communication are actually the best benefit from the information technology development, both in the business sector and in the communication and exchange of information among state bodies and authorities enabling the transfer of information and exchange of data with the furthermost parts of the globe to be realized within a very short period of time.

The global virtual world has become a very convenient place for work and private communication and as such it also represents a beneficial opportunity for lots of people, thus becoming very attractive and interesting to the criminals, as well in the course of the 1990s. The skilful perpetrators of computer crime, or the so-called high-tech crime, skillfully made use of the Internet, which on the other hand turned out to be "the teacher of skills" to criminals in other areas and throughout the whole world. This bond between àthecriminals and the Internet has produced two types of high-tech crimes, such as: hacking the net and using the net as a means and place for perpetrating of other crimes. Thanks to the Internet, the international cooperation among the criminals is very easy. Broadening the horizons of acting and the numerous forms in which it appears, high-tech crime today sets new challenges that endanger the citizens, the collective security, as well as the economic stability of many countries.[2]

Beside all the advantages and benefits, the computer gradually grows into an instrument of abuse for certain unconscious individuals, groups, even criminal organizations. The dark side of the introduction of information technology is marked by countless accompanying phenomena with strong negative features due to which the contemporary society becomes more and more exposed to huge risks in a large number with gradually increased fragility and "vulnerability". And this is all about the possible, numerous intentionally and unintentionally caused troubles in the legal use of computer technology. Unintentional problems are usually within the range of common mistakes causing no serious damage or risk to the citizens, their property or personal security. But, the deliberate problem situations caused by people motivated to induce damage of various scopes, from endangering personal security and integrity of citizens to causing serious damage to the property to "satisfy" certain personal or group interests, permanently in the area of unlawful gain. The unlawful, illicit use or abuse of computer technology is acquiring increased criminal character, that is to say, the criminals are more and more directed towards perpetrating computer crimes, by involving minimum knowledge at lowest costs but gaining high criminal proceeds. At the same time, the criminals are getting more and more skills in doing this and in this way they achieve higher scores. Furthermore, they are skillfully getting appropriate means for the purpose of successful execution of the so-called classical crimes which saves their time and minimizes their risk when perpetrating a single or a serial crime, due to fewer traces left in the course of the action and less evidence produced. The latency of traces and evidence provide for criminals' "security" while performing the acts which means perpetrating crimes without being reported, suspected or disclosed and even prosecuted.

As the computer crime represents a modern form of crime, or crime supported by the progress in information technology, at the same time displaying features of organized crime, there are difficulties in locating and determining the most significant theoretical and practical problems related to its uncovering, proving, disclosing and prevention. It seems that the

1 Petrović S. , *Kompjuterski kriminal*, *drugo izdanje*, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2001, str. 2.

2 Urošević V. i Uljanov S. , *Uticaj karderskih foruma na ekspaziju i globalizaciju zloupotreba platnih kartica na Internetu,* NBP Žurnal za kriminalistiku i pravo, Kriminalističko – policijska akademija, Beograd, 2010 godina, str. 13.

criminal practice is before the theory, and it is so due to a simple reason of non-existence of theoretical knowledge systems and sub-systems at criminal method level[3]for fighting computer crime.

The manner in which the computer crime is executed and the degree of application of computer technology both as an instrument and as an object of criminal attack, compose the specifics of the type of crime. What makes the difference between this and classical and economic financial crimes, is actually the need to improve the specific research methodology related to computer incidents and to provide the electronic evidence in a specifically defined procedure requiring corresponding professional knowledge and skills in several scientific areas (informatics, law, criminology, forensics) that should end up in successful criminal investigation and adopting corresponding sanctions against the perpetrator(s). From the aspect of time and location of the crime, it acquires international dimensions and requires necessary international collaboration of two or more countries, at authorized state bodies of investigation level, to guarantee a unique procedure against the perpetrators based upon harmonization of national regulations of these countries.

The criminal investigation of computer crime is a complex procedure that requires professional knowledge in an array of scientific areas exclusively made possible through organized team work of competent professionals. By employing their professionalism, they are expected to contribute considerably to the successful planning, coordinating and conducting the investigation to uncover and prove the computer incidents involving elements of crime, as foreseen in the Criminal Code and above all to the provision of undisputable electronic evidence acceptable to the judiciary, both in the course of the criminal process and when reaching the verdict for the perpetrators, as well as if there is need for a parallel procedure for determining the type and size of the illicit property gain, or any other damage caused towards the victims of this kind of crime. In order to determine the kind and size of the illicit proceeds, financial investigation is taken in order to define the gained goods (type and size) by perpetrators of computer crime and to provide possible freezing and confiscating of the proceeds and property acquired via illegal criminal activity.

## THE CONCEPT AND FORMS OF COMPUTER CRIME

There are several definitions of computer crime which are basically reduced to the fact that it is a crime involving a computer as either an instrument or an object of the criminal attack. What makes this type of crime different from other forms of criminal behavior that can be organized within a frame of foreseeable behaviors, computer crime permanently assumes new forms and variations of criminal behavior, and accordingly new definitions of the concept of computer crime need to be upgraded. The computer crime is one common formulation encompassing various forms and kinds of criminal behavior. Namely, it is a crime directed against the security of information (computer) systems in general, or in particular involving various methods and various means in order to gain personal or benefit for third parties, or causing damage of some sort to others.[4]

The international community has recognized the issue of computer crime as a serious security problem, as a "benefit and quality" of the modern world and the rapid development of the information technology. In order to do a research into this security phenomenon, which

3 Ангелески М. , *Основни криминалистички теорески проблеми на борбата против организираниот криминалитет,* Научен проект: Конституирање на Република Македонија како модерна правна држава – на тема „Правната држава и организираниот криминал, Правен факултет – Скопје, 1996, стр. 110.

4 Јовашевиќ Д. , *Лексикон кривичног права*, ЈП Службени лист СРЈ, Београд, 2002.

in fact represents a serious danger manifested through numerous forms of criminal activities by a differentiated layer of perpetrators who use their knowledge, skills and abilities for criminal purposes, the term computer crime has to be defined first in line with determining the forms and types and the possible perpetrators. Primarily, the computer crime was defined as "any illegal act, for the successful realization of which knowledge of computer technology is considered indispensable".[5]

According to Sulejmanov "computer crime understands any activity involving the computer as an instrument of perpetrating a crime".[6]This definition has been broadened these days throughout the world to include several criminal activities related to the access to computer systems, computer fraud, computer forgery, computer espionage and sabotage and theft of computer time.

When defining computer crime, Slobodan Petrović[7] adopts the descriptive approach determining it as: destroying, damaging or alienating computer systems or their components; destroying, damaging, alienating and unauthorized alteration, publishing or using of data; perpetrating classical crimes; unauthorized use of computer resources and violation or decoding the protection shields.

The computer crime does not represent a "rounded phenomenological category" and due to this, it is completely impossible to come up with a uniquely acceptable definition of the term. Namely, the computer crime is rather a common form that is being manifested via various criminal variations.

In 2004 and 2009 the alterations and amendments to the Criminal Code of the Republic of Macedonia adopted a larger number of computer crimes incriminating them in accordance with the recommendations of the Computer Crime Convention of 2001 and the supplementary Protocol of 2003. According to the Criminal Code[8]and the chapter-classification, the following computer crimes have been defined:

- **ChapterXV–Crimes against human and civil rights and freedoms**

1. Endangering the safety – Art. 144 Para. 4;
2. Breaching the secrecy of letters or sealed packages –Art. 147;
3. Abuse and misuse of personal data - Art. 149;
4. Denial of access to public information system – Art. 149 – a;
5. Unauthorized wiretapping and recording – Art. 151;
6. Unauthorized camera recording – Art. 152;
7. Copyright and similar rights infringement– Art.157.
8. Infringement of the right of distributors of technically specifically protected satellite signals –Art. 157 – a;
9. Piracy of audio-visual works–Art. 157 – b.and
10. Piracy of phonographs–Art. 157 – c.

- **ChapterXVIII – crimes against integrity and respectability**

1. Insult – Art. 173para. 2;

- **Crimes against gender freedom and morality**

5 Николоска С. *Компјутерски кривични дела против слободите и правата на човекот и граѓаните во Република Македонија,* Хоризонти бр. 6, Битола, 2010, стр. 243.
6 Сулејманов З. ,*Криминологија*, Скопје, 2003, стр. 631.
7 Petrović S . , *op. cit*., str. 58.
8 Сл. весник на РМ бр. 37/96, 19/04, 07/08 и 114/09.

1. Displaying child pornography material –Art. 193,
2. Production and distribution of child pornography –Art. 193 – a.
3. Enticing a child under 14 years of age for the purpose of committing aggravated sexual assault of that child - Art. 193 –b

- **ChapterXXIII -Crimes against property**

1. Damaging and unauthorized accessing computer systems – Art. 251;
2. Creating and installing computer viruses – Art. 251 – a;
3. Computer fraud – Art. 251 – b.

- **ChapterXXV–Crimes against public finances, payment system and economy**

1. Creating, purchasing or alienating of means for forging – Art. 271 para. 2 and 3;
2. Payment card fraud – Art. 274 – b;
3. Infringement of the right to protected patent and a topography of integrated circuits – Art. 286.

- **ChapterXXXII–Crimes against legal traffic**

1. Computer fraud – Art. 379 – a.

- **ChapterXXXIII–Crimes against public order**

1. Terrorist organizationsArt. 394 – a;
2. Terrorism – Art. 394 – b;
3. Financial terrorism –Art. 394 – c;
4. Distribution of racist and xenophobic materials by means of using the computer system –Art. 394.

## SCOPE, STRUCTURE AND DYNAMICS OF COMPUTER CRIMES ACCORDING TO THE CRIMINAL CODE OF THE REPUBLIC OF MACEDONIA

"The evidencing, monitoring and suspending of crime and the introduction of prevention programmes and actions are immediately connected with the possession of empirically tested knowledge about the phenomenological characteristics of the crime. If the society is to confront this crime, then it must have a hold of scientifically tested notions about the phenomenon known as crime. Consequently, its massive occurrence necessarily selects statistical methods and procedures of evidencing, monitoring and processing of the collected data, as well as their presenting in a way to provide an opportunity for realizing the phenomenological characteristics, to identify the occurrence and relations of etiological meaning, and, based on the above, to setup crime prevention, elimination and eradication programmes".[9]The presentation and analysis of statistical data related to computer crimes are needed for comparing the most frequently perpetrated acts and for the process of disclosing and/or reporting, even sanctioning the suspects involved in this type of crime. The statistics are also important in the context of improving the process of criminal investigation and in the direction of paying attention to the forensics of providing electronic evidence acceptable for the judiciary and relevant to the confirmation of the crime in line with determining the degree of guilt of the perpetrators. Due to this, the Organization of the UN adopted the Dublin Declaration in 2003.

9Арнаудовски, Љ., *Методолошки проблеми на статистичкото евидентирање и следење на економскиот криминалитет,* МРКПК, бр. 2 - 3, Скопје, 2008, стр. 454.

The Declaration comprises ten recommendations, and the Sixth one determines the need for building a European system of crime statistics and adopting a strategy for producing information necessary for the analyzing and following the global tendencies related to this crime.

This paper analyzes and presents the data on the reported, indicted and convicted perpetrators of computer crimes, as foreseen in the Macedonian penal legislations and organized in separate sections in accordance with featuring the same or similar criminal characteristics.

In the investigated period 2011-2015, the Macedonian criminal and penal practice notices the execution of the incriminated acts as anticipated or in accordance with the Criminal Code of the Republic of Macedonia. Regardless of the crime section investigated, we have a situation of non-reporting the perpetrators. In practice, certain continuity in doing the same or similar crimes can be traced, and for that reason we present only the data related to the crimes involving cases of the reported, indicted or convicted perpetrators of computer crimes.

## Scope, structure and dynamics of the reported, indicted and convicted perpetrators of computer crimes

The statistical analysis of the data related to the reported, indicted and convicted perpetrators of computer crimes in the Republic of Macedonia for the investigated period between 2011 and 2015 has been carried out. According to the data collected at the State Statistical Office and extracted from the Annual Reports for the years 2011, 2012, 2013, 2014 and 2015, there are the reported, indicted and convicted perpetrators for the following types of computer crimes:

1. Abuse of personal data – Art. 149,
2. Unauthorized wiretapping and recording – Art. 151,
3. Copyright and similar rights infringement– Art. 157,
4. Infringement of the right of distributors of technically specifically protected satellite signals – Art.157 – a,
5. Piracy of audio-visual works–Art.157 – b,
6. Piracy of phonographs–Art. 157 – c,
7. Displaying child pornography material –Art. 193,
8. Production and distribution of child pornography –Art. 193 – a,
9. Damaging and unauthorized accessing computer systems – Art. 251,
10. Computer fraud – Art. 251 – b,
11. Payment card fraud–Art. 274 – b.

The data are categorized per year with separate tables displaying the number of the reported, the number of indicted and the number of convicted perpetrators, and then a comparative analysis of the indicted versus the reported and convicted versus the indicted and reported ratios is performed.

*Table 1: The reported perpetrators of computer crimes in the Republic of Macedonia between 2011 and 2015*

| Year | Art. 149 | Art.157 | Art.157 – a | Art. 157 – b | Art. 157 – c | Art.193 | Art.193 – a | Art.251 | Art.251 – b | Art. 274 – b | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2011 | / | / | 2 | 12 | / | **2** | **1** | 45 | / | **8** | **70** |
| **2012** | / | / | **5** | **1** | / | **6** | **2** | 23 | / | **11** | **48** |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **2013** | / | / | **12** | **1** | / | **3** | / | 41 | **5** | **16** | **78** |
| **2014** | **23** | **8** | / | / | / | / | / | 30 | / | / | 61 |
| 2015 | / | 9 | 3 | / | / | / | / | 50 | 2 | 13 | 77 |
| Total | 23 | 17 | 22 | 14 | / | 11 | 3 | 189 | 7 | 48 | 334 |

The data related to the 334 reported perpetrators of computer crime are shown in the table no. 1. 189 out of this total number, or 56.6% are reported as perpetrators of "Damaging and unauthorized accessing computer systems" crime, Art. 151; 46 or 14.4% as perpetrators of "Payment card fraud" crime – Art. 274 – b, whereas the rest as perpetrators of the remaining kinds of crime. The main motive of the perpetrators is unlawful gain of property that can be deduced based on the fact that the majority of perpetrators are indicted for performing crimes against property and financial crimes by utilizing their information knowledge for criminal purposes and gaining criminal proceeds. The data regarding the degree to which the prosecution authorities succeed in gathering evidence relevant to presenting the prosecution case are shown in the tables 2, 3 and 4. Namely, out of the total of 334 reported, 242, or 72.5% of the perpetrators have been indicted or tried, whereas 86.6% of them have been convicted, thus indicating the quality of evidence and the efficient crime investigation authorities that successfully planned and realized the whole process and managed to gather relevant evidence, mostly electronic and resulting from the team work and professionalism of approach.

As regards the crime dynamics and persecuting the perpetrators, it can be concluded that these crimes are processed for a shorter period of time as compared to other kinds of crimes, such as the classical economic and financial crime. Again, the electronic evidence material plays a special role in the process, and it is provided following a procedure defined with specific protocols and respecting the measures for provision and securing the evidence in the course of its adaptation for presentation at court.

*Table2: Indicted perpetrators of computer crimes in the Republic of Macedonia between 2011 and 2015*

| Year | Art. 149 | Art. 150 | Art. 157 | Art. 157 – a | Art. 157 – b | Art. 157 – c | Art.193 | Art.193 – a | Art.251 | Art.251 – b | Art.274 - b | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2011 | / | / | / | 4 | 15 | 1 | / | 1 | 9 | / | 7 | 37 |
| 2012 | / | / | / | 4 | 14 | 2 | 1 | / | 25 | / | 5 | 51 |
| 2013 | / | / | 1 | 4 | 3 | / | 1 | / | 33 | 3 | 8 | 53 |
| 2014 | 9 | 1 | 6 | 8 | 1 | / | / | / | 14 | / | / | 39 |
| 2015 | / | / | 12 | 3 | 1 | / | / | / | 20 | / | 26 | 62 |
| Total | 9 | 1 | 19 | 23 | 34 | 3 | 2 | 1 | 101 | 3 | 46 | 242 |

*Table3: Convicted perpetrators of computer crimes in the Republic of Macedonia between 2011 and 2015 +*

| Year | Art.149 | Art.157 | Art.157 – a | Art. 157 – b | Art. 157 – c | Art. 193 | Art. 193 – a | Art.251 | Art.251 – b | Art.274 –b | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2011 | / | / | 4 | 15 | 1 | / | 1 | 9 | / | 3 | 33 |
| 2012 | / | / | 1 | 13 | 2 | 1 | / | 21 | / | 1 | 39 |
| 2013 | / | 1 | 4 | 3 | / | 1 | / | 27 | 3 | 4 | 43 |
| 2014 | 7 | 6 | 7 | 1 | / | 1 | / | 14 | / | / | 36 |
| 2015 | / | 9 | 3 | 1 | / | / | / | 20 | / | 26 | 59 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Total | 7 | 16 | 19 | 33 | 3 | 3 | 1 | 91 | 3 | 34 | 210 |

*Table 4:Percentage of process efficiency with reference to the reported, indicted and convicted for a computer crime in the Republic of Macedonia between 2011 and 2015*

| **Year** | Reported | Indicted | | Convicted | | |
|---|---|---|---|---|---|---|
| | | Number | % | Number | % in relation to indicted | % in relation to convicted |
| 2011 | 70 | **37** | 52.9 | **33** | 89.2 | 47.1 |
| **2012** | 48 | **51** | 106.3 | **39** | 76.5 | 81.3 |
| **2013** | 78 | **53** | 67.9 | **43** | 81.1 | 55.1 |
| **2014** | 61 | **39** | 63.9 | **36** | 92.3 | 59.01 |
| **2015** | 77 | **62** | 80.5 | **59** | 95.2 | 76.6 |
| **Total** | 334 | **242** | 72.5 | **210** | 86.8 | 62.9 |

## CRIMINALISTIC CHARACTERISTICS OF COMPUTER CRIME

Computer crime, just like all other forms of crime, follows a specific modus operandi that is permanently being improved by the very perpetrators by introducing new elements related to the degree of using the computer technology and criminalist informatics. The location and the time of execution of the crime in response to the "two golden questions in criminology – where and when", diverge to some degree from the traditional criminology studies when compared to common or economic crimes. The location where the crime has been performed is related to the location of the computer used for the crime, but the criminal attack or the consequences from that attack can be felt in a very faraway place.[10] Very often the consequences are felt at the very moment of the criminal activity, but there are also cases of longer lasting activity with consequences following after a given period of time, simultaneously in several locations across the world (computer frauds).

The criminal investigation of computer crime is above all conditioned by the criminalist characteristics it displays and which should be studied referring to the following:[11]

- The mechanism of typical manners of executing and concealing computer crimes;
- The crime situation;
- The specifics regarding the creation and masking of typical traces and evidence – mostly electronic traces and evidence;
- The individual and personal characteristics of the perpetrator and those of the victim, and
- The specifics of searching and finding sources of criminalist information and creating the thesaurus for that purpose (the theses of investigating the crime act and the versions involved).

The criminal investigation in cases of computer crime is specific with regards to providing the electronic evidence, the range and application of special methods, tools and ways of providing the electronic evidence, but also the combination of digital and other material and ideal evidences for the purpose of disclosing and confirming the crime situation and identification of the perpetrator(s), and above all providing grounds for quality trial completed with appropriate sanction based on relevant and well-grounded evidence. A large problem is pres-

10 Бошковић М, *Криминалистичка методика I*, Полицијска академија, Београд, 1998, стр. 308 .
11 Ангелески М.,*Криминалистичка методика*, Скопје, 2008, стр. 111 – 112.

ent in the past years related to acceptance of digital evidence by the judiciary, i.e. the judges that are sort of prone to take more credit in material and ideal evidences. To put it in other words, the judges would rather have confidence in witnesses than digital evidence (as if there are suspicions or uncertainty about whether it should be considered as relevant evidence and in what way). However, the training for judges and prosecutors improves the condition when it comes to disclosing the crime situation involving elements of computer crime and including the measure of taking away the computers and/or programmes involved in the crime activity in order to extract the digital evidence stored in the computer memory.

According to most of the global studies, the best results for every computer incident are achieved based on team work involving experts in the area of criminology, criminal law and informatics, from the very moment of disclosing through to the presentation of the provided digital evidence, their analysis and the processed digital evidence in an acceptable form for the court. Still, not all experts in criminology or criminal law possess the corresponding competences for participation in the investigation processes for computer crimes. In such cases it is expected to have professionals from the units dealing with investigating computer crimes in the police, to include the public prosecutor as involved in the criminal law and an informatics expert experienced in police investigation related to the application of computer methods and techniques in extracting digital evidence. Informatics experts trained correspondingly in the area of criminology are also trained in criminalities way of thinking, or to achieve relevant digital evidence by employing the method of suspecting in close cooperation with professional police inspector specialized in computer crime.

The public prosecutor is part of the team in order for the provision of evidence to be lawful and pursuant to legal provisions to avoid the danger of erasing, concealing or "inappropriate handling of the extraction of evidence".

In investigating the crimes, the investigator usually seeks for the motive (why), the instruments (how) and the opportunity (when).

It would be ideal to have some overlap of the logical motive, the tools and the opportunity for committing the crime in question (why would someone do it, how was it done, when was it done) with the motive, the tools and the opportunity on the part of the indicted (why would s/he do it, how s/he did it, did s/he have the opportunity to do it).

It is often easer proved than done in cyber crimes. The motives are diverse, varying from curiosity to making money, gaining power and to revenge.

Today there is a growing number of unsatisfied workers, lots of jobless people and lots of fired people from work. Yet, this can sometimes be misleading. Very often most unsatisfied employees are the ones that do not even think of vandalizing the employer's computer system.[12]However, this cannot be overseen as a possible version and the practice shows linkages among the unsatisfied, the fired and the criminal structures that welcome the knowledge and skills as well as the data the former employees have.

The criminal investigation of computer crime is also known as computer forensics, because without the provision of relevant evidence, the perpetrator cannot be prosecuted and the damage done or the illicitly gained property cannot be evidenced. When criminally investigating the computer crime, operational police forces plan the primary measures, either individually or in cooperation with the Computer crime fighting unit in order to check the indicted, their movements, contacts, expenditure, etc. to provide the grounds for operational combinations of tactical measures investigating activities and special measures and activities with unique managing the case to identify the perpetrators, the involvement of domestic and/

12 Џејмс Х.С. и Норби Џ.Џ. , *Форензика, вовед во научни и истражни техники,* Табернакул, Скопје, 2009, стр. 557.

or international perpetrators and clarification of criminal activities, particularly clarifying whether the problematic activities in question share elements of computer or other forms of classical or economic crimes.

The pretrial (police) procedure plays a particularly important role in identifying, disclosing, proving and preventing the computer crime, above all in relation to obtaining relevant notions, primary information about the perpetrators, but also to the consequences of their criminal activities that are mainly manifested through piling up material goods by people that do not usually hold well paid job positions. The material consequences, in terms of movable and immovable property gains that cannot be easily achieved in a short period of time, are most often the starting point in disclosing and unveiling this type of crime.

The pretrial procedure is taken up in order to provide the public prosecutor with material needed to estimate whether the grounds for suspecting can grow into solidly founded suspicion, as a higher degree of suspecting based upon the collected evidence leading to the conclusion that certain person has committed a crime in order to later on file to the court for taking up a trial.[13]

According to the FBI (USA), the pretrial procedure in computer-related incidents is carried out in several phases, such as:

- Launching the investigation,
- Determining whether it is about a computer incident, and
- Analyzing the evidence.

The pretrial procedure has three stages as follows:[14]

The first stage involves: securing the location of the incident, evidence acquisition, hypothesis about the attack and investigating alternative explanations.

The second stage involves: incident analysis, analysis of the evidence gathered through the first one and the alternative solutions to determine whether we speak about a computer incident or something else (technical error, it is an incident, but does not bear the marks of a crime in accordance with the law etc.). The third stage involves analyzing the evidence, preparing a presentation of the computer incident including the evidence to present to the responsible authorities – the public prosecutor, who is to present the case to the criminal court.

The investigation procedure related to computer incidents generally incorporates the following:

- Checking the evidences, log data bases and every other information related to the suspect;
- Gathering information from people who could possibly have certain details related to the case;
- Controlling all investigation stages;
- Planning the search (locating the computer in question);
- Detailed inspecting the resources of the suspect (home, office, internet cafes etc.);
- Providing digital evidence and analyzing them.

The criminal investigation of computer incidents represents a step-by-step reaching the "truth". But, this should be conducted by applying the corresponding and lawful measures and activities, and because it is about a specific way of providing the evidence, the dedication is to

13 Калајџиев Г, *Казнено процесно право*, Скопје.
14 Николоска С., *Методика на истражување компјутерски криминал*, Ван Гог, Скопје, 2013, стр. 111.

be exactly in the direction of providing the evidence material that is of key importance to the further course of the investigation.

The first steps are undoubtedly related to several incidents and of course several versions. The first step to be taken should provide the answer to: Is it a crime or something else? Then, the next steps should be in function of providing the answers to the remaining eight golden rules of criminology, according to Peter Stevenson[15]:

1. Eliminating the obvious;
2. Formulating the hypothesis of the attack;
3. Reconstructing the crime;
4. Discovering the computer used to commit the crime;
5. Analyzing the computers that are the source and the target of the attack, as well as every other computer used as mediators;
6. Collecting evidence; taking the computers as well, if possible;
7. Handing out the conclusions and the evidence material to the investigators and to persons legally prosecuting the perpetrators (prosecutors).

The main focus of the investigation is of course put on the suspects, then on searching for the evidence and other traces, but it is clear that attention should be paid to collecting valuable information from the citizenship as a measure of explaining the circumstances and in function of disclosing and proving the case. The best combination in conducting the investigation related to computer incidents, involves the joint, team work of the prosecution authorities and experts in the area of informatics with special education in the area of criminology, or people who are to discover and extract the relevant evidence and assist in selecting the direct and indirect digital evidence.

Every participant in the investigation process acts in accordance with his/her legal authority and personal competences, professional knowledge, and in coordination with other involved persons and respecting their competences and knowledge.

**There is nothing like a superstar in the investigating of computer crime.**

What is needed is timely reacting, planning and acting.

## CONCLUSIONS AND RECOMMENDATIONS

The computer crime in the Republic of Macedonia is a realistic phenomenon involving elements of several crimes, with the same or similar characteristics. The Macedonian legislation has foreseen incrimination of a number of crimes as typically computer crimes, but of course this does not mean that they can only be executed using the computer as a means, using the computer systems and networks for transfer and abuse of information, or having the computer systems as main targets of a criminal attack.

According to the data obtained through the investigation, regarding the reported, indicted and convicted perpetrators, conclusions can be drawn that this kind of crime is being perpetrated due to various motives, and the object of attack are usually personal data, the data related to children and possible abuse in production of child pornography that is again distributed via the computer networks, leading to high criminal proceeds. According to the most frequently perpetrated, or crimes for which there are the largest numbers of reported and convicted perpetrators, it is the crime of "Damaging and unauthorized accessing com-

15 Џејмс Х.С. и Норби Џ.Џ. , *Форензика, вовед во научни и истражни техники,* Табернакул, Скопје, 2009, стр. 556.

puter systems" crime as per Art. 251, with 56% reported out of the total number of reported for computer crimes in the course of the period that has been investigated. This kind of crime was the first crime to be incriminated in the Macedonian Criminal Code in 1996 involving several different criminal behaviors. Furthermore, it has to be added that according to their experience the criminalists are almost always very cautious with regards to the classification of such criminal behaviors. Having in mind the essence of this crime, several types of the criminal behaviors related to it can easily be qualified with regards to other crimes as well. In the Republic of Macedonia, for a rather long period of time there was no record of incriminating a separate crime with the purpose of prosecuting the criminal perpetrators in relation to the payment card abuse. Criminologists tried to come to terms with providing evidence and proving that the perpetrators had unlawfully discovered data, and produced the fraudulent payment cards. This crime also involved certain criminal behaviors with elements of damaging computer systems and installing viruses. As a matter of fact, it is the efficiency of the criminologists, especially forensic experts in collecting electronic evidence and their processing and presentation for the purpose of successful trial and corresponding sanctioning the perpetrators. Namely, 72.5% out of the total of reported perpetrators are convicted, which means that in the course of the process criminalists have managed to raise the general suspicion to the level of specific suspicion by applying legal measures and activities in order to have the public prosecutor involved based on this suspicion and presenting the case in a criminal trial against the accused. 86.8% of the accused are convicted perpetrators, whereas the percentage of convicted out of all reported is 62.9. As I am interested in researching the economic crime in the Republic of Macedonia for a longer period, and computer crime is embedded within the economic crime, I can freely conclude that the efficiency of the prosecution is pretty high regarding the provision of undisputable evidence as estimated by the court in comparison to the overall economic crime where the percentage of conviction is about 12.7 for the period between 1997 – 2006. For the period between 2007 and 2013, there is an increase to 28.9%[16], but still it is pretty lower than the previously mentioned 62.9%. This is a comparison of the crime with the largest number of accused and convicted perpetrators according to the analysis of the period between 2007 and 2013, with 2017 perpetrators, 184 were accused, 110 convicted, whereas the percentage of convicted in relation to the reporting was 53.1 as compared to the recently obtained data according to which there were101 accused and 91 convicted, or 48.1% out of the total 189 reported. It is the obligation of criminalist and forensic experts in cooperation with the public prosecutor to respect the standard procedures and steps in providing evidence in the pretrial paying particular attention to following the rules for providing and keeping the electronic evidence which is of great importance in court in the course of reaching the verdict. The criminalist practice in the Republic of Macedonia with regards to computer crime is rather extensive having in mind that a special Sector for computer crime and digital forensics is in a process of development within the Organized Crime Unit and also the increased degree of awareness about the incidenceof computer crime, as well as about the development of skills, tactics and techniques for obtaining primary information about the computer incidents in line with increasing the professionalism of forensic workers and their role in providing relevant electronic evidence that can be adapted into a form acceptable for the court. Of great importance is the criminalist procedure developed via a planned approach and division of roles in the process of investigation, but also the team work in disclosing the cases and providing the evidence. It is proved that there is no such thing as "perfect crime", there are certain "omissions" and "oversights" in the course of the investigation that may sometimes mean missing to get hold of "solid, indisputable evidence" of key importance in court.

16 Николоска С., *Економска криминалистика*, Ван Гог, Скопје, 2015, стр. 96 – 97.

# BIBLIOGRAPHY

1. Ангелески М , *Основни криминалистички теореси проблеми на борбата против организираниот криминалитет,* Научен проект: Конституирање на Република Македонија како модерна правна држава – на тема „Правната држава и организираниот криминал, Правен факултет – Скопје, 1996.
2. Ангелески М., *Криминалистичка методика*, Скопје, 2008.
3. Арнаудовски, Љ., *Методолошки проблеми на статистичкото евидентирање и следење на економскиот криминалитет,* МРКПК, бр. 2 - 3, Скопје, 2008.
4. Јовашевиќ Д., *Лексикон кривичног права*, ЈП Службени лист СРЈ, Београд, 2002.
5. Кривичен законик на Република Македонија, Сл. весник на РМ бр. 37/96, 19/04, 07/08 и 114/09.
6. Николоска С. *Компјутерски кривични дела против слободите и правата на човекот и граѓаните во Република Македонија,* Хоризонти бр. 6, Битола, 2010.
7. Николоска С., Методика на истражување компјутерски криминал, Ван Гог, Скопје, 2013.
8. Николоска С., Економска криминалистика, Ван Гог, Скопје, 2015.
9. Petrović S., *Kompjuterski kriminal*, *drugo izdanje*, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2001.
10. Сулејманов З., *Криминологија*, Скопје, 2003.
11. Urošević V. i Uljanov S., *Uticaj karderskih foruma na ekspanziju i globalizaciju zloupotreba platnih kartica na Internetu,* NBP Žurnal za kriminalistiku i pravo, Kriminalističko – policijska akademija, Beograd, 2010.
12. Џејмс Х.С. и Норби Џ.Џ., *Форензика, вовед во научни и истражни техники,* Табернакул, Скопје, 2009.

# CYBER CRIME, VIRTUAL CURRENCIES AND FUTURE REGULATION

**Dijana Jankovic**, LL.D
Judge of the Appellate Court in Nis

**Abstract**: The Internet has created boundaryless territories and has helped in evolving a unique method to share and transfer information, in growth of e-commerce and in creating a global platform for all nations and its citizens. On the other hand, the Internet has spawned new forms of crimes and made old crimes easier to commit, such as cyber-stalking, identity theft, child pornography, fraud and scams, copyright violations, hacking and creating malicious code, the list goes on and on. The criminals use technological advancements to distance themselves from their illegal activities and profits through use of virtual banking and electronic money transfer systems, which allow criminals to buy, sell, and exchange counterfeit goods without any physical interaction. Though such services use digital logs that serve to identify a sender and a receiver's digital identities, criminals possess the means to obfuscate their digital identity by simply spoofing their Internet Protocol address or by using another individual's account, essentially making their activities untraceable. New virtual currencies, such as bitcoin, add yet another layer of anonymity by allowing users to transfer value without the collection of any personally identifiable information. Regulations often fail to affect such virtual currencies due to lack of foresight by the regulation writers, creating a legal grey area. Thus, criminals can continue to capitalize on technological innovation to bolster their illegal activities. Virtual currencies began creating controversy soon after their launch. This article investigates an increasingly important yet under-developed body of law: regulation of virtual currency. Furthermore, this article discusses bitcoin currency - like features and the first regulatory actions take in the European Union and in the United States of America. The goal of this paper is to raise awareness regarding legal and enabling technologies, which facilitate acts of cybercrime. In perusing these avenues of inquiry, the author seeks to identify impediments which obstruct police investigations, prosecutions, and digital forensics interrogations.

**Key words:** cybercrime, virtual currencies, bitcoin, criminal law, piracy.

## INTRODUCTION

The people all over the world work daily to create a better world. They create products and services that improve the world's ability to communicate, to learn, to understand diverse cultures and beliefs, to be mobile, to live better and longer lives, to produce and consume energy efficiently and to secure food, nourishment and safety. Most of the value of this work is intangible - it lies in people's entrepreneurial spirit, their creativity, ingenuity and insistence on progress and in creating a better life for their communities and for communities around the world. These intangible assets, often captured as copyrights, patents, trademarks, trade secrets and other forms of "intellectual property," reflect most developed countries' advantage in the global economy.[1]

1 Farah, P. D., Tremolada, R., *Intellectual Property Rights, Human Rights and Intangible Cultural Heritage*, Journal of Intellectual Property Law, Issue 2, Part I, 2014, pp. 21–47.

We are facing the digital challenge in the field of the infringement of the intellectual property. The Internet and other technological innovations have revolutionized society and the way we can obtain information and purchase products lowering barriers to entry and creating global distribution channels, they have opened new markets and opportunities for exports of information, goods and services, including enabling small and medium sized businesses to reach consumers worldwide. These innovations have also facilitated piracy and counterfeiting on a global scale.[2]The Internet has resulted in an effective new distribution channel for counterfeit goods.[3]All of this has enormously increased the number of counterfeit products on the market.

The aim of this paper is to investigate various aspects of the legal protection from online crime. Specifically, it is assumed that the cybercrime appears in different forms and as such is the subject to protection of many legal authorities. A special form of the violation rights is performed by the internet and computer data usage. In a broader sense, the suppression of illegal behaviour in the area of computer protection often includes the offenses that directly violate the rights protected by the intellectual property rights. In this paper, different forms of cybercrime by different law areas are analysed, with particular reference to a wide array of problems concerning of virtual currencies.

## CYBER CRIME IN THE INTERNET AGE

The Internet has created boundaryless territories and has helped in evolving a unique method to share and transfer information, in growth of e-commerce and in creating a global platform for all nations and its citizens. Online piracy is a major flipside to this development.[4]The Internet has become the first place of call for anyone in search of information, ideas or simple contact with like-minded people. Unparalleled opportunities also exist through social network sites, blogs and other interactive facilities for individuals to make information public about themselves, exchange opinions and share knowledge on every question. Infringement of copyright on the Internet has become a common phenomenon.[5] Infringement can take place either wilfully or through ignorance.

There is a close nexus between intellectual property and the Internet and their convergence in the digital era is inevitable.[6]The intellectual property - Internet nexus can be looked at from three perspectives – the author, the user and the service provider. An author creates a piece of work and registers it under the existing intellectual property laws to enjoy certain benefits, but the digital world hinders the complete enjoyment of these rights. Copyright owners perceive the Internet as threat to their exclusive rights due to the following reasons: (1) wide distribution is relatively simpler and quicker on the Internet; (2) anyone can distribute it to a mass audience; (3) the quality of copies is virtually indistinguishable from the original; (4) distribution is almost costless; and 4) users can easily and cheaply obtain copyright material on the Internet.[7]

2 Horan, A., Johnson, C., Sykes H., *Foreign Infringement of Intellectual Property Rights: Implications for Selected U.S. Industries*, Office of Industries U.S. International Trade Commission Washington, 2005.
3 Hadda, C., *Fake Drugs, Real Disaster*, Business Week, Feb. 9, 2004, p. 44.
4 Brenner, S. W., *Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?* Rutgers Computer and Technology Law Journal, No. 30, 2004, pp. 1-104.
5 Edwards, L., Waelde, C., *Law and the Internet*, 3rd edition, Hart Publishing, Oxford, 2000, p. 186.
6 Richet, J.L., From *Young Hackers to Crackers*, International Journal of Technology and Human Interaction, No. 9, 2013, pp.53-62.
7 Hemmige, N., *Piracy in the Internet Age*, Journal of Intellectual Property Rights, No. 18, 2013, pp 457-464.

Over the past years, the idea of how to reconcile intellectual property rights and the Internet technologies and platforms has become a pivotal point of all Internet governance discussions.[8] With the emergence of the Internet as a means of communication, creativity, innovation and ideas and with the increasing accessibility to information, traditional concepts of intellectual property appear increasingly antiquated and inapplicable in a space where information is democratized, people become increasingly more empowered to create exchange and distribute content and innovation and creativity proliferate.[9]The Internet has spawned new forms of crimes and made old crimes easier to commit, such as cyber-stalking, identity theft, child pornography, frauds and scams, copyright violations, hacking and creating malicious codes, the list goes on and on.[10]

In the course of the rising importance of the Internet in regards to daily communication in the middle of the 1990s, criminal prosecution authorities were increasingly faced with the phenomenon of data network criminality.[11]The internet and e-commerce have become major enablers for the distribution and sale of counterfeit goods. Counterfeiters are able to function across multiple jurisdictions, evading capture, and are also able to take down and set up new websites overnight without losing their customer base.[12]

Consumers are drawn to e-commerce sites because they are always available and items are delivered directly to consumers' homes. Online shopping can also be cheaper than shopping in retail shops, as there are no overheads in terms of rent, personnel, etc. Some websites are of such high quality and sophistication that they rival (and in some cases are even better than) those of the rights holder.[13]

The Bern Convention for the Protection of Literary and Artistic Works [14] establishes minimum rights.[15] Since 1996, the World Intellectual Property Organization (WIPO) and the signatories of the Berne Convention have been trying to develop a new international treaty, known as the Berne Protocol, to protect copyright holders in the digital context.

The United States of America has extended its copyright law and enacted the Digital Millennium Copyright Act (DMCA)[16] which came into force in 1998. The Act contains six exceptions to infringement including educational research, encryption research, protection of minors, reverse engineering, privacy of individuals and security testing. The DCMA added Section 512 specifically to the Copyright Act which brought forth the limitation

8 Brenner, S. W., Koops, B.-J., *Approaches to cybercrime jurisdiction*, Journal of High Technology Crime, 15(1), 2004, pp. 1-46.
9 Hunton, P., *The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation*, Computer Law & Security Review, 27, 2011, pp. 61-67.
10 Holt, T. J., *Exploring the Intersections of Technology, Crime and Terror*, Terrorism and Political Violence, 24(2), 2012, pp. 337-354.
11 Dörr, D., Janich, S.,*The Criminal Responsibility of Internet Service Providers in Germany*, M*ississippi Law Journal, 80* Miss. L.J. 1247, 2011, 1247-1261.
12 Schwartz, K. E., *Criminal Liability for Internet Culprits: The Need for Updated State Laws Covering the Full Spectrum of Cyber Customization*, Washington University Law Review, No. 87, (2009), pp. 407-436.
13 Reilly, D., Wren, C., Berry, T., March, *Cloud computing: Pros and Cons for Computer Forensic Investigators,*International Journal Multimedia and Image Processing, 1(1), 2011, 26-34.
14 Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886, completed at Paris on May 4, 1896, revised at Berlin on November 13, 1908, completed at Berne on March 20, 1914, revised at Rome on June 2, 1928, at Brussels on June 26, 1948, at Stockholm on July 14, 1967, and at Paris on July 24, 1971, and amended on September 28, 1979.
15 Kahandawaarachchi,T., *Liability of Internet Service Providers for Third Party Online Copyright Infringement: A Study of the US and Indian Laws*, Journal of Intellectual Property Rights Vol 12, November 2007, pp 553-561.
16 The Digital Millennium Copyright Act (DMCA) of 1998, US Copyright Office Summary December 1998, Pub. L. No. 105-304, 112 Stat. 2860, Oct. 28, 1998.

of liability on the service providers in case of online copyright infringement and assigned rule in case of non-profit educational institutions.

Louis Vuitton successfully sued Akanoc Solutions Inc., Managed Solutions Inc. and Steven Chen[17] for "their role in ousting websites that directly infringed Louis Vuitton's trademarks and copyrights". Although the websites did not directly sell the counterfeit merchandise, they listed an email address allowing customers to initiate a transaction. Louis Vuitton was able to prove wilful intent, as they had sent the defendants 18 notices of trademark and copyright infringement. The jury awarded Louis Vuitton USD 10.5 million in statutory damages for wilful trademark infringement of the 13 trademarks against each defendant, for a total of USD 31.5 million, plus USD 300 000 for statutory damages for wilful copyright infringement and infringement of 2 copyrights against each defendant, totalling USD 900.000.[18]

In the United Kingdom the Digital Economy Act of 2011[19]came into force in June 2012 which covered the subjects that deal with digital encroachment of intellectual property, namely, copyright infringement, television services, radio services, regulation of the same, etc. With respect to copyright the Act involves two major parties – the Internet service providers and copyright holders.[20]

Despite various laws protecting intellectual property, it is still an enormous task to keep a check on the copyright infringers on the Internet.

## CYBER CRIME AND VIRTUAL CURRENCIES

The nature of virtual currencies is difficult to apprehend, the underlying technology is complicated, their operations are conducted in a decentralized way, and they are almost unregulated. No one can predict if a particular virtual currency may become a direct competitor for existing currencies in the distant future, or if it might just collapse overnight.[21]

However, some danger might arise for intellectual property and payment systems, including reputational damage for systems which are not directly exposed to virtual currencies. The most problematic field is consumer protection, as there are no safety nets, such as deposit guarantee funds, available to alleviate losses.

Extending prudential supervision to virtual currencies might be difficult, if not impossible, so most regulators are now pondering how to regulate the points of contact between virtual currencies and fiat money, i.e. where one is exchanged for the other.[22] The Paris terrorist attacks in late 2015 have revived interest in virtual currencies, as there is a growing fear that

17 Case Nos. 10–15909, 10–16015 Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., Managed Solutions Group, Inc.,Steven Chen [2011] United States Court of Appeals, Ninth Circuit, Decided: September 09, 2011.

18 More details of this case can be found through the publication United States Court of Appeals for the 9th Circuit case number: 10- 15909 D.C. No. 5:07-cv-03952-JW and No. 10-16015 D.C. No. 5:07-cv-03952-JW Opinion, 9 September 2011.

19 Digital Economy Act of 2010, UK National Archive.

20 Mansell, R., Steinmueller W. E., *Copyright Infringement Online: The Case of the Digital Economy Act Judicial Review in the United Kingdom*, Originally presented at the Communication Technology & Policy Section, International Association for Media and Communication Research Conference, 13-17 July 2011, IAMCR.

21 Tu, K. V., Meredith M. W., *Rethinking Virtual Currency Regulation In The Bitcoin Age*, Washington Law Review, No. 90, 2015, pp.270-347.

22 Financial Action Task Force-FATF, *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services,* FATF, Paris, 2013, p.21.

they could be used with criminal intent.[23] The European legal framework should be adapted to take the terrorist threat into account.[24]

The criminals use technological advancements to distance themselves from their illegal activities and profits through use of virtual banking and electronic money transfer systems, which allow criminals to buy, sell, and exchange counterfeit goods without any physical interaction.Though such services use digital logs that serve to identify a sender and a receiver's digital identities, criminals possess the means to obfuscate their digital identity by simply spoofing their Internet Protocol address or by using another individual's account, essentially making their activities untraceable.[25]

New virtual currencies, such as Bitcoin, add yet another layer of anonymity by allowing users to transfer value without the collection of any personally identifiable information.[26]Regulations often fail to affect such virtual currencies due to lack of foresight by the regulation writers, creating a legal grey area. Thus, criminals can continue to capitalize on technological innovation to bolster their illegal activities.[27]

Bitcoin was first introduced in a "white paper" by an anonymous author (or authors) under the pseudonym "Satoshi Nakamoto" in 2008.[28] Although the origins of Bitcoin remain mysterious, this decentralized digital currency has gained popularity worldwide. Satoshi Nakamoto's paper presented the electronic cash system as a challenge to the existing financial institutions that process payments. Bitcoin operates on a peer-to-peer network,[29] akin to file sharing services, in which participants collaborate to develop the network by sharing records of Bitcoin transactions.

While there is a public record and chain of custody of each Bitcoin, the identity of the owner may remain concealed, which is why it is sometimes described as "pseudonymous," rather than truly anonymous.[30] Bitcoins are initially generated by a process called "mining," in which computers solve complex math problems based on cryptography, rewarding the "miners" with Bitcoins. The cryptographic algorithm applied by miners is known as SHA-256. Miners subsequently can distribute the Bitcoins to third partiesthrough electronic wallets. Nakomoto's paper mapped out how Bitcoin prevents double spending, but referenced the possibility that a "greedy attacker" could disrupt the system

These transactions are verified by network nodes and recorded in a public distributed ledger called the blockchain, which uses Bitcoin as its unit of account.[31] Since the system works

23 Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing, COM (2016) 50 final, 2 February 2016.
24 Scheinert, C., *Virtual currencies Challenges following their introduction*, EPRS-European Parliamentary Research Service, Briefing, 2016, pp. 1-10.
25 Bennett, D, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations*, Information Security Journal: A Global Perspective, 21(3), 2012, pp.159-168.
26 Krohn-Grimberghe, A., Sorge. C, *Bitcoin: Anonym Einkaufenim Internet?* University of Paderborn, Department 3 - WirtschaftsinformatikAnalytischeInformationssysteme und Bl, Germany, 2012, s.3.
27 Bryans, D., *Bitcoin and Money Laundering: Mining for an Effective Solution*, Indiana Law Journal, No.89, 2014, pp. 441-472.
28 Despite many efforts, the identity of Satoshi remains unknown to the public and it is not known whether Satoshi is a group or a person. Satoshi in Japanese means "wise" and someone has suggested that the name might be a portmanteau of four technology companies: SAmsung, TOSHIba, NAKAmichi, and MOTOrola. Others have noted that it could be a team from the National Security Agency (NSA) or an e-commerce firm.
29 Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*,
URL=https://bitcoin.org/bitcoin.pdf , Accessed 1 January 2017.
30 Feuer, A., *Prison May Be the Next Stop on a Gold Currency Journey*, N.Y. Times, Oct. 25, 2012,
31Szczepański, M., Bitcoin: Market, economics and regulation, European Parliament Research Service (EPRS), European Parliament, 2014, pp. 1-9.

without a central repository or single administrator, the U.S. Treasury categorizes Bitcoin as a decentralized virtual currency. Bitcoin is often called the first cryptocurrency, although prior systems existed and it is more correctly described as the first decentralized digital currency. Bitcoin is the largest of its kind in terms of total market value.[32]

Bitcoin's image is polarized. Some view it as a tool used by criminals to commit crimes, whereas others view it as a tool for a legal system of currency that is free from unlawful government interference.[33]

Its proponents argue that bitcoin has many properties that could make it an ideal currency for mainstream consumers and merchants. For example, bitcoins are highly liquid, have low transaction costs, can be used to send payments quickly across the internet, and can be used to make micropayments. This new currency allowing organizations to receive donations and conduct business anonymously.[34]

On the other hand, bitcoin's decentralization and peer-to-peer infrastructure allows it to be virtually immune to the risks of server raids or the loss of a central database to hackers.

In October 2013 (USA), prosecutors filed a criminal complaint in the Southern District of New York and obtained a grand jury indictment in the District of Maryland against Ross William Ulbricht, owner of the Silk Road website (Silk Road). The Silk Road was a secret marketplace where illegal goods and services could be purchased online with bitcoins. The Silk Road operated on a Tor network, which allowed users to conceal their Internet Provider addresses and identities.

Once users gained access to the network, they could purchase various drugs, guns, fake drivers' licenses, pirated media content, malware, computer-hacking services, and even murder for hire or "hitmen." As alleged, Ulbricht himself offered an undercover federal agent $80,000 to murder a Silk Road employee who was arrested and whom Ulbricht feared would expose the network.

The Southern District of New York criminal complaint charged Ulbricht with narcotics trafficking conspiracy, computerhacking conspiracy, and money-laundering conspiracy. The Maryland indictment included counts for conspiracy to distribute a controlled substance and for attempted witness murder and attempted commission of murder for-hire. Total sales on the Silk Road purportedly generated the equivalent of about $1.2 billion in revenue and $80 million in commissions. The FBI has seized over $164 million worth of bitcoin from the website.[35]

Subsequently, charges were brought against two defendants who operated services exchanging dollars for bitcoins and knew the bitcoins were being used to purchase illegal goods and services on the Silk Road. The complaint identified numerous incriminating e-mails from Charlie Shrem, who served as chief executive officer of a money exchange service, and alleges that Shrem deliberately violated the company's anti-money laundering policies in order to earn profits.

Robert Faiella, whose identity was not known to Shrem, operated a bitcoin exchange service on the Silk Road under the user name "BTCKing." Faiella used Shrem's company's

32 Kaplanov, N. M., *Nerdy Money: Bitcoin, the Private Digital Currency and the Case against Its Regulation*, Loyola Consumer Law Review, 25, no. 1 , 2012, pp. 110-174

33 Ron, G. D, Shamir, A., *Quantitative Analysis of the Full Bitcoin Transaction, Quantitative Analysis of the Full Bitcoin Transaction Graph*, Department of Computer Science and Applied Mathematics, The Weizmann Institute of Science, Israel, 2012, p.12.

34 Grinberg, Reuben, *Bitcoin: An Innovative Alternative Digital Currency*, Yale Law School, Hastings Science & Technology Law Journal, Vol. 4, December 9, 2011 pp.160-208.

35 Gerkis, J. P., Krikunova, S., *Bitcoin and Other Virtual Currencies: Approaching U.S. Regulatory Acceptance*, Administrative & Regulatory Law News, American Bar Association,Vol. 39, No. 3, 2014, pp 4-9, 5.

services to maintain his anonymity and facilitate dollar-to-bitcoin exchanges on behalf of Silk Road users. Both have pleaded not guilty. The action demonstrated that merely having anti-money laundering policies in place is insufficient; rather, regulators will demand a strong practice of compliance and will not tolerate transgressions.

Also, the prosecutors in the Northern District of Illinois entered into a plea agreement with the defendant Cornelias Jan Slomp, a citizen of the Netherlands, for selling and importing massive amounts of drugs through the Silk Road website. Slomp's fingerprints were cross-referenced in a criminal database as authorized by a Mutual Legal Assistance Treaty with the Netherlands; he was subsequently arrested upon arrival in Miami.[36]

Major concern regarding bitcoin is its use in money laundering, tax evasion, trade in illegal drugs, child pornography and financing terrorist activity. These concerns were stoked also after the Liberty Reserve, a private and centralized digital currency was shut down on money laundering concerns. Interestingly, while prosecutors have previously stopped alternative private currencies dead in their tracks, the government's treatment of Bitcoin has recognized its legitimate uses. In 2011, a federal jury in North Carolina convicted the Liberty Dollar founder, Bernard von NotHaus, for making, possessing, and selling his own coins under 18 U.S.C. §§ 485 and 486.Unlike bitcoins, Liberty Dollar coins resembled U.S. coins in that they were marked with the dollar sign, and the words "dollar," "USA," "Liberty," and "Trust in God." NotHaus continues to challenge the verdict.

More recently, a co-founder of another virtual currency, Liberty Reserve, pleaded guilty to money laundering violations alleged for his role in the creation and operation "of an anonymous digital currency system that provided cybercriminals and others with the means to launder criminal proceeds." Conversely, the charges against Silk Road founder Ulbricht noted that "bitcoins are not illegal in and of themselves and have known legitimate uses."

On September 19, 2016, the U.S. District Judge Alison J. Nathan of the Southern District of New York denied the defendant Anthony R. Murgio's motion to dismiss charges brought against him for, among other things, operating a bitcoin exchange in violation of federal and state money transmitting laws. The decision adds to a growing body of federal precedent upholding the application of money transmitting laws to bitcoin exchange businesses.[37]

The indictment against Murgio specifically alleges that the bitcoin exchange he allegedly ran — Coin.mx — was an "unlicensed money transmitting business" in violation of 18 U.S.C. § 1960 (Section 1960). Section 1960 defines "money transmitting" to include "transferring funds on behalf of the public by any and all means." In moving to dismiss the indictment, Murgio argued that (i) bitcoin does not qualify as "funds"; (ii) exchanging bitcoin does not involve "transferring" customers' fundsto other persons or places; and (iii) operating a bitcoin exchange in the state of Florida, where Coin.mx operated, does not require a license. Judge rejected each of Murgio's arguments.

First, the court found that bitcoin does constitute "funds" within the plain meaning of that term. Rejecting Murgio's contention that "funds" refers only to "currency," Judge found that the term instead encompasses any "pecuniary resources" that can be used as a "medium of exchange," and that bitcoin meets that description. Second, Judge refused to dismiss the indictment based on Murgio's contention that Coin.mx acted merely as a seller of bitcoin and not as a "transmitter" of funds. Third, as for Murgio's argument that Coin.mx did not require a license to operate, Murgio cited a recent trial court decision in a Florida case - *Florida v. Espinoza* - holding that Florida's licensing requirement for money transmitters does not

36 Ibid, op.cit. p.6.

37 Latham & Watkins, White Collar Defense and Investigations Practice and Financial Institutions Industry Group, *Bitcoin Again Held to Be "Funds" for Federal Money Transmitting Purposes*, September 23, 2016, Number 2016.

apply to bitcoin exchangers. After carefully considering the analysis in Espinoza, the Judge found it unconvincing. The Judge concluded that the Florida Supreme Court, if faced with the question, would hold that Florida's money transmitting statute does indeed apply to bitcoin exchange businesses. In support of this conclusion, the Judge noted that the Espinoza court did not sufficiently analyse or explain why a bitcoin exchanger would not qualify as a seller of "payment instruments" - one of the types of businesses to which Florida's licensing requirement applies - given that the term is defined to include any type of "monetary value".[38]

The Murgio decision reflects a growing judicial consensus around the application of state and federal money transmitting laws to Bitcoin exchangers. The decision, however, does leave one issue open - whether merely exchanging bitcoins for fiat currency involves the "transfer" of funds within the meaning of Section 1960. Depending on the government's evidence, the issue may or may not prove significant at trial.

One of the most common initial questions about Bitcoin is whether the online currency is legal, given the government's monopoly on issuing legal tender.[39] Current law and regulation does not envision a technology like bitcoin, so it exists in something of a legal grey area. This is largely the case because bitcoin does not exactly fit the existing statutory definitions of currency or other financial instruments or institutions, making it difficult to know which laws apply and how.

The legal status of bitcoin varies substantially from country to country and is still undefined or changing in many of them.[40]While some countries have explicitly allowed its use and trade, others have banned or restricted it. Likewise, various government agencies, departments, and courts have classified bitcoins differently.

In the USA the federal reference is the regulatory guideline issued in by the Financial Crimes Enforcement Network (FinCEN), which is an agency within the U. S. Treasury Department. FinCEN distinguishes between "users", "administrators", and "exchangers". A user of convertible digital currency is not a money service business (MSB) under FinCEN's regulations and therefore is not subject to registration, reporting, and record-keeping regulations. However, an administrator or exchanger which accepts and transmits or buys and sells convertible digital currency is a money service business and specifically a money transmitter, unless in some exceptional cases. Money service business must enforce Anti-Money Laundering (AML) and Know Your Client (KYC) measures. Anti-Money Laundering and Know Your Client are generally applied to all financial intermediaries in the business of currency exchange and they have been extended to people or business dealing with digital currencies.[41]

On March 25, 2014, the Internal Revenue Service (IRS) provided guidance that treats "convertible virtual currency" like bitcoin as property and subjects it to the capital gains tax. This adds additional hurdles to miners, exchanges, merchants, payment processors,employers, and some consumers, while it generally is recognized as beneficial for investors.

38 Case 1:15-cr-00769-AJN, Document 198, Filed 09/19/16, Page 1 of 36, United States District Court Southern District of New York, September 19, 2016,
URL= https://cdn.arstechnica.net/wp-content/uploads/2016/09/murgio-order.pdf , Accessed 20 May 2017.
39 He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., SaadiSedik, T., Stetsenko, N., Verdugo-Yepes, C.,*Virtual Currencies and Beyond: Initial Considerations*, IMF Staff Team, International Monetary Fund, Monetary and Capital Markets, Legal, and Strategy and Policy Review Departments, 2016, p.16.
40 Financial Action Task Force-FATF, *Guidance for a Risk-Based Approach to Virtual Currencies*, FATF, Paris, 2015, p.12.
41 Tasca, P., *Digital Currencies: Principles, Trends, Opportunities, and Risks*, Deutsche Bundesbank and ECUREX Research, University of Zurich, Department of Banking and Finance, 2015, p.49.

The situation in Europe is very different compared to the USA. There is hardly any specific law, directives or regulations on digital currencies at the EU level. Moreover, single member states have continuously provided new regulatory guidance by often adopting different approaches on the topic. In this regards, the European Banking Authority (EBA) highlights the need to define, in the long term, a harmonised regulatory framework which secures the operation of digital currencies to authorized subjects and defines, among other things, the requirements for capital and governance of market participants and the separation of customer accounts from business accounts. In the short term, the EBA identified the urgent need to mitigate the risks arising from the interaction between the digital currency schemes and regulated traditional financial services.

According to the European Central Bank, traditional financial sector regulation is not applicable to bitcoin because it does not involve traditional financial actors.[42]Others in the EU have stated, however, that the existing rules can be extended to include bitcoin and bitcoin companies.[43]

In October 2015, the European Court of Justice ruled that bitcoin transactions are exempt from consumption tax similarly as traditional cash. Europe's highest court ruled in response to a request by Swedish tax authorities (Case *Skatteverket v. David Hedqvist*), who had argued bitcoin transactions should not be covered by a European Union directive exempting currency transactions from value added tax (VAT).The court ruled that bitcoins should be treated as a means of payment, and as such were protected under the directive. "Those transactions are exempt from value added tax under the provision concerning transactions relating to currency, bank notes and coins used as legal tender", the European Court of Justice concluded.[44]

The National Bank of Serbia (NBS) issued a statement advising that bitcoin is not legal tender in Serbia and cannot be subject to sale and purchase by banks and licensed exchange dealers.[45]

Bitcoin crimes are likely to emerge as an important significant phenomenon thereby forcing the relevant stakeholders to look at appropriate legal frame works which can effectively regulate certain activities.

## THE FIGHT AGAINST CYBER CRIME IN SERBIA

The Republic of Serbia signed both the Convention and the Protocol in Helsinki on April 7, 2005, at the time of the State Union of Serbia and Montenegro, and the National Parliament of the Republic of Serbia ratified both documents in 2009.[46] The compulsory application of the Convention commenced in August 2009. The mentioned documents served as a legal

42 European Central Bank, *Virtual Currency Schemes*, Frankfurt am Main: European Central Bank, October 2012, URL= http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. Accessed 1 January 2017.
43 Szczepański, M., *Bitcoin: Market, economics and regulation*, European Parliamentary Research Service, Annex B: Bitcoin regulation or plans therefor in selected countries, Members' Research Service, November 2014, pp. 2-9.
44 *Bitcoin currency exchange not liable for VAT taxes: top EU court*, Reuters, 22 October 2015, URL= http://www.reuters.com/article/us-bitcoin-tax-eu-idUSKCN0SG0X920151022 .Accessed 6 January 2017.
45 Fletcher, K., National Bank of Serbia states Bitcoin is not legal tender in country , CoinReport , 09 October 2014, URL= https://coinreport.net/national-bank-of-serbias-states-bitcoin-is-not-legal-tender-in-country/. Accessed 6 January 2017.
46 Act of Formal Confirmation of the Convention on Cybercrime, „Official Gazette of the Republic of Serbia" no. 19/2009

basis for domestic laws and standards, as well as for establishing specialized state bodies to combat cybercrime in general.[47]

The most important regulations adopted and adjusted to the provisions of the Convention include: the Criminal Code,[48] the Law on the Liability of Legal Entities for Criminal Offences,[49], Criminal Procedure Code,[50] the Law on Special Measures for the Prevention of Crimes against Sexual Freedom Involving Minors,[51] the Law on Seizure and Confiscation of the Proceeds from Crime,[52] and the Law on Special Authorizations for Efficient Protection of Intellectual Property.[53]

Serbia has set up specialized units (high-tech crime prosecutor, police cyber unit, specialised customs unit, tax unit and tax police) aimed at enforcing the legislation in this area. The length of investigations has been shortened. It fully updated an electronic database of customs offences in the field of intellectual property rights and introduced electronic handling of requests for protection of intellectual property rights. Along with the development of information technologies, the issue of legal regulations that can prevent and sanction cybercrime has gained significance.[54]

The Criminal Code of the Republic of Serbia regulated criminal offences regarding violation of computer data security, thus clearly contributing to a more efficient fight against cybercrime. Still, this regulatory framework did not fully embrace the deviant forms of behaviour manifested as misuse of computer technologies and computer systems (e.g. Internet harassment, unauthorized alteration of the contents published on the Internet, etc.).

Cybercrime Unit has been established within the Ministry of Interior of the Republic of Serbia: Cybercrime Unit for combating cybercrime. The Unit acts upon requests of the Special Prosecutor's Office, in accordance with the law the Department for Electronic Crime and Department for Combating Crime in the area of Intellectual Property as organizational parts for performing duties in regard to more specific areas of cybercrime combating were also established within the Cybercrime Unit.

The Higher Prosecutor's Office in Belgrade has the jurisdiction for the territory of the Republic of Serbia to proceed in cybercrime matters. The Higher Prosecutor's office established special cybercrime department - Special Prosecutor's Office. In the Higher Court in Belgrade a Cybercrime Department is established which has first-instance jurisdiction in cybercrime matters for the territory of the Republic of Serbia.

Criminal offences against security of computer data defined by the Criminal Code of the Republic of Serbia are the following: 1. Damaging Computer Data and Programs, 2. Computer Sabotage, 3. Creating and Introducing of Computer Viruses, 4. Computer Fraud, 5.

47 Spasić, V., *Savremeni oblici piraterije u autorskom i srodnom pravu*, Pravni život 56 (513), 207, 293-309. (Contemporary forms of piracy and copyright act and other regulations).
48 Criminal Code, "Official Gazette of the Republic of Serbia" no.85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016.
49 Law on the Liability of Legal Entities for Criminal Offences, "Official Gazette of the Republic of Serbia" no.97/2008.
50 Criminal Procedure Code, "Official Gazette of the Republic of Serbia" no. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014.
51 Law on Special Measures for the Prevention of Crimes against Sexual Freedom Involving Minors, "Official Gazette of the Republic of Serbia" no. 32/2013.
52 Law on Seizure and Confiscation of the Proceeds from Crime, "Official Gazette of the Republic of Serbia" no.32/2013.
53 Law on Special Authorizations for Efficient Protection of Intellectual Property, "Official Gazette of the Republic of Serbia" no. 46/2006 and 104/2009.
54 Vida M. Vilić, *Criminal Law Protection of Personality: Implementation of Council of Europe's Convention on Cybercrime No. 185 Of 2001 Into Serbian Legislative*, International Scientific Conference on Ict and E-Business Related Research, Doi: 10.15308, Sinteza, 2016, pp. 66-73.

Unauthorized Access to Computer, 6. Computer Network or Electronic Data Processing, 7. Preventing or Restricting Access to Public Computer Network, 8. Unauthorized Use of Computer Network, 9. Manufacture, Procurement, and Provision to Others of Means of Committing Criminal Offences against Security of Computer Data.

Act Amending Criminal Law[55] prescribesa new criminal act of persecution (stalking). Stalking has become the established term for acts of persistent persecution that cause its victims psychological strain. They include daily phone calls to victims' homes (also during night-time) or workplaces, "waylaying", bombarding with letters, emails and SMS messages, unwanted gifts, as well as spreading disparaging rumours, psychological harassment, threats, physical violence and sexual assaults.

Thanks to the introduction of Article 138a (Criminal Code) entitled "Persecution" it is now possible to counter the psychological terror caused by various forms of persistent persecution by resorting to criminal law. Behaviour is deemed persistent if sustained over a longer period. It is liable to punishment if it interferes with the victim's life to an unacceptable degree and can be counted in judicial practice among the following behavioural patterns, e.g.:

- Trying to be close to the victim (e.g. following by car, waylaying at home or in the workplace);

- Contacting by telecommunication or any other means of communication or via third parties (e.g. frequent letters, emails or text messages);

- Ordering goods or services for the victim by using the latter's personal data (e.g. clothes from a mail-order company);

- Inducing third parties to contact the victim by using the latter's personal data (e.g. placing contact ads on behalf of the victim).

The basic form of the criminal act can be punished by imprisonment of up to three yearsor fine.

Besides criminal offences that are listed in the Criminal Code of the Republic of Serbia, the Law on the organization and competences of government authorities combating cybercrime[56] also regulates this legal matter and, additionally, widens the scope of criminal offences which are deemed to be cybercrime, and those are criminal offences against intellectual property, property, economy and legal instruments, where computers, computer systems, data and products thereof appear as the objects or the means of committing a criminal offence and if the number of items of copyrighted works is over 2000, or the amount of the actual damage is over 1.000.000,00 RSD, as well as criminal offences against freedoms and rights of man and citizen, sexual freedoms, public order and constitutional system and security, which can be considered, due to the manner in which they are committed or tools used, as cybercrime offences.

In Serbia the most common forms of cybercriminal are related to Internet auction sites (e-shop), abuse of credit cards, phishing and identity thefts, "Nigerian" or "419" scams, and the most common infringements by the Internet frauds are copyrights.

The regional character of some types of cybercrime results from the specific features of the South-Eastern European region, particularly the Western Balkans, where connections are established based on the similarities among languages, cultures, ethnic backgrounds, and family and friendly ties. This has resulted in the establishment of some Internet services of regional influence and enabled abuse through collaboration and use of the same *modioperandi* in the misuse of the Internet. Perpetrators are mostly young men with no criminal background and

55 Act Amending Criminal Law, "Official Gazette of the Republic of Serbia" no. 94/2016.
56 Law on the organization and competences of government authorities combating cybercrime, "Official Gazette of the Republic of Serbia No 61/2005 and 104/2009".

with special technical and technological know-how, while organized groups mostly engage in the violation of computer data security. A high victimization risk results from insufficient awareness of the necessary measures of protection and actions necessary for the appropriate functioning of the system. An additional obstacle in the detection and proving of crimes lies in the fact that perpetrators can commit crimes at different locations in real time, as a result of insufficient harmonization of legislation at the international level. The online payment card abuse is mostly committed by young persons who use the obtained data for the purchase of goods at online stores and auction websites. Criminal groups from the region are becoming increasingly sophisticated in their actions and are connecting with foreign criminal groups. Their activities are concentrated on the European Union and the United States.

Serbia's Republic Agency for Telecommunications (RATEL) published on July 21, 2008, a document that contains the technical requirements for authorized monitoring of some telecom services and provides a list of obligations for the telecom operators. The Internet Service Providers (ISPs) are obligated to enable governmental bodies to access updated databases with personal data on users, contracts, maximum speed of data transfer, identification addresses as well as access to database about email users.

In Serbia cybercriminals are exploiting the global recession by luring in susceptible victims through the promise of easy money.[57]

Online frauds take place at auction websites and online stores, where goods are ordered but never delivered. Takeovers of business communications between company representatives from the region and business partners mostly from Asia, Africa and Latin America have also been registered. In both cases, perpetrators abuse the victims' trust and defraud both physical persons and business representatives. Perpetrators abuse data obtained by identity theft, impersonating legitimate business users.The effects of abuse lie in the financial damage caused both to the company, as the injured party, and the business partner whose identity was abused. Identity theft through phishing represents the unlawful obtaining of personal and financial data. Specially created e-mails and copies of websites of banks and other financial institutions are most frequently used for this purpose. Online frauds in the region are mostly carried out by well-organized foreign groups that use methods of social engineering.

On December 7, 2009,the OSCE organized investigation training course in Belgrade for cybercrime experts in South-Eastern Europe on combating malicious software. Fifteen computer crime experts from Serbia and neighbouring countries took part in the course, which highlighted techniques used by computer criminals. The course marked the first time the OSCE's Strategic Police Matters Unit has partnered with the commercial sector to offer training for police officers.[58]

In Serbia cybercriminals are increasingly focusing on Adobe PDF and Flash files, to infect victims with malware. In addition, they use rich content applications such as Flash files to distribute a malicious code. Flash-based ads on the Web, because of their binary file format, enable the cybercriminals to hide their malicious code and later exploit end-user browsers to install malware.

Serbia is rapidly developing its information technology market and the number of Internet subscribers is increasing every day. Along with this development, there is a need to have better and more comprehensive laws to tackle the issues that may arise in the near future.

Also, Serbia has a long way to go in bringing a comprehensive legislation on the liability of Internet service providers in cases of copyright infringement in digital context. It is of

57 Milovanović, Z., *Kompjuterski kriminalitet i elektronsko piratstvo,* Pravniživot 41(394), 1991, 993-1008. (Computer crime and electronic piracy).
58 OSCE helps train cybercrime experts in South-Eastern European, Belgrade, December 7, 2009,http://www.osce.org/spmu/51707

utmost importance for a country such as Serbia with an increasing number of Internet users and thereby increasing the threat to infringing the rights of copyright holders. At the same time, Serbia is becoming digitalized and if new laws are not brought in to protect the Internet service providers from copyright infringement by subscribers and the related aspects, it would adversely affect the Internet service provider industry as a whole though the cases regarding the same are yet to come before any court of law in Serbia.

Moreover, it is also important for Serbia to update its laws regarding this aspect to be in competition with other European countries.[59]

## CONCLUSION

Technology is now deeply enmeshed within the fabric of society. Criminals understand that technology is a highly effective force multiplier which can be abused to enable illicit activity, and leveraged to facilitate access to a global constituency of victims living online. Our collective dependency on technology makes this threat extremely difficult to eliminate. The relative ease with which offenders engage in new scopes of crime, and the high gains afforded to perpetrators, ensure that motivation for recidivists remains strong. Manifestations of crime emanating from the intellectual property domain are among the most formidable challenges for workers in criminal justice systems worldwide. As society evolves and technology goes forward our understanding of the origins of criminality must be continuously revised. The persistence, prevalence and seriousness of IPR and cybercrime offending demands a greater response from the international community.

## REFERENCES

1. Bennett, D, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations*, Information Security Journal: A Global Perspective, No. 2, 2012, pp.159-168.
2. Brenner, S. W., *Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?* Rutgers Computer and Technology Law Journal, No. 30, 2004, pp. 1-104.
3. Brenner, S. W., Koops, B. J., *Approaches to cybercrime jurisdiction*, Journal of High Technology Crime, No. 15, 2004, pp. 1-46.
4. Bryans, D., Bitcoin *and Money Laundering: Mining for an Effective Solution*, Indiana Law Journal, No.89, 2014, pp. 441-472.
5. Correa, C. M., *Intellectual Property Rights, the WTO and Developing Countries,* London and New York, Zed Books Ltd., 2000, pp. 35-37.
6. Dörr, D., Janich, S.,*The Criminal Responsibility of Internet Service Providers in Germany*, M*ississippi Law Journal, 80* Miss. L.J. 1247, 2011, 1247-1261.
7. Farah, P. D., *Tremolada, R., Intellectual Property Rights, Human Rights and Intangible Cultural Heritage*, Journal of Intellectual Property Law, 2014, pp. 21–47.
8. Grinberg, Reuben, *Bitcoin: An Innovative Alternative Digital Currency*, Yale Law School, Hastings Science and Technology Law Journal, Vol. 4, December 9, 2011 pp.160-208.

59 Milovanovic, G., Barac, N., Andjelkovic, A., *Cybercrime - A Treat for Serbian Economy*, SecuritateaInformațională, ConferințaInternațională, ediția a VII-a, 15-16 aprilie 2010, pp 111-114.

9. Hemmige, N., *Piracy in the Internet Age*, Journal of Intellectual Property Rights, No. 18, 2013, pp 457-464.

10. Hunton, P., *The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation*, Computer Law & Security Review, 27, 2011, pp. 61-67.

11. Kaplanov, N. M., *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation*, Loyola Consumer Law Review 111, No. 25, 2012, pp.111-174.

12. Kahandawaarachchi,T., *Liability of Internet Service Providers for Third Party Online Copyright Infringement: A Study of the US and Indian Laws*, Journal of Intellectual Property Rights No. 12, 2007, pp 553-561.

13. Krohn-Grimberghe, A., Sorge. C, *Bitcoin: Anonym Einkaufenim Internet?* University of Paderborn, Department 3 - WirtschaftsinformatikAnalytischeInformationssysteme und Bl, Germany, 2012.

14. Maskus, K. E, *Intellectual Property Rights in the Global Economy*, Washington, DC: Institute for International Economics, 2000, pp. 57-60.

15. Ma, Zhong-fa., Gao, Wei-na., *Impact of the ' Tomato Garden' Software Internet Piracy Case on Combating Copyright Infringement in China*, Journal of Intellectual Property Rights Vol 17, January 2012, pp 27-36.

16. Milovanovic, G., Barac, N., Andjelkovic, A., *Cybercrime - A Treat for Serbian Economy*, SecuritateaInformațională, ConferințaInternațională, ediția a VII-a, 2010, pp 111-114.

17. Nuth, M. S., *Crime and technology – Challenges or solutions? Taking advantage of new technologies: For and against crime*, Computer Law and Security Report, No. 24, 2008, pp.437– 446.

18. Reilly, D., Wren, C., Berry, T., March, *Cloud computing: Pros and Cons for Computer Forensic Investigators,*International Journal Multimedia and Image Processing, 1(1), 2011, pp.26-34.

19. Richet, J.L., From *Young Hackers to Crackers*, International Journal of Technology and Human Interaction, No. 9, 2013, pp.53-62.

20. Ron, G. D, Shamir, A., *Quantitative Analysis of the Full Bitcoin Transaction, Quantitative Analysis of the Full Bitcoin Transaction Graph*, Department of Computer Science and Applied Mathematics, The Weizmann Institute of Science, Israel, 2012, pp.1-19.

21. Schwartz, K. E., *Criminal Liability for Internet Culprits: The Need for Updated State Laws Covering the Full Spectrum of Cyber Customization*, Washington University Law Review, No. 87, (2009), pp. 407-436.

22. Szczepański, M., *Bitcoin: Market, economics and regulation*, European Parliamentary Research Service, Annex B: Bitcoin regulation or plans therefor in selected countries, Members' Research Service, November 2014, pp. 2-9.

23. Tasca, P., *Digital Currencies: Principles, Trends, Opportunities, and Risks*, Deutsche Bundesbank and ECUREX Research, University of Zurich, Department of Banking and Finance, 2015.

24. Tu, K. V., Meredith M. W., *Rethinking Virtual Currency Regulation In The Bitcoin Age*, Washington Law Review, No. 90, 2015, pp.270-347.

25. Vida M. Vilić, *Criminal Law Protection of Personality: Implementation of Council of Europe's Convention on Cybercrime No. 185 Of 2001 Into Serbian Legislative*, International Scientific Conference on Ict and E-Business Related Research, Doi: 10.15308, Sinteza, 2016, pp. 66-73.

# HOW DIFFICULT IS TO PROVE THE CRIMINAL ACTS IN THE FIELD OF CYBERCRIME?

**Jelena Matijašević-Obradović, PhD**[1]

**Ivan Joksić, PhD**

Faculty of Law for Commerce and Judiciary, University Business Academy in Novi Sad

**Abstract:** The innovative activities in the sphere of scientific-technical achievements and information technologies have become a component part in the functioning of a modern society. The lawseeks legal norms to regulate inventive social relations. Thus, performing the protective functions of the criminal law made it necessary to establish an incrimination field of unauthorized procedures, the criminal acts in the field of cybercrime, which require adequate criminal response. It is necessary to regulate the procedural forms of proving criminal acts in the field of cybercrime.Given that the criminal law has assumed a transnational character, animportant segment of its modernisation includes harmonisation with international and European legal instruments, as well as the solutions present in the procedural law of developed European countries.

In accordance with the above, the authors of the paperwill show the characteristics of the evidentiary proceedingsfor criminal acts in the field of cybercrime. In order to make a fuller and more comprehensive analysis, we will engage in the research of the international legal instruments, comparative law and domestic legal solution. The topic will then be viewed in the light of the prosecutorial and judicial practices in our country.

**Key words:**cybercrime, evidentiary proceedings, electronicevidence, prosecutor's office, the court.

## INTRODUCTION

Great opportunities in all spheres of social life, available to modern man, have caused his exposure to new and serious risks. There is no social activity in which information systems have not found their implementation.Just for these reasons, the presence of the information technology brings with it certain types of risks. Society becomes dependent on the information-communication elements, because without their functioning, basic lever and the mechanisms of a society - the work of public services, the performance of the activity of general interest, the provision of services and performance of the activity of the economic entities –would not be able to achieve its purpose.

All types of attacks on the information infrastructure may cause great damage to the society. Thereby, committing an offense in this field does not require great preparation and material investments. So, many changes that are brought about by the development of this segmentwereverysuited to antisocial and criminal activities, supporting and encouraging their emergence, spread and intensity.In the beginning of the implementation of the computer technology, computers were not eligible for greater abuse, because their application was not widespread, so that they were available only to a narrow circle of users - IT experts.The

1 E-mail: jela_sup@yahoo.com

rapid development of computer technology, simplification of its use, as well as the availability of a wider range of users, allowed the abuse of computer technology for different purposes.

Procedural solutions of the European-Continental legal area mostly does not include special evidentiary actions or special authorization related to the disclosure of the criminal acts in the field of cybercrime, and in the procedure of the detection and prosecution of these crimes the provisions on the regular procedure, applicable to all other criminal offensesare most often used.It is necessary to emphasize that, the perpetration of offenses in the field of cybercrime produces a special type of evidence, which is in its nature different from the classic evidence. It is Electronic (Digital) Evidence.

## MODALITIES OF PROCEDURAL SOLUTIONS IN THE FIELD OF CYBER CRIME

Information and communication technologies have become irreplaceablein the functioning of a modern society. It is the fact. Their necessity has launched a whole range of issues in which we are not always able to provide legal answers.Hence, the international, regional and national frameworkshave launched mechanisms for the protection of society and the individual from of abuse in this area. The introduction of new legal solutions in the substantive criminal law requires the provision of procedural forms in which they can be put into practice. In this context, the most tangible results are brought about byadopting the Council of Europe Convention on Cybercrime[2]which establishes minimum standards in this area of law.The Convention represents a major European legal instrument in the area of cybercrime. Hence, our criminal legislation is fully established on the model of the provisions of this Convention, respecting, thereby, the specificity of our legal area.

The legal position of cybercrime, in substantive and procedural criminal legislation, can be best observed through the classification of regulations in three groups:[3]

*The first group* includes the legal texts which regulate the most important status issues. In the Republic of Serbia that is the Law on the Organization and Jurisdiction of the state bodies for the fight against Cybercrime[4], as the status legal text, which establishes the organization and jurisdiction of government authorities in the fight against cybercrime.

*The second group* includes the regulations of the substantive law which provide for a number of actions that represent socially unacceptable behavior, which violate or breach clearly identified protective structures. This group, according to the opinion of our legislature, includes crimes, misdemeanors and economic offenses.Thus,substantivelaw regulations including:CriminalCode (chapter XXVIII, articles 298-304a)[5], the Law on copyright and related rights[6] and the Law on special authorizations for the effective protection of intellectual property rights[7].In addition to the criminal acts that are directed against the security of computer technology and the

2 Convention on Cybercrime, Council of Europe, Budapest, 23. XI 2001.; European Treaty Series (ETS) - No. 185, *http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc*, 5 August 2010.
3 A similar principle is inherent in the legislation of the countries belonging to the Continental-European legal area.
4 The Law on the Organization and Jurisdiction of the state bodies for the fight against Cybercrime, Official Gazette of RS, no. 61/05 and 104/09.
5 Criminal Code, Official Gazette of RS, no. 85/09, 88/05-corr., 107/05-corr., 72/09, 111/09, 121/12, 104/2013 and 108/2014.
6 The Law on Copyright and Related Rights, Official Gazette of RS, no. 104/09, 99/11 and 119/12.
7 The Law on special authorizations for the effective protection of intellectual property rights, Official Gazette of RS, no. 46/06 and 104/09-Other Laws.

elements of the information system, there is a large number of traditional (classic) crimes.[8]With use of computers and computer components, thesetypes ofcrime are done faster and easier, offenders are more difficult to trace, but the consequences are far greater.[9]

*The third group*includesprovisions of the criminal procedural law which establish the legal framework in terms of mechanisms and authorization of the state authorities in the procedure of detection and collection of evidence, the prosecution and trial of persons who have made the criminal acts in the field of cybercrime. These provisions are contained in the Criminal ProceduralCode of the Republic of Serbia.[10]

Certain concerns sparked a question of the organization of the judicial system of the state in the direction of creating preconditions for successfully combating the new forms of criminal activity. The question is whether to opt for a comprehensive systemic change, i.e. a change in the system of regulations in order to create a suitable legal framework, orbe oriented towards partial change of certain legal provisions in order to create conditions for providing timely and adequate response to new forms of criminal conduct. States have responded differently to these questions, depending on their own police and judicial capacity.In this part, we canpresent two basic methods or models of treatment:

*The first method* is very efficient, but very demanding, given that it requires a high degree of political and social awareness about the necessity of the changes that should be made.

*The second method* is economic and less demanding, given that it does not affect the basis of the legal system of a state.However, this method can be left behind a series of unresolved issues, such as the issue of competencies for the individual criminal acts, collisionnew and existing legal solutions, etc.

In accordance with the possibilities that have, the Republic of Serbia, in order to the criminal protection from new forms of cybercrime, has opted for another way of organization of its judicial system. Our legislature opted for partial changes of certain legal solutions, with the adoption of new provisions, which establish new state bodies for the treatment in these criminal cases. However, the process of harmonisation of the existing and new legal solutionhas created a number of unresolved issues in terms of competence, led to the application outdated substantive and procedural legislation, and caused a series of problems in the practice.

Our procedural legislation recognizes a third type of regulations which are set assessment mechanisms and authorization of all the participants in the criminal proceedings in terms detection of offenders, collection of evidence, their prosecution and trial. Criminal acts in the field of cybercrime does not represent the basis for the creation of a special criminal procedural forms, but only the basis for the Organization and Jurisdiction of the special state authorities who participate in their discovery, prosecution and trial. There are no specifics in terms of the procedural regulation. Because of the specialization of state bodies in combating

8 As an example, may be noted the activity of an organized criminal group that the local public is marked as "road mafia". Namely, it is known that members of this group (the toll workers and workers at companies dealing with computer technology) developed a special soundcard device and software with which concealed the toll vehicles at toll plazas along the highway (daily, in an average of 300 - 350 vehicles of foreign and domestic license mark). According to some figures, the Republic of Serbia damaged by over 700 million dinars, because of these activities. In criminal procedure that followed, were apprehended dozens of persons against whom criminal chargeswere filed. Source: Milošević, M. The current problems of suppression of cybercrime,*Nauka, bezbednost, policija (NBP*), 1/2007, p. 63.

9 Matijašević, J., and Petković, M. *Crimes against the security of computer data - analysis current solutions and importance in the context of the suppression of cybercrime*, Proceedings "The criminal-forensics research" (Ed. M. Matijević), The International Association in Criminology, Banja Luka, 2011, pp. 598-609.

10 Criminal Procedural Code, Official Gazette of RS, no. 72/2011, 101/2011, 121/2012, 32/2013 and 45/2013.

these criminal acts, is adopted the Law on Organization and Jurisdiction of the state bodies for the fight against cybercrime.[11]

Given that the procedure for criminal acts in the field of cybercrime does not change the process structure (process steps and stages), but only certain provisions of the rules of entities or the procedural actions, cannot be word on the special criminal procedure, but only on procedural variability. In doing so, there are four sets of criteria for the establishment of process variability: a) weight of the criminal acts; b) the type of criminal acts; c) type of criminal sanctions or other criminal measures; d) the subjects of the criminal proceedings. According to this classification of the criteria, cybercrime offenses could be subsumed under the criteria - according to the type of criminal acts, and in this group could be also grouped the criminal offenses of organised crime, corruption, war crimes, and other extremely serious crimes.

In this field, special importance is given to provisions that regulate collection and providing evidence. In fact, it is very important to ensure the quality of evidence. In doing so, the validity of the evidence provided by the use of evidence determined by the law.

## THE EVIDENCE IN CRIMINAL PROCEEDINGS FOR CYBERCRIME OFFENSES

Specifics of criminal acts in the field of cybercrime are visible through the use of specific evidence. Such evidence is, by its nature, different from the so-called classic evidence, which appear in connection with the general crime. We call them - *electronic evidence*.[12]Generally speaking, electronic evidence is information or data important for the investigation, which is stored or transmitted via a computer. Such evidence has the same value as well as all other material evidence and we can apply on them exactly the same procedural rules as well as on any other evidence. However, what we cannot forget about electronic evidence is their specificity, arising from their nature. They are very sensitive, and very easily can modify, delete or otherwise destroy. Also, electronic evidence can be placed on the individual computer, computer network or remote server outside of the territorial jurisdiction of the bodies which collect them, can be visible or invisible, which, in addition to the mentioned possibilities for their easy changes or destruction(intentionally or due to improper handling), imposes a number of specific features in their acquisition.[13]

Digital evidence plays an important role in various phases of cybercrime investigations. It is in general possible to separate four phases. The first phase is identification of the relevant evidence. It is followed by collection and preservation of the evidence. The third phase in-

11 Brkić,S. *Criminal procedural law II*, Faculty of Law, University ofNovi Sad, Novi Sad, 2010, p. 304.
12 In criminalisticsand judicial practice for the term electronic evidence is used the term*digital evidence*. This is a terminological, not substantive difference. It is interesting to note that the classification of sources of digital evidence in criminalistics done by storing the data on: 1) Temporary form of digital evidence. A typical representative of this form is the RAM memory, which without external sources of power ceases to exist; 2) A non-permanent form. With this form there is some internal power source such as the batteries. However, as well as temporary form, if we remove the battery, information would be lost. An example of this form is the RAM on a laptop that has the power to the battery; 3) Semi-permanent form. It is a persistent medium that can be changed - e.g. hard disk, floppy disk, CD, DVD; 4) Permanent (continued) form. This is ROM memory. Source: Mohay, G., et al., *Computer and intrusion forensics*, Arttech, Boston 2003, p. 25.
13 Radulović,S. The specificity of obtaining electronic evidence of the commission of cybercrimecriminal offenses, *Revija za bezbednost*, 12/2008, pp. 17-18.

cludes the analysis of computer technology and digital evidence. Finally, the evidence needs to be presented in court.[14]

In addition to the procedures that relate to the presentation of digital evidence in court, the ways in which digital evidence is collected requires special attention. The collection of digital evidence is linked to computer forensics. The term 'computer forensics' describes the systematic analysis of IT equipment for the purpose of searching for digital evidence. The fact that the amount of data stored in digital format is constantly increasing highlights the logistic challenges of such investigations. Approaches to automated forensic procedures using, for example, hash-value based searches for known child-pornography images or a keyword search therefore play an important role in addition to manual investigations.[15]

The basic principles of obtaining electronic evidence imply that any action by authorized person cannotchange contents of reviewed data. These principles is necessary to consistently applied, in any particular case, in order to preserve the integrity of the evidence which is obtained, and documented process of obtaining that allows the repetition of the process (if the need arises later in the process). Thus ensuring their probative force.[16]Considering that the facts is the basis for a decision on the existence or non-existence of a criminal offense and criminal responsibility of the offender, it is necessary to bear in mind the specificity of electronic evidence, which could have a significant impact on the complete determination of the facts.

The Convention on Cybercrime is in this segment paid attention to the importance of the specifics of electronic evidence.[17]Convention contains specific procedural ways that enable or facilitate the collection of this type of evidence. In contrast to the Convention, many of the national legislation do not provide specific procedural rules and the authorization of the state authorities in this domain. In such cases is applied general procedural rules as well as in the case of the collection of all other evidence. This approach certainly imposes the view that is required specification of the approach in criminal procedure. This is certainly one of many shortcomings of our criminal procedural legislation whose characteristics will be analyzed in detail in the following text.

The criminal procedure for the offenses in the field of cybercrime is a process variability, which in the context of the process of proving the relevant facts indicates that, regardless of the specific nature of electronic evidence, exist lack of specific authorization and mechanisms of public authorities responsible for prosecuting these types of crimes. According to the provisions of the Criminal ProcedureCode, evidence include: 1) A search of dwellings and persons (Articles 152-160); 2) Temporary seizure of objects (Articles 147-151); 3) Treatment with suspicious items (Article 154); 4) Interrogation of the defendant (Articles 85-90); 5) Examination of witnesses (Articles 91-101); 6) Investigation (Articles 133-136) and 7) Expertise (Articles 113-132) - IT specialists. The Criminal Procedure Code stipulates the obligation for all state authorities that provide the necessary assistance to the courts and other participating bodies in criminal proceedings, particularly in the case of detection of crime and finding the offenders. There are also requirements of issuing orders to disclose information about business or personal accounts of suspected persons.[18]

14 Gercke, M.*Understanding cybercrime: phenomena, challenges and legal response*, International Telecommunication Union, Telecommunication Development Bureau, Switzerland 2012, p. 84.
15 *Ibid*.
16 Radulović, S. *op. cit*., p. 18
17 The Law on Ratification of the Convention on Cybercrime, Official Gazette of RS, no. 19/2009.
18 The rules which apply to the other, "classic" evidence shall be also applied on the electronic evidence. Electronic evidence, however, differs from classic evidence according to several characteristics that are inherent to its nature. First, they arise in the area of electronic communications and electronic data: any electronic data is a string of ones and zeros, that create meaningful data provided by the User; then, this

In addition, the Criminal Procedural Code provides opportunities for the use of special investigative techniques that have remained out of reach of bodies for the fight against cybercrime, bearing in mind that, according to the legal provisions, they are applicable only for crimes of organized crime, as a form of criminal procedure that also fall into the category of process variability. The only measure that can be applied during the prosecution of criminal offenses in the area of cybercrime, refers to the fact that the public prosecutor may request that the competent national authority, bank or other financial organizations, carry out an examination of business persons for whom there are grounds for suspicion that they committed a criminal offense, for which the law prescribes a prison sentence of at least four years, and to submit documents and information that may serve as evidence of a criminal offense or property obtained through criminal offense, as well as information on suspicious financial transactions, in terms of the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism.[19]On the request and data collected, public prosecutor is obliged to immediately inform the investigating judge, who, on the written and confirmatory request of the public prosecutor, may decide that the competent authority or organization to temporarily suspend specific financial transaction, payment and issuing of suspicious money, other valuable paper or objects for which there are grounds for suspicion that they originate from a criminal offense or from the proceeds of a criminal offense or are intended for commission, or concealment of the offense. Limited circumstances in this case is that the measures applicable only in terms of the criminal offenses for which the law prescribed by the sentence of imprisonment of at least four years, as in the case of the prosecution of criminal acts in the field of cybercrime, reduces the possibility of its wider application.[20]

As regards the assessment of the degree of compliance of national legislation with the provisions of the Convention on Cybercrime, it is necessary to provide a detailed overview of all implemented solutions that still have not been included in the national criminal procedural framework. Earlier in the paper, we pointed to the fact that criminal procedural legislation of the Republic of Serbia contains a number of solutions that are not compatible with the Convention, neither with solutions of our substantive criminal law. Taking into account the specifics of the cybercrime offenses, as the characteristics of the national legislation in this area, we will consider the difficulties that arise when investigating and prosecuting these crimes, focusing on issues that are common in practice.[21]

space is not precisely defined, either in theory or in practice - it can easily happen that certain evidence is so well hidden that cannot be detected; Cybercrime offence, therefore, can go by unpunished, but even unnoticed - the victim or the victims of a high technology crime does not need to be aware that this offense is done. Source: Prlja, D., Reljanović, M. and Ivanovic,Z. *The Internet Law*, Institute for Comparative Law, Belgrade, 2012, p. 145.

19 The Law on the confirmation of the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Official Gazette of RS - International Treaties, no. 19/2009.

20 Measures can be applied in the following offenses: Damage the computer data and program (Article 298, paragraph 3) - in terms of the qualified form of the offense; Computer sabotage (Article 299); Computer fraud (Article 301, paragraph 2 and 3) - in terms of qualifiedforms of the offense; Display, collection, possession pornographic materials and exploitation of a minor person for pornography (Article185, paragraph 2 and 3) - in terms of qualified forms of the offense; Exploitation computer network or communication other technical means for the execution of criminal offenses against freedom of gender according to a minor person (Article 185b); Unauthorized use of Copyright works or objects of related rights (Article 199, paragraph 3) - in terms of the qualified forms of the offense; Fraud (Article 208, paragraph 1, 3 and 4) - in terms of primary and qualified forms of the offense; Forgery and abuse of payment cards (Article 225, paragraph 1, 2, 3 and 4) - in terms of primary and qualified forms of the offense, etc.

21 See: Komlen Nikolić, L., et al., *Combating cybercrime*, Public Prosecutors Association and the Deputy Public Prosecutors in Serbia, Belgrade, 2010, pp. 135-140.

## DIFFICULTIES IN PROVINGCYBERCRIME OFFENSES

The new Criminal Procedural Code arranged evidentiary procedure on precisely definedAnglo-Saxonsystem.[22]Hence, all complexity of cybercrime is evident, as when investigating and prosecuting its perpetrators, both in the process of conducting an evidentiary procedure. When working on solving these crimes is necessary to make a circle of persons who may be potential perpetrators. To carry out these criminal actions will require technical expertise, knowledge and skills which affects the narrowing circle of potential perpetrators.[23]Hence, the purpose of a more comprehensive and more substantial approach to the field of cybercrime is necessary to point out its main features:

a) Transnational character which, as a general rule, follows cybercrime. Unlike conventional forms of crime, cybercrime is characterized by significantly expanded space of criminal activity that does not require the presence of the perpetrator at the place of the commission of the offenses. This implies a change in the definition of that place and therefore the building of the new tactics of the criminalisticsmeasures and activities, including problems of validity of the criminal laws and police and judicial jurisdiction.[24]

The users of computer technology without control can move in the virtual IT world, regardless of state borders. Unauthorized actions may be carried out regardless of the temporal category, and regardless of where the offender is located. The target can be any system, the person or the situation. Therefore, the international exchange of information carries with it a number of risks that are, if happens abuse, extremely difficult to solve, and on that occasion to establish the identity of the perpetrator and his location. On the other hand, computer crime is performed in a specific area, called cybernetic or*cyber* space, which entails a lot of new and interesting implications.[25]

Cyberspace offers endless possibilities: different ways to communicate with other persons and to express their own thoughts and feelings, comprehensive and free information about any subject, the various forms of entertainment, business opportunities and more. Important features of cyberspace are the global and transnational scope, beyond the territorial control of national states.[26]

A large number of crimes in this area are related by their nature to a larger number of countries. Often in these situations raise questions about the possibilities of prosecution of the offenses, whose action is taken in the territory of several states at the same time, or the ways of prosecution the perpetrator or perpetrators of the offense in the country, whose law does not provide for this offense. In these cases there is no universal solution, nor a unique response. These "safe countries" have the most imperfect legislation, and not because of its policy of impunity for cybercrime, but because of non-recognition of the social danger which it represent. One of the reasons is the relative underdevelopment of the country in terms of modern technology, the lack of experts who would be able to deal with the problem, and the lack of political will to take change on this field.

b) Relativity of the principle*ignorantia iuris non excusat*.Relativize the principle that ignorance of the law does not justify, as the principle that the lack of knowledge of the law harms

22 Škulić, M. and Ilić, G. *Guide for the implementation of the new Criminal Procedural Code*, Paragraph, Belgrade, 2013, p. 123.
23 Aleksic, Ž. and Škulić, M. *Criminology*, Faculty of Law, University of Belgrade, Belgrade, 2010, p. 392.
24 Banović, B. *Preservation of evidence in criminalisticstreatment of the economic criminal acts*, Police College, Belgrade-Zemun, 2002, p. 135.
25 Petrović,S. *The information revolution in the context of abuse of information technology*, available at: http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-20.pdf, September 20, 2010.
26 According to: Drakulić, M. and Drakulić, R. *Cybercrime*,http://www.bos.rs/cepit/idrustvo/sk/cyberkriminal.pdf,September 3, 2010.

(*ignorantia iuris nocet*) does not lead to suppression of their application, or to the simplification of their meaning. The point of certain deviations is that in the sphere of cybercrime there are situations when persons who are taking the actions of certain criminal offenses in fact do not have purpose or intention to harm anyone, or to unlawfully gain some benefits. It may happen that the person via e-mail system infects all other e-mail addresses that are in the computer's memory, and that they are not aware of the presence of malicious software on their own computer. It may also happen that by e-mail people come in possession of illegally obtained materials which are further distributed (e.g.an illegally obtained film), etc. If such activities do not represent everyday practice, but rather sporadic occurrence, their social risk practically does not exist, and such a case does not represent the occasion for the initiation of the court proceedings in the particular case.[27]

Additionally, it is necessary to make a few remarks.

Before expansive use of the Internet, one of the ways that attackers usually used to connect to a private network and gain access to confidential information was dialing a phone number of the modem over a public telephone network.[28]However, communication standards and protocols have been replaced by new versions, the solutions that have been largely redesigned or completely new solutions. Quickly evolving also imposed and communication software: drivers for network adapters, software that provides routing functions, as well as servers that provide services at the application layer of the OSI reference model, such as Web servers and email servers.[29]

Today, technical developments have improved daily life – for example, online banking and shopping, the use of mobile data services and voice over Internet protocol (VoIP) telephony are just some examples of how far the integration of ICTs into our daily lives has advanced. However, the growth of the information society is accompanied by new and serious threats. Essential services such as water and electricity supply now rely on ICTs. Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs. Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways.[30]

c) The necessary level of professional knowledge. In order to properly determine relevant material facts in the criminal procedure, and took correct positions on the specific questions, the judge, the prosecutor, the local police must have an enviable knowledge of the matters in question. However, the states rarely implemented specialization and specific training of judges and other participants in the fight against cybercrime, although in practice many of the procedures shown that experts cannot interpret the facts in a way that judges without any prior knowledge could understand enough, to decide, based on them, about someone's criminal responsibility.

d) The determination of the identity of the offenders. The question of the identity of the offender in the area of cybercrime can be very difficult to solve, given that one person can manipulate the computer of another person, even at a time when the owner is working on that

27 It is interesting to note that the USA has one of the world's most developed legislation in the field of computer-related rights, and the issue of the use of electronic documents is regulated by a special regulation, or the Federal Rules of Evidence. So, for example, in the Rule 1001 clearly indicates that the electronic records have the same legal effect as well as documents written by hand. Source: Prlja, D. and Savovic, M. E-mail as evidence in Criminal law, *Foreign Legal Life*, 2/2009, p. 79.

28 Pleskonjić, D., Maček, N., Đorđević, B. and Carić, M.*The security of computer systems and networks*, Mikro knjiga, Beograd 2007.

29 Jovanović, M., Maček, N., Franc, I. and Mitić, D. Modern high-tech threat: the vulnerability of software products and threats, In: Proceedings "Ziteh-16" (ed. Slobodan R. Petrović), Association of court experts in information technology,IT expert, Beograd 2016, 1-10, pp. 1-2.

30 Gercke, M. *op. cit*., p. 2

computer. There are different categories of perpetrators of computer crime, given that there are a lot of offenses, but also bearing in mind the motives that drive them for the commission of these activities.

In order to reach a solution to the problem of identifying the real perpetrators of the cybercrime, the investigative actions must be thoroughly implemented, which again points to the need for a certain degree of professional knowledge by prosecutor and police authorities which conduct the investigation. This should particularly bear in mind, because the majority of computer fraud brought to such a perfect form of manipulation by others computers, which must be very carefully deal with potential suspects, until they reach unequivocal knowledge that they were in any way could be involved in the commission of offenses.[31]

e) There are difficulties in detecting the perpetrator who committed the offense using a public network and a laptop computer. The Internet is one of the fastest-growing areas of technical infrastructure development.

The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for developing countries. The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services. E-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone services are growing faster than landline communications.[32]

As a result of the development of new possibilities for Internet communication, it has become quite possible that someone uses a public network available in public areas, Internet cafes, or for the purpose of certain abuses advantage of the ability to access an open network of another user. In such cases, the perpetrator is almost invisible and certainly it is impossible to trace because they are in the locations and IP addresses available to any person.[33]

f) The question of the validity of the electronic evidence. The notion of electronic evidence has already been discussed.In this context we will mention the difficulties that may arise during its appreciation in criminal proceedings. In the case when the currently provided data are not sufficient to connect a specific person to a committed offense, the question is how valid the content of the hard disk, flash memory and other electronic evidence can be, especially in cases where a judge, prosecutor and other relevant entities do not have adequate degree of knowledge in the field of cybercrime.[34]

31 See: http://arstechnica.com/tech-policy/news/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense.ars,May 1, 2009.

32 Gercke, M. *op. cit*., p. 1

33 In the court case No.Kž. 1.321/2010 of the Belgrade Appellate Court, in judgment dated March 16, 2010, judged that "it is not necessary for the existence of a special order to control communication when message can be clearly photographed or when preserved (for person or company) and can now combine the case file."However, in the case if message is not retained, the public prosecutor may order the expert, and to obtain from the phone company, transcripts of messages with a listing of outgoing and incoming messages. During the trial, at main hearing, if the message is at a mobile phone, the court may make an investigation on the phone by direct observation. In connection with this approach, the Supreme Court of Serbia, took the following legal position: "view the content of a mobile phone - to review and read the contents of messages sent to each other between the accused and witnesses, is an investigation on mobile thing, because this is not about the material that has been obtained by surveillance and recording of telephone and other conversations or communications or other technical means or optical recording of persons, which can be acquired only in accordance with Article 232 of the Criminal Procedural Code. Therefore this is a legal proof. "The judgment of the Supreme Court of Serbia Kž.1. 2678/2007 from February 18, 2008. See:http://www.ssssns.com/index.php/2013-05-10-05-52-52/sudska-praksa/316-sms-poruka-kao-dokaz-u-krivicnom-postupku,March 25, 2013.

34 Due to the importance of the issue of electronic evidence, the European Union implemented from 2005 to 2007, a project entitled "Eligibility of electronic evidence in court". The project included an

The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law-enforcement agencies are allowed to investigate and prosecute cybercrime effectively.[35]

g) International cooperation between the different legal systems around the world. Given that there are no general international acts to solve concrete issues of international cooperation, the two countries is usually left to bilateral agreements and even informal contacts, to gain a certain degree of cooperation in the field of cybercrime. It should be notedthatthe case of informal contacts and cooperation would imply question the legal validity of such collected evidence.

Cybercrime often has an international dimension. E-mails with illegal content often pass through a number of countries during the transfer from sender to recipient, or illegal content is stored outside the country. Within cybercrime investigations, close cooperation between the countries involved is very important. The existing mutual legal assistance agreements are based on formal, complex and often time-consuming procedures, and in addition often do not cover computer-specific investigations. Setting up procedures for quick response to incidents, as well as requests for international cooperation, is therefore vital.[36]

Also, it should be noted that some states do not predict cybercrime offenses in their laws, some only declaratively recognized this phenomenon while the legal provisions are not applied in practice, and finally, in some countries, there are specifics in terms of analyzing and regulating certain legal issues in this area. All this facts can be a nuisance in cooperation between countries in the field of cybercrime, even when cooperation is achievable and welcome. If we look at the situation in our country, the Law on Mutual Legal Assistance in Criminal Matters[37], failed to regulate specific aspects of mutual assistance in criminal matters in the area of cybercrime in which, more than any other, the speed of treatment is crucial for the successful conduct of criminal proceedings.

*Other issues.* In the area of the prosecution of cybercrime offenses, may occur other issues related to processes, the offender, legal aspects, etc. Among the prominent dilemmas is the question of motivation for commission offenses in this field. The motives are different, given that, there are various profiles of the offenders. Unlike the criminal acts in the field of organised crime, with the cybercrimeoffenses financial gain is not the only, nor the dominant motive. In contrast to this,"wish for financial gain is the main motive for the largest number of committed criminal acts of organized crime. One of the most important issues is how to deal with juvenile offenders whose level of psycho-physical development is insufficient to understand the significance and consequences of committed actions. If we admit that children from 13 to 14 years are, often, experts in the use of IT, we think that the age of criminal responsibility should be "reduced" to the appropriate age range. This is confirmed by the statistics in terms of age of perpetrators of these crimes.[38]

On the basis of the above, it is necessary to develop adequate preventive activities in the field of cybercrime, given that the suppressed in this segment often is not the best solution,

analysis of the legislation and judicial proceedings in the sixteen member states of the European Union. Results showed that in some jurisdictions there is no definition of electronic evidence, while others contain such a definition, but they are not sufficiently precise. The common conclusion is that in all jurisdictions electronic evidence equated with classic evidence as follows: electronic documents with paper documents, electronic signature with the handwritten signature and e-mail with the usual mail. In procedural rules in both civil and criminal matters, have not been established common standards for the collection, storage and execution of electronic evidence in court. Mainly used by analogy in relation to the classical evidence, although some countries such as Great Britain and Belgium have defined the rules for the collection of "computer evidence".

35 Gercke, M. *op. cit*., p. 3

36 Gercke, M. *op. cit*., p. 3

37 Law on Mutual Legal Assistance in Criminal Matters, Official Gazette of RS, no. 20/09.

38 See: Komlen-Nikolić, L., et al., *op. cit*., p. 143.

and in certain situations is completely pointless. In certain cases of serious crimes, such as the production and distribution of child pornography, large-scale offinancial fraud, links between cybercrime and organised crime and terrorism, prison sentences are completely reasonable. In less serious cases, such as minor scam attempts, intrusions into the computer or computer system without any harmful effects, etc.,the question is how much is a reasonable prison sentence, even criminal sanction in general. A separate issue is how to handle recidivism, or how to prevent it and channel the knowledge of such offenders (when it comes to minor offenses) to socially useful work, through alternative sanctions and stimulating creativity, rather than punishment and destructiveness.[39]

## CONCLUSION

When we review the important issues that have been allocated in the practice and compare with the current criminal procedure law as well, it can be concluded that the current Criminal Procedural Code, like the other procedural and legal legislation of Continental-European legal area, does not provide for specific evidentiary actions nor special authorities related to the detection of crimes in the area of cybercrime. In addition, in criminal proceedings for cybercrime offenses cannot be applied special investigative methods that are, according to law, applicable only for the crimes of organised crime, corruption and other extremely serious crimes. Therefore, in the procedure of detection and prosecution of these crimes, competent state authorities use the relevant provisions of the Criminal Procedural Code for regular procedures, applicable to all other crimes.

In this situation, criminal procedural problems are part of the customary practice. In order to finish a job that is in their jurisdiction, and all because of the lack of appropriate procedural instruments, the state authorities who applied the Criminal Procedural Code, often resort to analogy and extensive interpretation of its legal norms. Thus, while securing and seizure of digital evidence and other material, authorized bodies apply the provisions of the Criminal Procedural Code relating to the searching of objects and persons, and temporarily confiscation of objects; also, to check some computer equipment on the place where it has been committed a criminal acts, authorized bodies apply the provisions of the Code relating to the investigation; also, in terms of expertise confiscated equipment and its digital content, authorized bodies apply the general provision of expertise.[40]

In this context, we must emphasize the incompatibility of the Criminal Procedural Code with the provisions of the Criminal Code, which in 2003 joined the tendencies towards the development of modern criminal legislation, and through the adoption of the latest novelties significantly brought the regulations in the field of cybercrime closer to the regulations presented in the Convention on Cybercrime. Namely, the reality is more inventive than any legislator. Because of that, it is necessary, for the next novel in substantive, especially procedural, legislation, to adapt the national legislation to international frameworks and standards that have been recognized by ratifying the Convention on Cybercrime. Building flexible legal norms, which will be adjusted to changes without becoming obsolete and therefore unenforceable, but also taking into account preventive measures, can greatly suppress and prevent numerous unlawful actions in the field of ICT, which will protect human and social goods and values, safety and confidence in the computer system, and the protection of human rights and freedoms, to get a higher degree.

39 *Ibid.*, pp. 177-178.
40 *Ibid.*, pp. 141-142.

## REFERENCES


1. Aleksic, Ž. and Škulić, M. *Criminology*, Faculty of Law, University of Belgrade, Belgrade, 2010.
2. Banović, B. *Preservation of evidence in criminalistics treatment of the economic criminal acts*, Police College, Belgrade-Zemun, 2002.
3. Brkić, S. *Criminal procedural law II*, Faculty of Law, University of Novi Sad, Novi Sad, 2010.
4. Convention on Cybercrime, Council of Europe, Budapest, 23. XI 2001.; European Treaty Series (ETS) - No. 185, *http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc*, 5 August 2010.
5. Criminal Code, Official Gazette of RS, no. 85/09, 88/05-corr., 107/05-corr., 72/09, 111/09, 121/12, 104/2013 and 108/2014.
6. Criminal Procedural Code, Official Gazette of RS, no. 72/2011, 101/2011, 121/2012, 32/2013 and 45/2013.
7. Drakulić, M. and Drakulić, R. *Cybercrime*, http://www.bos.rs/cepit/idrustvo/sk/cyberkriminal.pdf, September 3, 2010.
8. Gercke, M. *Understanding cybercrime: phenomena, challenges and legal response*, International Telecommunication Union, Telecommunication Development Bureau, Switzerland 2012.
9. Jovanović, M., Maček, N., Franc, I. and Mitić, D. Modern high-tech threat: the vulnerability of software products and threats, In: Proceedings "Ziteh-16" (ed. Slobodan R. Petrović), Association of court experts in information technology ITveštak, Beograd 2016, pp. 1-10.
10. Komlen Nikolić, L., et al., *Combating cybercrime*, Public Prosecutors Association and the Deputy Public Prosecutors in Serbia, Belgrade, 2010.
11. Matijašević, J., and Petković, M. *Crimes against the security of computer data - analysis current solutions and importance in the context of the suppression of cybercrime*, Proceedings "The criminal-forensics research" (Ed. M. Matijević), The International Association in Criminology, Banja Luka, 2011, pp. 598-609.
12. Milošević, M. The current problems of suppression of cybercrime, *Nauka, bezbednost, policija (NBP*), 1/2007.
13. Mohay, G., et al., *Computer and intrusion forensics*, Arttech, Boston 2003.
14. Petrović, S. *The information revolution in the context of abuse of information technology*, available at: http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-20.pdf, September 20, 2010.
15. Pleskonjić, D., Maček, N., Đorđević, B. and Carić, M. *The security of computer systems and networks*, Mikro knjiga, Beograd 2007.
16. Prlja, D. and Savovic, M. E-mail as evidence in Criminal law, *Foreign Legal Life*, 2/2009.
17. Prlja, D., Reljanović, M. and Ivanovic, Z. *The Internet Law*, Institute for Comparative Law, Belgrade, 2012.
18. Radulović, S. The specificity of obtaining electronic evidence of the commission of cybercrime criminal offenses, *Revija za bezbednost*, 12/2008.
19. The Law on Mutual Legal Assistance in Criminal Matters, Official Gazette of RS, no. 20/09.
20. The Law on the Organization and Jurisdiction of the state bodies for the fight against Cybercrime, Official Gazette of RS, no. 61/05 and 104/09.
21. The Law on Copyright and Related Rights, Official Gazette of RS, no. 104/09, 99/11 and 119/12.

22. The Law on special authorizations for the effective protection of intellectual property rights, Official Gazette of RS, no. 46/06 and 104/09-Other Laws.
23. The Law on Ratification of the Convention on Cybercrime, Official Gazette of RS, no. 19/2009.
24. The Law on the confirmation of the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, Official Gazette of RS - International Treaties, no. 19/2009.
25. Škulić, M. and Ilić, G. *Guide for the implementation of the new Criminal Procedural Code*, Paragraph, Belgrade, 2013
26. http://arstechnica.com/tech-policy/news/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense.ars, May 1, 2009.
27. http://www.ssssns.com/index.php/2013-05-10-05-52-52/sudska-praksa/316-sms-poruka-kao-dokaz-u-krivicnom-postupku, March 25, 2013.

# SPECIALIZED ICT SYSTEM FOR SAFE TRANSFER OF CONFIDENTIAL DATA BY APPLICATION OF CRYPTOGRAPHIC METHODS IN COMPUTER NETWORKS

**Miladin Ivanović**
**Slobodan Nedeljković**
**Predrag Djikanović**
**Vojkan Nikolić**
Ministry of Interiorof the Republic of Serbia, Department of Analytics, Telecommunication and Information Technologies

**Abstract:** The process of automation of business processes today implies the use of digital data and information and communication technologies (ICT) as a basic means of operation. The digital form of data, as such, has enabled the individual, group and organization, the economic and public sector to easily collect large amounts of data and information, through a variety of services provided by ICTs. Data protection at all stages (collecting, storing, processing, downloading) is a permanent challenge for all operators of the ICT system, and in particular it comes to the expression of confidential and sensitive data. Detection of confidential data in the financial, medical and security sectors can result in a security risk to persons, organizations, property, and even state interests. In this respect, the development of specialized systems for the protection of confidential data has become an obligation for such organizations that, as a rule, operate or strive for business based on electronic data exchange. The application of cryptography and cryptographic techniques in these tendencies is an indispensable need, but also a legal obligation, and the development of a system that can meet security needs and set standards is a constant challenge for organizations.

In this paper, a model for the protection of confidential data will be presented based on the use of specialized cryptographic devices and certain cryptographic methods that ensure secrecy, authenticity, integrity, non-consistency and availability of data in all phases. Through a flexible architecture and system organization, the model provides primacy in almost all organizations, regardless of size and complexity.

**Keywords:** information security, cryptography, cryptographic algorithms, cryptographic devices, keys

## INTRODUCTION

With the development of Internet services such as e-mail, social networks, Cloud Services, Internet of Things, e-government services and other related services, more efficient business, greater availability and exchange of information is possible in real time. The increasing use of mobile devices and services (smart phones, tablets, etc.), their low price and distribution have changed the roots of functioning of individuals and organizations. The current availability of information that characterizes the use of the listed ICT services has accelerated all spheres of life, whether it is a civil, business or public sector.

"Connection (interconnection), as a basic link in the information exchange system, has enabled simple communication of remote points in the space. This once very expensive and time-consuming venture is today easily accessible – the development of global communications networks such as the Internet, social networks, mobile information and communication technologies and various other services offered by ICT, their simplicity, flexibility, affordability and low cost, made it easy for everyone to communicate with each. Today, people, organizations, institutions and states exchange large amounts of information every day. There is more and more information and their accessibility is getting bigger and naturally new challenges for their users arise, which arise in this kind of information environment as it is today."[1]

In line with the development of the aforementioned ICT services, the laws regulating the issue of electronic documents, electronic signatures, electronic business, and electronic communications have been adopted, enabling citizens, state authorities, public administration and other organizations to fully turn to electronic commerce. "Qualified electronic signature in relation to data in electronic form shall have the same legal effect and probative value as a personal signature, i.e. a personal signature and seal, in relation to paper data. An electronic signature may have legal effect and may be used as evidence in a legally regulated procedure, except where, in accordance with a special law, it is required that only a personal signature has legal effect and probative value."[2] Established regulation was a tailwind to advanced organizations that fully digitized their business processes, ejected paper from use, and turned to the use of electronic documents and services in the daily exchange of official acts and information.

These changes did not circumvent the business processes and information flows in security structures, such as the military, police, intelligence and other security services. The growing need for rapid delivery and exchange of information, which is especially evident in organizations of this type, encouraged these services to use communication ICT services such as email, Document Management System, File Transfer Service, mobile applications and other.

The advantages that modern e-commerce provides to individuals and organizations, however, is accompanied by high risks. Cyber crime and the risks that exist in the computer world have become a daily event that has affected many organizations, resulting in unauthorized access to data, data changes, data outbursts, data theft, Crypto Ransomware and other forms of crime. Detection and alienation of confidential (secret) data is a particularly high risk that can often endanger security of persons, organizations, property, and even state interests, especially in the medical, financial, public and security services.

"31.9% of user computers were subject to at least one Malware-class web attack during the past year. 261.774.932 URLs on the Internet have been recognized as malicious web content by antivirus programs. 1,445,434 work stations of individual users were meta encryptors. In 2016, 22.6% of the crypto-ransomware attack was targeted at organizations. The percentage of attacks on Android operating systems of a total of 21% is with an increase of 7% annually ... "[3]

## PROTECTION OF CONFIDENTIAL DATA

Information security is a major challenge for organizations that operate electronically today, especially when it comes to state security services. As a separate segment of information

1 M. Ivanović, D. Batoćanin, T. Baković, Safe service transformation as a mechanism for interoperable integration of technologically diverse systems, YU INFO 2016.
2 Law on Electronic Signature, "Official Gazette of RS", no. 135/2004.
3 M. Garnaeva, F. Sinitsyn, Y. Namestnikov, D. Makrushin, A. Liskin, Kaspersky Security Bulletin: OVERALL STATISTICS FOR 2016, Kaspersky Lab.

security, the protection of secret (confidential) data is distinguished, taking into account the nature of these data and the risks that may arise in case of their disclosure or alienation. "Secret information shall be information of interest to the Republic of Serbia, which is determined and marked by a certain degree of secrecy by law, other regulation or decision of the competent authority enacted in accordance with the law."4

The area of classified information protection is regulated in the Republic of Serbia through the Law on Information Security5, as the umbrella regulation, and then through the Secrecy of Data Act6 and accompanying bylaws and regulations. "This law regulates a unique system of determining and protecting classified information of interest to national and public security, defense, internal and external affairs of the Republic of Serbia, protection of foreign classified information, access to classified data and cessation of their secrecy, authority of the authorities and supervision over the implementation of this Law, as well as liability for non-performance of obligations under this law and other issues of importance for the protection of confidentiality of data."7

As a special aspect of the protection of classified information, the area of managing secret data in ICT systems and networks has been recognized, where the Data Privacy Act foresees the obligatory application of cryptographic protection measures. "The transfer and delivery of classified information using telecommunication information means is done with the obligatory application of the prescribed crypto-protection measures."8 Specific measures of cryptographic protection and other security measures related to the protection of classified information in ICT systems are prescribed in the Decree on Special Measures Protection of Classified Information in Information and Telecommunication Systems9 and other by-laws and regulations. The said regulation prescribes special measures for the protection of classified information in information and telecommunication systems related to the physical protection of facilities and security zones in which classified information is handled, the mandatory application of fire protection, protection against compromised electromagnetic radiation (KEMZ), the provision and protection of equipment, protection of software support, protection of computer networks and other organizational protection measures. In addition to the above, the aforementioned Regulation also prescribed the mandatory use of verified methods and means of cryptography, which means that all methods and means must be approved by the competent authority (in the concrete case of the Ministry of Defense, Center for Applied Mathematics and Electronics – CPME).

"Secret information shall not be transmitted through a system outside the security zones without the use of cryptographic protection methods and tools, which have been approved by the authority responsible for carrying out cryptographic protection operations."[10]

## MODEL OF SPECIALIZED CRYPTOGRAPHIC SYSTEM FOR TRANSFER OF CONFIDENTIAL DATA

Secure data transfer systems on computer networks are specialized systems that involve the use of verified cryptographic algorithms and other security mechanisms that prevent ac-

4 Law on Classified Data, "Official Gazette of RS", no. 104/2009.
5 "Official Gazette of the Republic of Serbia" No. 6/2016.
6 "Official Gazette of RS", no. 104/2009.
7 Ibid.
8 Ibid.
9 "Official Gazette of the Republic of Serbia" No. 53/2011.
10 Decree on special measures for the protection of classified information in information and telecommunication systems, "Official Gazette of RS", no. 53/2011.

cess to data by unauthorized persons and which provide maximum security and control over data at all stages of the life cycle.

"Cryptography is art and science in concealing information. Without the ability to hide information, the existing network computing environment would not be possible. In the most general sense, cryptography represents a logical barrier to protecting information from unauthorized users."[11]

The model of the specialized system with the cryptographic data processing described in this paper is a software-hardware system based on an application document management solution (information), including cryptographic and other functions that take place in the system, as well as specialized cryptographic devices.

In a cryptographic sense, the system is based on the use of symmetric and asymmetric cryptographic algorithms, and the use of Public Key Infrastructure (PKI), electronic certificates, digital signatures and other operations to ensure the highest possible level of data protection.

The basic purpose of a symmetric cryptographic algorithm is to encrypt information transmitted through a computer network (transport code algorithm). In accordance with the legal regulations regulating the field of data protection, the symmetric cryptographic algorithm used in the system would have to pass a security assessment by the competent authority, which in the Republic of Serbia is the Center for Applied Mathematics and Electronics – CPME (organizational unit of the Ministry of Defense of the Republic of Serbia). This symmetric cryptographic algorithm represents the most complex and powerful method of data protection in the system, which ensures that unauthorized persons cannot come up with the content of information in case of interception of packets in transmission through computer networks or another way of insight into documents that are created and transmitted in the system . Asymmetric cryptographic methods are based on the use of electronic certificates, public and private keys, and asymmetric cryptographic algorithms such as RSA (Rivest-Shamir-Adleman), Elliptic curve algorithm (ECC) and others. The objective of asymmetric cryptography in the system is to provide reliable electronic identification of users in the system (authentication) using PKI infrastructure and electronic certificates, as well as to ensure authenticity, integrity and non-validity using digital signature, HASH functions and public key encryption (Public Key Encryption).

## CRYPTOGRAPHIC DEVICES IN THE TRANSFER OF CONFIDENTIAL DATA SYSTEM

Taking into account that the greatest secret of such a system is exactly the cryptographic algorithm, its structure, control parameters and keys, the use of specialized hardware cryptographic devices (HSM) has begun. These devices are advanced computers that perform secure management of critical keys and parameters, provide crypto-processing of high performance and reliability, as well as high level of security of stored data and cryptographic parameters. In order to prevent the possibility of compromising the system by accessing the device by unauthorized persons, the devices are enriched with Tamper Protection, which ensures that all parameters are deleted from the algorithms and keys stored in the cryptographic device when opening the device (breaking the case, unscrewing screw housings, etc.). In addition, cryptographic devices are compatible with FIPS 140-2 Level 4 standard, which guar-

11 Hamid R. Nemati, Li Yang, Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, Information Science Reference, Hershey-New York, 2011.

antees a high and consistent level of performance, reliability and security of these devices and their operating systems.

These cryptographic devices are equipped with a specialized FPGA (Field-Programmable Gate Array) chip whose purpose is to perform high-performance symmetric cryptographic operations. The cryptographic algorithms themselves are programmed into these chips using the hardware description language of the programming language, and the programming process is performed in the highest level security environment, which, in addition to organizational protection measures, includes strict physical and logical access control and protection against compromised electromagnetic radiation (use of Faraday cages).

All control parameters of the symmetric cryptographic algorithm and the corresponding keys are located on the commemorative unit of the cryptographic device. In order to ensure the high security of these parameters and keys, smart cards were used as secure commemorative units. In this way, the protection of cryptographic parameters in transport (transfer of cryptographic parameters to the cryptographic device itself) is ensured, as well as in the device itself.

## TRANSFER OF CONFIDENTIAL DATA THROUGH THE SYSTEM

Access to the system for transferring confidential information requires highly secure logical access control, in order to prevent access to unauthorized users. In terms of the above, the "hard" dual-factor authentication based on the use of user smart cards (electronic identification scheme of high reliability) is implemented in the system. User management in the system is performed through a specially developed user management and access rights (Identity Access Management System). Each user in the system is authorized to access the system, and access to documents and document management functions is granted in the form of a special privilege (role).

In order to ensure the management of documents in the system (creation, verification, signing, encryption, sending, receiving, etc.), a document management system (Document Management System) has been developed. Through this component, which users access through the client (user) application, all document management features are enabled. The user interface was developed in the example of the email client, which made an intuitive user environment, natural for the end users. The user application is enriched with the text editing environment (Text Editor), so all text management operations are performed in a protected application environment, and all the basic text processing operations that are characterized by related applications, such as Microsoft Word and others, are provided. It should be noted that the user application itself does not store documents (neither in the creation, nor after sending and receiving). All documents in the warehouse system are accessed by the central system and the corridor in accordance with the defined access rights, by transferring the contents of the document to the working memory (displaying the contents of the document in the text processing environment). When logging users to a user application, the application downloads metadata and other information about documents that do not represent a secret from the central system (document number, title of the document object, sender, recipient, document status, etc.).

Within the user application, it is possible to create a document template, in order to ensure the commodity in operation, shortening the time in creating document types and avoiding unnecessary errors in the form and structure of the documents. Upon completion, the doc-

ument may be sent for verification to the superior officer. Document verification is a process that can be repeated unlimited number of times. After aligning the content to the document form (final verification), the responsible person can perform the digital signature of the document. Thus, a digitally signed document is then encrypted with a dedicated cryptographic algorithm (transport code algorithm) and sent to a central system that notifies the recipient of the inbox. It should be noted that the document is encrypted at all stages of the transport through the system, including the verification process, and encryption, as already described, is performed in specialized hardware cryptographic devices (HSM).

## CENTRAL COMPONENT OF THE CONFIDENTIAL DATA TRANSFER SYSTEM

The basic component of the presented model is the central system. This system component consists of a central server, database, and specialized hardware cryptographic devices of high performance. The central server system manages all system functions. Through the central server, users access the system via an administrator console. In addition, the central server is responsible for managing documents in the system, managing the database system, managing cryptographic and other devices and other functions necessary for system operation (receiving requests, data management and client applications, analytics, etc.).

The central database system is designed to store documents and other data processed in the system, and the database structure is based on a relational model. All confidential documents in the database are encrypted by a special symmetric cryptographic algorithm (encryption algorithm for storage), and encryption and decryption operations are performed in a separate hardware cryptographic device, in order to ensure high performance of the system. In addition, using a special cryptographic storage algorithm provides separation of the cryptographic functions in storage from those used in the transport of documents through the system, thus maximizing the security of data in the system, and reducing the possibility of detecting database contents if the system gets compromised in the transfer of documents.

Cryptographic devices in the central system are high-performance devices equipped with multiple FPGA processors that provide the ability to cryptographic processing of more competitive cryptographic operations. These cryptographic devices are managed by the central server upon the client's received request (client application). In this way, it is possible to manage client connections (requests) exclusively by the central server, which performs the prioritization of requests and manages the cryptographic device according to the given algorithm, which ensures maximum system performance.

In addition to the implemented protection mechanisms, it is necessary to emphasize that according to the current legislation regulating the field of information security and the protection of classified information, the system for transfer of confidential documents with cryptographic processing will have to pass the process of approval (verification) by the competent authority in order to be used in practice for the transfer of documents with a security code.

## CONCLUSION

The transfer of confidential data through the information and communication system is an increasing need for organizations operating in the modern age, characterized by an increasing need for quick access to information. Managing confidential documents (secret

documents) in such an environment presents a major security challenge for all organizations, especially for security services and services that have particularly sensitive data whose disclosure can lead to a threat to the security of individuals, organizations, assets, and public interests. In response to the challenges presented by the organization, efforts are being made to build specialized systems that can respond to imposed security challenges and ensure maximum data security at all stages.

The presented model of a specialized system for transferring confidential data provides a logical and physical architecture that can be adapted to the needs of almost all organizations, regardless of size and complexity. Using special hardware cryptographic devices and smart cards in the system, the maximum level of security of confidential information and cryptographic parameters of the system is ensured in all phases. By combining various coding algorithms, as well as symmetric and asymmetric cryptographic functions, non-integrity, integrity and confidentiality of the highest level are ensured, which can meet the requirements of the current legislation in the Republic of Serbia.

## REFERENCES

1. Decree on special measures for the protection of classified information in information and telecommunication systems, "Official Gazette of RS", no. 53/2011.
2. Hamid R. Nemati, Li Yang, Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, Information Science Reference, Hershey-New York, 2011.
3. Law on Classified Data, "Official Gazette of RS", no. 104/2009.
4. Law on Electronic Signature, "Official Gazette of RS", no. 135/2004.
5. M. Garnaeva, F. Sinitsyn, Y. Namestnikov, D. Makrushin, A. Liskin, Kaspersky Security Bulletin: OVERALL STATISTICS FOR 2016, Kaspersky Lab.
6. M. Ivanović, D. Batoćanin, T. Baković, Safe service transformation as a mechanism for interoperable integration of technologically diverse systems, YU INFO 2016.

# THE IMPORTANCE OF EDUCATION AND RAISING AWARENESS AMONG CITIZENS ABOUT DIFFERENT FORMS OF ATTACKS IN CYBER SPACE

**Nebojša Jokić**[1]
Computer Emergency Response Team (CERT),
Ministry of Interior of the Republic of Serbia
**Aleksandar Maksimović**[2]
Computer Emergency Response Team (CERT),
Ministry of Interior of the Republic of Serbia

**Abstract:** Use of the Internet and modern information and communication technology permeates all spheres of social life today. Large-scale expansion, development and implementation of information and communication systems in all fields provide real opportunity and the possibility of today's man to adequately respond to the growing challenges of the modern era of civilization. In parallel with the development and use of new technologies and systems, growing threats to their security is therefore a threat to the safety and security of citizens. There is almost no individual who has not experienced a phishing attack, social engineering or ransomware. For these reasons, many countries in the world build and strengthen the capacity of the information security system, and legal and institutional frameworks, in order to be able to respond to the growing security challenges, risks and threats in the cyber environment. But all this has no real effect, and every form of protection falls apart, if each one individually is not educated and do not raise awareness in this field.
**Keywords**: raising awareness, cyber attacks, internet, ICT, information security.

## INTRODUCTION

Almost a half of the century has passed since the appearance of the first digital computers. Although modest in scope, and large in size, they were initially intended to facilitate and accelerate complex calculations in scientific and technical fields, as well as to process large amounts of data both in business and administrative fields. The appearance of modern computers, the widespread distribution and large quantity of various user programs has affected life of ordinary people all around the world. This technology provides enormous opportunities and greatly facilitates our lives. Today's computers are becoming smaller in dimensions, yet with a drastic increase in performance and are used in almost all scientific fields of planning, data collection, calculations and data processing, analysis and design processes and evaluation of the same. For example, in teaching, education, traffic, communication, information, education, art, entertainment, device management, security, artificial intelligence, etc. However, it must be understood that modern technology brings with it a lot of risks.

1 nebojsa.jokic@mup.gov.rs
2 aleksandar.maksimovic@mup.gov.rs

The development of computer networks, their expansion and integration into the system of the global network – the Internet, leads to abuse in the sense of violating its originally designed function – communication and information transfer. Technology, on the one hand, has become a powerful tool, but it can be misused, as it has become globally accessible, and therefore increases the number of potential risks from attacks on the Internet. The Internet has increased the ease and speed of unlawful activities, eliminating physical limitations and reducing the physical effort of fraud. Illegal activities can be caused by a variety of forms of malicious programs or a direct attack by a malicious attacker. The reasons for the occurrence of these attacks are different and generally can be divided into material and immaterial motivation. In the first place, the reason is the acquisition of financial profit. Other motives for attacks on the computer systems include the challenge, curiosity, self-certification, data theft, espionage and others.

According to recent research, this technology is used by nearly 2.5 billion world population, and therefore it must be understood that it brings with it a lot of risks. On the one hand, technology can become a powerful tool in our hands, but it can also be directed against us because it has become globally accessible.[3] Unfortunately, we can conclude that such technological progress has accompanied the development of the idea of using new technologies for illegal purposes. The Internet has increased the ease and speed of criminal activities, removing physical limitations and reducing physical effort to deceive someone. For example, billions of dollars can be stolen in the "online" environment in a matter of minutes from the bank, in contrast to the time before the onset of the Internet when robbers physically robbed banks and were limited by time and amount of money they could take out of the bank, with a huge amount of physical energy they had to spend. Unlike the first computers that were isolated from the influence of other computers, after the beginning of their mass production, computer networks were designed in a very short period of time in order to share and distribute data on different computers to individual or all users of a particular network. Examples of such networks can be found practically in every organization today, whose employees use computers in their work, networked into a unified system for easier and faster interaction. Unfortunately, such system is twice vulnerable – both from the outside and from the inside.

Information security involves very complex processes that involve different aspects of the use and protection of information technologies, and above all the process of defining responsibilities for all participants in these systems, because they are generally the most sensitive place in any security scheme. The "human" factor can annul the best protection: a malicious worker, a careless worker, a worker who is not aware of the policy and the importance of security of the system as a whole (organization), and above all the security of information assets as its key element.[4]

In line with all the facts presented, it is stated that information security is the cornerstone of security in the broadest sense of the word and it becomes a priority for the preservation of business and all other state and social goods and processes.[5] The first step in creating this ambiance is a well-designed security system that should be awareness-raising and building a culture of information technology users in order to be able to recognize security challenges, risks and threats in cyberspace and to adequately respond to them.

3 Bjelajac, Ž., Zirojević, M.: *Security culture in the globalization era*, Institute for International Politics and Economy, Belgrade, 2014.
4 Milanović, Z., Radovanović, R.: Information-security culture – imperative of contemporary society, NBP: Journal of Criminal Justice and Law, No. 3, Academy of Criminalistic and Police Studies, Belgrade, 2015
5 Whitman, E. M.; Mattord, J. H.: *Principles of Information Security*, Fourth Editional, Course Technology, Cengage Learning, 2012.

## Types, forms and ways of manifesting attacks in cyber space

Attacks in the cyber space can have different motives, goals and methods, and according to these characteristics, divisions can be made. As in other areas, the motto defines the goal, and then, depending on the goal, the resources available, the object of the operation, and methods of attacks to achieve the goal are selected.

When it comes to cyber attacks, ones think first of cyber crime. In this type of attack, the primary motive is financial gain, and categories can be traditional such as scams or forgeries, through the distribution of illicit materials such as child pornography, to the endangering of other information systems. The perpetrators of these attacks can be individuals, small groups, as well as members of organized criminal groups with large logistical support.

| Offering | Price |
|---|---|
| 1-day DDoS service | US$30-70 |
| 1-hour DDoS service | US$10 |
| 1-week DDoS service | US$150 |
| 1-month DDoS service | US$1,200 |

| Offering | Price |
|---|---|
| Bots (i.e., consistently online 40% of the time) | US$200 for 2,000 bots |
| DDoS botnet | US$700 |
| DDoS botnet update | US$100 per update |

| Offering | Price |
|---|---|
| Winlocker | US$10-20 |
| Winlocker builder | US$20-25 |
| Winlocker source code | US$8 |

*Figure 1. Price list of online attack services.*

Cyber crime has a steady growth in recent years, both in absolute terms and in relation to other forms of crime. Attacks can be carried out in a variety of ways, from relatively simple to highly sophisticated, and very often starting with some form of social engineering or social engineering is applied at some stage of the attack. Lately, the dominant form of cybercrime is the various forms of locking computer resources or user files and requests to pay for redemption to unlock resources or files. In order to lock, the user must be convinced by a social engineering method to initiate malware execution, which is called ransomware due to the its specificity. When ransomware locks resources or files, the user receives a message with a lock notification, the amount requested for unlocking, instructions, and a payment deadline.


*Figure 2. A file encryption notification window and a payment request.*

Locking resources occurred in January this year in the famous hotel in Austria, where the criminals were able to take control of the information system and in a moment lock all rooms in the hotel so that guests are not able to get into them, disable the hotel staff to make a valid card to unlock the door and made a request for the purchase of two bitcoins (about $ 1,800 at the time). Hotel management very quickly accepted the claim and paid the ransom, after which the criminals enabled staff access to information system.[6]

Another example of ransomware emerged in California, where the criminals in February 2016 encrypted files in the information system of a hospital. Criminals have made a request for the amount of 40 bitcoins (about 17,000 US dollars at the time) to deliver the decryption key, which the hospital accepted.[7] According to the competent authorities of this hospital, it took 10 days to restore the information system to the state before the attack. By the end of 2016 at least 13 similar attacks on hospitals in America was reported.[8]

In these two examples, criminals were paid after the ransom and enabled users to restore the information system and data to the state before the attack, but it is important to note that, statistically, this happens in about 80% of cases, but in 20% of cases, criminals do not allow unlocking of the systems after the ransom is paid.[9] Also, in some cases criminals repeated attacks if the operators of the information system did not make the necessary actions to ensure their system.

Operations in cyberspace are among the activities of many armies for a long time. In fact, these activities may have offensive and defensive character. Due to the increasing dependence the society of information and communication technologies, disturbance of the normal functioning of these systems can do damage comparable to the conventional weapons

6 The New York Times: *Hackers Use New Tactic at Austrian Hotel: Locking the Doors*, January 30, 2017.
7 CBS San Francisco: *California Hospital Pays $17,000 To Hackers In "Ransomware" Attack*, February 18, 2016.
8 Healthcare IT News: *Ransomware: See the 13 hospitals attacked so far in 2016*, October 05, 2016.
9 Kaspersky Security Bulletin 2016: *Story of the Year: The Ransomware Revolution.*

attack. For these reasons, the activities in form of warfare which are conducted in cyberspace are called cyber warfare.

An example of cyber warfare occurred during the Russian-Georgian war that took place in August 2008. Cyber attacks on the site of the Georgian president began in July with the aim of preventing access to it, and continued in August during the armed conflict. During this period, the Georgian side was exposed to cyber attacks on the website of Georgian institutions (President, Parliament, Ministry of Foreign Affairs), news agencies, commercial organizations. Complete Internet traffic was rerouted from Georgia through Russia for the most part of this period, and many servers were inaccessible due to massive DDoS attacks. At the time of the ceasefire, on 14 August, most of the servers in Georgia were unavailable. The Russian side after the conflict has denied any involvement in the attacks and attributed them to a Russian crime group.[10]


*Figure 3. Hacked site of the Georgian Ministry of Foreign Affairs.*

Iran's nuclear program was for many years a stumbling block in relations between Iran and Western countries. Because of the different positions on this issue Iran was under sanctions, but the nuclear program progressed. Iranians were careful and kept their information systems separate from the Internet, but that was not enough to be protected. Malware was inserted in the information systems, which caused the irregular rotation and irreparable physical damage to the centrifuge for enrichment of Uranium (it is estimated that one fifth of total number of centrifuges were destroyed), which set back Iranian nuclear program for several years. This case is interesting for several reasons, firstly because it is not a true "cyber" attack because it has not used the network, and then it was necessary to prepare a very complex involvement of experts of different profiles. US officials have admitted their involvement and cooperation with Israel in this operation.[11]

Lately, more attention is paid to cyber terrorism, which is understandable in circumstances of recent classic terrorist attacks. The aim of cyber terrorists is not money, but as classical terrorism, to cause suffering, panic and distrust in state institutions, as well as the application of various forms of damage to resources that are essential to the daily lives of people, especially systems that belong to critical infrastructure.

10 The New York Times: *Before the Gunfire, Cyberattacks*, August 12, 2008.
11 The New York Times: *Obama Order Sped Up Wave of Cyberattacks Against Iran*, June 1, 2012.

To accomplish their goals, cyber terrorists apply various kinds of cyber attacks. One of the known examples of cyber terrorism was hacking the website of the French TV station TV5MONDE, whose program is distributed in more than 200 countries, when the pictures of fighters of the Islamic State with combative message were left.[12] This act of cyber terrorism did not have a destructive character, but it achieved the goal because it has caused a lot of media attention and demonstrated that the Islamic State had in their ranks individuals with special knowledge and skills, and that the systems of some of the most important institutions are vulnerable to attacks from cyber space.


*Figure 4. Site Hacked TV5MONDE.*

Cyber terrorism will in future certainly be in the focus of the security services, because it showed that terrorists have no scruples in their activities, nor respect to the international law and customs.

Because of its nature that provides access to all the devices that are connected to it, the Internet is an ideal tool for cyber espionage. Many of the data, in particular those relating to personality (primarily thanks to social networks) can be reached by using legal methods. However, for accessing the information that are protected, illegal methods must be used, usually a combination of different types of attacks. Cyber espionage is specific because the attackers are trying to remain undetected, as long as possible, and extract data from systems they are able to penetrate.

Several detected intrusions into computer systems are published. From these examples one can see the sophistication of attacks and assess their implications. The most famous example is the operation called "Titan Rain" during which the attackers for at least three years drew data from information systems related to the US defense industry. It was confirmed that the computers used for attacks are located in China, but it could not be determined whether

12 France 24: *France's TV5Monde targeted in "IS group cyberattack"*, April 9, 2015.

it is a state-sponsored espionage, or just criminals from China or any other country that has used (generally) very insecure computers in China.[13]

In some cases, the attackers were motivated by ideological reasons or personal desire to somehow harm the exact particular institution, organization or individual. These activities may be related to the reduction in the availability of resources of the attacking entity on the Internet, making difficulties for doing business, reputational damage and the like. Characteristic of these attacks is that the attackers do not have any financial benefit from the attack and have no intention to harm anyone except attacked subject, which these attacks classify into a separate group called cyber vandalism.

Some authors under cyber vandalism classify the use of social networks and other forms of mass communication in order to organize meetings that are not officially approved and which have elements of the fight against the current government, such as those in Arab countries in 2010 and 2011 ("the Arab spring").

The most famous examples of cyber vandalism are related to activities that a group calling itself Anonymous occasionally performs, which carried out attacks on the resources of the countries and institutions that are deemed to violate human rights. Some of the most popular activities of this group are hampering access to the site of the Church of Scientology in the United States, public disclosure of the names of 1,589 members of a pedophile website, hacking of Donald Trump's site after the announcement of the intention to ban Muslims entry into the United States or publishing the names of about 1000 members and sympathizers of the Ku Klux Klan.


*Figure 5. The mask is a symbol of Anonymous.*

For each attack on the information systems certain techniques are used, those that are considered to be the most suitable at given moment. On the other hand, information systems connected to the Internet are using a variety of technologies to protect against attacks in order to remain accessible to their customers and preserve information and resources. Today's

13 Washington Post: *Hackers Attack via Chinese Web Sites*, August 25, 2005.

technology, when properly implemented, can provide a fairly high level of security to the information systems that it protects, but it is not omnipotent. Regardless of all investments and technologies that should cover every known attack, there is always a human factor that can drastically affect the security of information systems. A large number of attacks on information systems begin with some form of social engineering that is applied to the regular users of the system, in order to obtain information about their credentials, privileges they have on the system or the characteristics of the system, so that attackers can implement the most appropriate technology in the later stages of the attack. To reduce the risk of this form of threats, users of the information system must have a high awareness of methods and ways of an attack and how the consequences can be avoided.

## The necessity of the development of security awareness and safety culture of ICT users in cyberspace

Various authors define the notion of "safety culture" in various ways, but in general under security culture we may consider "a set of security activities that are reflected in the recognition of hazards, responding to it, avoiding the threats, eliminating the hazards or by referring to those entities how to act professionally and how to preserve endangered values".[14] This means that the safety culture needs to help users understand the security challenges, risks and threats, and to teach them how to adequately respond to them.

Safety culture has reflection, directly or indirectly, to overall security of ICT users and protection against risks to which they are exposed. Accordingly, three main elements of safety culture can be distinguished:[15]

- technology
- policies, and
- rules and beneficiaries.

These elements are in constant correspondence with each other and each of them has a direct impact to the other two. User's policy or rules affect how the use of technology, and the daily development of new technologies require new policies. For the establishment of the security elements of the organizational culture it is necessary to implement five vital components of security culture (Figure 6):[16]

- **Information Culture** (*Informed culture*) – means that the organization collects and analyzes relevant information and actively disseminates safety information and advice on the basis of that analysis;

- **Culture Trust** (*Just culture*) – involves identifying the natural limits of human performance, and indicates that errors and unsafe user actions will not be penalized if they were unintentional, while, on the other hand, those who act recklessly, or unreasonably assume certain risks, will be disciplined;

- **Culture of reporting** (*Reporting culture*) – is creating an atmosphere where people do not have barriers to report security issues without fear of injustice, but also are encouraged and rewarded for providing information related to security. Employees need to know that culture of trust will be implemented and that authorities will act according to the information submitted; otherwise they will decide that there is no benefit from their reporting;

14 Stanarević, S., Ejdus, E .: *Glossary of Security Culture*, Center for Civil-Military Relations, Belgrade, 2009.
15 Roer, K.: *Build a Security Culture*, IT Governance Publishing, United Kingdom, 2015.
16Chia, A., Ruighaver, B., Maynard, B.: *Understanding Organizational Security Culture*, Proceeding of PACIS Japan, 2002.

- **The culture of learning** (*Learning culture*) – means that the organization is able to learn from its mistakes and is ready to make changes. The purpose of the culture of learning is that people understand the processes of management of the security system by personal example;

- **Cultural adaptation** (*Flexible culture*) – means the type of culture in which people and organizations are able to effectively adapt to changing requirements.


*Figure 6. Diagram of vital components of security culture.*

The security awareness of ICT users is a segment of the security culture and basically represents the knowledge or perception of certain situations or fact of a phenomenon, in this case in the field of information security. Safety awareness is related only to users of ICT, and people, as opposed to the security culture, which represents the cohesion of technology policies (rules) and people.[17]

Security awareness helps people to understand or be aware of the importance of education and training related to security. The aim of the training is actually a practical application of newly acquired knowledge and behavioral change in the use of new technologies, a knowledge of something is only one step towards changing this behavior.[18] In the cognitive process of acquiring new knowledge four steps are most important:

- attention
- memory
- reproduction and
- motivation.

17 Vroom, C.; Solms, R.: *Towards information security behavioral compliance*, Computers & Security, 23(3), 2004.
18 Milanović, Z., Radovanovic, R .: *Information-security culture – the imperative of modern society*, NBP: Journal for Criminology and Law, No. 3, Academy of Criminalistic and Police Studies, Belgrade, 2015.

All of them are equally important in educating users and raising their awareness to a higher level. Studies on security awareness have shown that the vast majority of users of information technology has no elementary education, nor the necessary knowledge in the field of information technology. That is a particular problem and practically impedes them of the clear definition and presentation of their own requirements and needs, as well as in understanding the actual features, benefits and limitations of digital life. This is particularly evident in situations where ICT users become victims of attacks in cyberspace, especially among employees in organizations, because adverse consequences may have far-reaching conditions. In order to properly overcome the above problems, and in order to properly protect against different forms of cyber attacks in the environment, it is essential that users of ICT systems in developing security awareness systematically carry out the following steps (Figure 7):[19]

- **Identification of threats** (*Identify threats*) – means understanding the external threats to cyber security of the organization itself, but also the interior threats due to improper use of ICT resources and lack of security awareness of employees,

- **Identification of vulnerability** (*Identify vulnerabilities*) – means the inventory of used systems with direct and indirect communication links, understanding the result of cyber security threats to these systems and the possibilities and limitations of existing protection measures,

- **Assessment of risk exposure** (*Assess risk exposure*) – implies positioning the likelihood of vulnerabilities of used systems from external threats, as well as the likelihood of vulnerability to which they are exposed due to their improper use. It also includes the determination of the security and protective effects on any individual or combination of vulnerability due to the use of the system,

- **Developing measures to protect and detect threats** (*Develop protection and detection measures*) – a reduction in the likelihood of vulnerabilities of used systems through protection measures, as well as reducing the potential impact on vulnerability due to the use of the system,

- **Establishment of contingency plans** (*Establish contingency plans*) – includes determining of response plans to minimize the impact of threats, which is implemented in order to protect the organization itself,

- **The response to cyber incidents of security** (*Respond to cyber security incidents*) – means the response to cyber security threats, which is realized by means of a plan of response and evaluation of the effectiveness of the plan for review and response to threats and vulnerabilities.

19 Martins, A., Eloff, J.: *Information security culture*, In: IFIP TC11 international conference on information security, Cairo, Egypt, 2002.

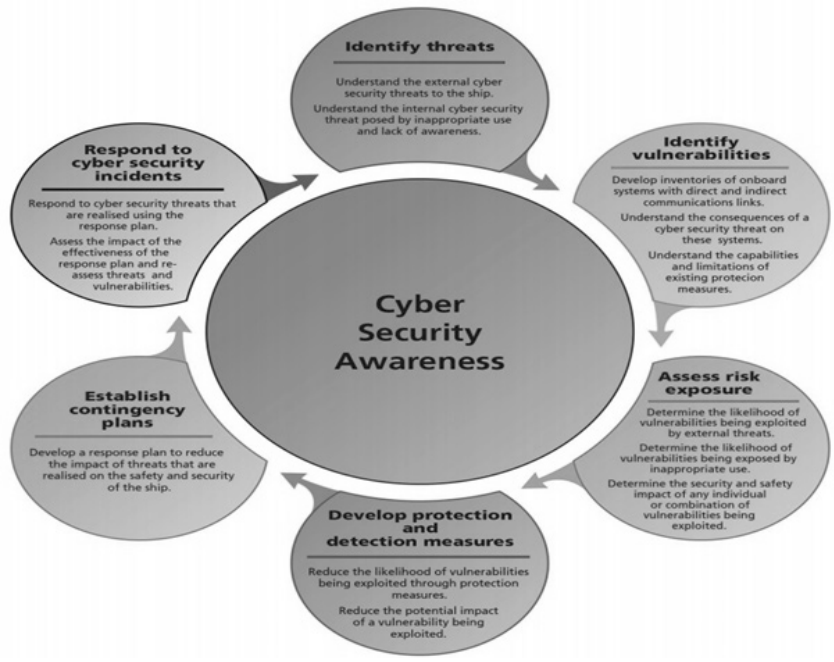



*Figure 7. Diagram of raising security awareness in cyberspace.*

## Methodology to raise security awareness and security culture and system of education of end-users of ICT in cyberspace

When creating a plan to raise security awareness and culture of information security to the employees in the organization, as well as to the individuals, it is necessary to define the following factors:[20]

- personal responsibility and loyalty of employees
- operations management
- security policy
- Code of Business Ethics and Behavior.

**Personal responsibility and loyalty of employees** is reflected in the handling and the use of information technology, such as: safe behavior in dealing with public and shared data and information, the way in which benefits hardware (flash drive, CD/DVD, computers, servers, mobile devices, etc.), software (operating systems and applications, backups, antivirus and firewall protection, etc.), networks (Internet and intranet, accessing other informational assets and services, copying large files, etc.), followed by the working environment and respect of all other procedures and security measures.

**Management activities** should stimulate, encourage and suggest employees to actively participate in the programs of education and training. Active participation of employees in the scheduled programs is the basis of security. These programs should provide sufficient knowledge of the needs and how to protect themselves, to explain the reasons for the ob-

20 Schlienger, T., Teufel, S.: *Information security culture – from analysis to change*, International institute of management in telecommunications, University of Fribourg, 2003.

servance and implementation of standard measures and procedures of protection, as well as to answer why information security is important to the organization. Adoption of new knowledge and changing perceptions of employees, as well as the practical application of the appropriate level of expertise and ability to jurisdiction in a particular situation, are the basis for the success of any security system. Also, education programs and training for employees should include specific technical issues related to security (using popular social networks and services, sending e-mails, browsing the Internet, and defense against malicious users and their destructive products). The quality of education and training should be regularly check, and periodically upgraded.

**The security policy** is one of the key elements of the methodology of raising the awareness of employees and represents a set of rules concerning access to and use of information technology and organization.[21] Security Policy prescribes a framework for best practice that can be understood and implemented by all employees to ensure the minimization of risks and effective response to different types of security incidents. General requirements and recommendations of the security policy include the following:[22]

- organization is the owner of the entire data property, as well as of all processes and electronic transactions;

- degree of protection and maintenance of IT assets should be raised to the highest possible level using all the recommendations of security experts and manufacturers of IT hardware and software, as well as all available funds;

- management is responsible for establishing and enforcing standards and procedures, as well as to control access to informational assets of the organization and control of user access to the Internet and Intranet, and their personal example should demonstrate and support the raising of awareness of the need to protect information assets, as well as through various levels of training aimed at self-protection and reducing the risk of attacks in cyberspace;

- new employees, like everyone else, must also sign the Statement on keeping and protection of confidential information, before receiving user accounts and permissions to enter the informational assets;

- users to whom security policy is intended are obliged to comply with the law to protect it, as well as to reference standards, guidelines and procedures of protection that is supportive;

- users of the computer system are obliged to take care of the entire IT assets (hardware, software, computer networks and data) and in case of perceived irregularities (defects, faults, deficiency etc.) to notify the competent person; this report must contain date, time, a detailed description of the identified problem and signature;

- users must commit to use informational assets properly and adequately to their licenses, which means that the following is not allowed: uncontrolled use of network resources and equipment for storing of private files (movies, music, pictures...) on a server or workstation, preinstallation and adjustment of existing software, as well as the installation of new, particularly unlicensed software, using other people's accounts and phishing, use and destruction of other people's data, assault and damage to other computers in the local network and Internet, inappropriate behavior on the Internet and sending compromising emails and messages that are spam, login to the forums, chat groups and other Internet services, as well as leaving the address of the organization;

21 Randjelovic, D .: *Management information systems and their protection*, Edition monographs, Academy of Criminalistic and Police Studies, Belgrade, 2014.
22 Zakaria, O.: *Understanding challenges of information security culture: a methodological issue*, The second Australian information security management conference, Perth, Australia, 2004.

- users must commit to remove known vulnerabilities in the system through regular updates of operating system, antivirus software and other user applications, and will not turn off protection programs on the system nor circumvent security dialogues;

- users must not make unauthorized copies of data and software and have only authorized access to systems and data;

- users must create a strong security passwords and keep them secret, as well as other identifying parameters for access to the system;

- users must commit to regularly make backup copies of all important files from its computers to a separate media or other disks that are not permanently connected to a computer (portable drives, fast memory, CD, DVD, etc.); backup on the Internet (cloud backup), which provide independent access to the resources of the site, are not recommended, but for those who have to use it is necessary to turn off automatic synchronization; also, users, where this option is available, should not publish personal data (scanned identity documents: identity cards, passports, credit cards, health cards, pictures, unprotected works of authorship, anonymous messages) and everything that could directly jeopardize their privacy as well as business information if they do not have a permit of management;

- users must use the so-called secure computers or virtual machines for experimentation, risk websites, opening suspicious e-mail, etc.;

- users must commit that downloading programs from the Internet is always carried out by authorized distributors and from sites of manufacturers (safest programs are open source, but the most dangerous are free);

- users will not install programs using link received by e-mail, social networks, chat, and so on without first verifying authenticity and validity of the same;

- users will not open e-mails received from unknown sender and will not send messages with personal or organization's confidential data;

- users must completely remove from use operating systems and programs for which there is no support of manufacturers;

- users must commit themselves to implement the policy of "blank screen" and "empty desk"; all employees should finish their working time with regularly shut down all active connections to remote computers, as well as its computer system; employees should take care to never leave open on the desk unattended confidential information (electronic and optical media, documents and notes);

- all user's computers and server stations must have digital certificates, which are issued by trusted certification authority, and used for unique identification of a computer;

- there must be a mandatory physical disjunction (separation) of Internet and Intranet network and segmentation of system to the functional units; a demilitarized zone for communication should be established between Intranet and Internet network; network gateway between public and private network must be controlled and monitored by firewall services, behind which a detector of intrusion into the internal network have to be installed (IDS/IPS type) which detects all attacks to the network, as well as vulnerabilities of configuration of the border firewall;

- security policy should be published and made available to all users.

**Code of Business Ethics and Behavior** in information security is a document that applies to all employees and whose purpose is to instruct them how to adapt their behavior on working environment, in accordance with ethical and professional standards and generally accepted values.[23] The Code should contain the following elements:

23 Chang, S. E.; Ho, C. B.: *Organizational factors to the effectiveness of implementing information security*

- attitude and associates
- relationship with clients and business partners, and
- the attitude towards property.

## CONCLUSION

The Internet by its appearance imposed the global change in the way and the speed of communication, both in social life and in the business environment of modern man. It is important to point out that the Internet has brought a drastic impact on the quality of life of "the ordinary man". In addition to the usual and inevitable use in business communications, men today use the Internet as a means of carrying out daily duties. Thanks to the wide range of opportunities that the Internet provides, for example, booking plane tickets, theatre, buying and selling various goods, providing services, watching TV, adjusting air conditioning, communicating and performing many other tasks dictated by the pace of life and work of modern man, the quality of life of every individual is raised to a higher level. Not surprisingly, the prevailing opinion is that the global dependence on the Internet is increasing every day.

On the one hand, it is evident that new technologies bring significant benefits to people, on the other hand they carry a number of risks to which every individual is exposed. The unlawful activity can be caused by various types of malicious programs or by direct attacks by malicious attackers. The reasons for the emergence of these attacks are various and generally can be divided into tangible and intangible motivated. First and foremost reason is to acquire financial gain, as other motives for the attacks on computer systems are challenge, curiosity, self-confirmation, data theft, espionage and others.

Devastating is the fact that at the present time on the rise is exposure of data of many organizations, companies and corporations, due to the large number of "security illiterate" and "information unconscious" personnel who have access to sensitive, and very often confidential information. The fact is that huge security implications can be made by the employee who is responsible for working with company's sensitive data, but who due to unsafe and unprofessional search of the Internet through a company's network receives and responds to emails with suspicious content, who use inadequate credentials for logging or not use them at all, who visit unsafe sites and the like.

For all results shown in this paper, it is important to constantly work on raising awareness and education about the different modalities and forms of attacks in cyberspace, both individually and collectively, because only with that approach there will be higher degree of protection in the field of information technology.

## REFERENCES

1. Bjelajac, G., Zirojević, M.: *Safety culture in the era of globalization*, the Institute for International Politics and Economics, Belgrade, 2014.
2. Vroom, C.; Solms, R.: *Towards behavioral information security compliance*, Computers & Security, 23 (3), 2004.
3. Zakaria, O.: *Understanding challenges of information security culture: a methodological issue, the second Australian information security management conference*, Perth, Australia, 2004.

*management*, Industrial Management & Data Systems, 106(3), 2006.

4. Martins, A., Eloff, J.: *Information security culture*, In: IFIP TC11 International Conference on information security, Cairo, Egypt, 2002.

5. Milanović, Z., Radovanović, R.: *Information-security culture – the imperative of modern society*, NBP: Journal for Criminology and law, No. 3, Academy of Criminaistic and Police Studies, Belgrade, 2015.

6. Randjelović, D.: *Management information systems and their protection*, monograph edition, Academy of Criminaistic and Police Studies, Belgrade, 2014.

7. Roer, K.: *Build a Culture Security*, IT Governance Publishing, United Kingdom, 2015.

8. Schlienger, T., Teufel, S.: *Information security culture – from analysis to change*, International institute and management of telecommunications, University of Freiburg, 2003.

9. Stanarević, S., Ejdus, E.: *Glossary of security culture*, Center for civil - Beograd, 2009.

10. Chang, SE; Ho, CB: *Organizational factors to the effectiveness of implementing information security management*, Industrial Management & Data Systems, 106 (3), 2006.

11. Chia, A., Ruighaver, B. Maynard, B.: *Understanding Organizational Security Culture*, proceeding of PACIS Japan, 2002.

12. Whitman, EM; Mattord, JH: *Principles of Information Security*, Fourth Editional, by Course Technology, Cengage Learning, 2012.

13. Balduzzi, M.; Ciancaglini, V.: *Cybercrime and the Deep Web*, Black Hat EU, Amsterdam, 2015.

14. Goncharov, M.: *Russian Underground 101*, Research Paper, Trend Micro Incorporated, 2012.

15. Kaspersky Security Bulletin 2016: *Story of the Year: The Ransomware Revolution.*

# THE STUDY ON PREVENTION METHODS OF TELECOM FRAUD CRIME IN "INTERNET +" ERA

**Qiang Fan**[1]
Criminal Investigation Police University of China, Network Information Center, Shenyang

**Abstract:** The arrival of "Internet +" era has promoted the rapid development of relevant industries. At the same time, it has also brought a higher Internet crime rate and amount. Thus, methods and medium of telecom fraud crime are becoming "Internet +", which makes the crime show the features of rapid renovation means, involving a wide, more organized and cross-border area. As a result, it causes many difficulties in applying laws, investigating, collecting evidence, cooperating and chasing the dirty money. Therefore, how to effectively combat telecom fraud crime has become a problem to be solved in the contemporary world in "Internet +" era. This paper analyzes the new characteristics and new trend of Internet +" era of telecom fraud crime, combs the key and difficulties to prevent, summarizes and puts forward the countermeasures of telecom fraud crime of "Internet +" era, and provides a reference for the relevant law enforcement departments.

**Keywords:** "Internet +, telecom fraud, crime of fraud, prevention methods

## INTRODUCTION

In recent years, with the continuous promotion of "Internet +" process, the deep integration of social industries and information technology has brought convenient service to people. At the same time, telecom fraud also derives a series of new methods of fraud, which increases new difficulties in preventing and striking the crime. How to efficiently prevent and strike the new situation of telecom fraud crime has become a serious problem needed to be faced with and solved. Otherwise, this crime will become the bottleneck of promoting "Internet +" process.

## THE BASIC CONNOTATION AND CHARACTERISTICS OF "INTERNET +"

### The basic connotation of "Internet +"

The so-called "Internet +", can be understood as "Internet + traditional industries". Its main connotation refers to the process of integration between the new generation of information technology that is based on the Internet and the different departments of economic and social life. And this process will have a great, profound and extensive effect on human economic society.[22] The new generation of information technology includes mobile Internet, cloud computing, networking, big data, etc. The goal of "Internet +" action is to develop In-

1 58092638@qq.com
2 Ning Jiajun. Implementation Background, Connotation and Main Contents of "Internet +" Action Plan [J]. E-Government, 2015(6):32-38.

ternet advantages, to integrate Internet and traditional industries, to improve productivity through industrial upgrading, and eventually to fulfill the increase of social wealth.

**The basic characteristics of "Internet +"**

- Highly networked. The core of " Internet + "concept is the network interconnection. Entering " Internet + " era, the exchange of information is no longer confined between people and people. By using Internet technology, the exchange of information can happen between people and things, or between things and things.[33] All things can be integrated into the virtual network. And they achieve information exchange through this virtual network.

- Big data. Data is the main body of network transmission. All Internet affairs are based on data processing. In "Internet + " era, human social activities will bring lots of data in the Internet, which brings the explosive growth of data. Human society has entered "the era of big data".

- Mobile. If the core concept of "Internet +" is the network interconnection, then, the mobile Internet is the improvement of this concept. Users are no longer limited by the specific network way and region. Wide use of all kinds of mobile intelligent terminals has changed the way of users' getting information.

## THE NEW CHANGES OF TELECOM FRAUD CRIME IN "INTERNET +" ERA

**Traditional telecom fraud presents "Internet +" features**

The traditional telecom fraud is a criminal act through which criminals make up false information by telephone or SMS to cheat the victims' trust, and induce the victims to give or transfer money to the criminals.[44] However, "Internet +" expands the scope of telecom fraud, changes the operation mode of telecom fraud, enhances the convenience of telecom fraud, and puts forward a more big challenge to the prevention and control of telecom fraud. For example, the emergence and popularization of Internet phones have greatly reduced the cost of telecom fraud. The criminals can easily disguise as state organizations by using plug-in software and simulation software, which improves the success rate of fraud. Alternatively, criminals can disguise as banks and use the telephone banking password authentication mechanism to defraud victims' bank password to commit crime. In addition, criminals can easily obtain the basic information of the victims and the blank bankcards through the Internet. And criminals make the illegal proceeds of fraud legal through online banking, telephone banking, online financial investment, etc..

**The new forms of telecom fraud generated from "Internet +"**

The new forms of telecom fraud generated from "Internet +" are mainly divided into two types: to fraud victims' money directly or to obtain victims' account control right.[55] The former one mainly makes use of the non-contact feature of social networks. The criminals defraud the victims' trust by chatting, and then borrow or obtain money from them. Alternatively, they will disguise as well-known enterprises, the bank's website, customer service phone, and the staff of government departments to defraud the victims' trust, and make them

3 ZHOU Kai, TANG Ping. The New Situation and Countermeasures of Network Fraud Crime in "Internet+" Age [J]. Journal of Liaoning Police College, (5):22-27.
4 Hu Xiangyang, Liu Xiangwei, Peng Wei. Research on the prevention and control of Telecom fraud crime [J]. Journal of People's Public Security University of China (Social Sciences Edition), 2010(5):90-98.
5 Dong Bangjun, Wang Fa. The Research on the Investigation and Prevention of Telecom Fraud under the Background of "Internet +" [J]. Theory Monthly, 2016(8):109-156.

to transfer their money to a particular account. The typical performance of the latter one is that the criminals get victims' account information by various means. Then they call the victims or send fake e-mails to them by using change software and pseudo base station. Then they will obtain the victims' passwords and electronic verification codes by saying that the transaction is incorrect and the account is at risk, and at last control the victims' account and get illegal profits.

## THE PREVENTION DIFFICULTIES OF TELECOM FRAUD CRIME IN "INTERNET +" ERA

### Difficulties in applying the law

Telecom fraud is a new type of crime, and the laws and regulations that can handle such cases are not perfect. We can only deal with this crime according to the relevant laws and regulations. Moreover, every investigation department has different inconsistent understanding of the cases, and their treating standards are different too, so there are many problems in the specific operation, which affect the combating effectiveness. In addition, according to the relevant laws and regulations, the Telecom Management Bureau is responsible for supervising SMS operator to implement "mobile phone network real name system"; the CBRC is responsible for supervising Banks to implement "real name system" account; the Bureau of Information Industry is responsible for supervising Network operators to provide server and virtual space, etc.. However, to what extent should the regulations be applicable, and what kind of legal responsibilities should violaters bear, are not clearly defined, so the imperfection of the law makes the regulations become mere forms.

### Difficulties in investigating and collecting evidence

Telecom fraud is a remote, hidden and high-tech crime. The criminals, instead of making a face-to-face contact with the victims, make use of modern communication technology and Internet banking technology to complete the process of committing the crime in a very short period. Although some traces are left, these traces show as telecommunications, Internet and other intangible ways, which bring investigators difficulties in investigating and collecting evidence. Furhtermore, such criminals usually apply for relevant documents through fake identity, and it is difficult to grasp the trend after the crime. For example, VOIP network telephone gives the criminals much convenience and concealment. On the one hand, VOIP can display any number, on the other hand, the majority of servers are established overseas. Network data multiple jumping enhances the concealment, and increases the difficulties of investigation and evidence collection.

### Difficulties in investigating cooperation

Entering "Internet +" era, the tendency of telecom fraud organization and collectivization is more obvious. Their members are scattered throughout the world. From telecom fraud cases that have been solved, the main suspects are mostly scattered outside of China mainland, such as Taiwan, Singapore, etc.. Therefore, such cases often involve numerous communication and coordination issues, and involve the application of international law, which make the problem more complicated. Even in the same territory, there are still problems in investigating cooperation, because of the wide scope of criminals and victims distribution. Therefore, such cases require relevant units for collaboration, especially cross-border cooperation, which will increase the cost of handling cases, and the investigation work is sometimes difficult to continue when the cross-border cooperation mechanism is not perfect enough.

**Difficulties in chasing fraud money**

In the investigation of telecom fraud cases, the chasing of the fraud money is always a difficulty, mainly for two reasons. On the one hand, large amount telecom fraud is always cross border. Criminals usually transfer the money abroad after getting the money through international electronic exchange, underground banks and other ways, which brings great difficulties to the investigation departments to recover the money. On the other hand, even if criminals do not transfer the fraud money abroad, since they often set up many accounts to transfer money through online banking quickly and they can transfer millions of fraud money to many bankcards within a few minutes, and then they can withdraw and hide money in different places.

## THE PREVENTION METHODS OF TELECOM FRAUD CRIME IN "INTERNET +" ERA

**To make legislation perfect and enforce the law strictly**

The national legislature should provide for corresponding laws and regulations according to the new characteristics of telecom fraud in " Internet +" Era in order to ensure effective combating, which mainly includes the following points. The first one is to identify the connotation and denotation of telecom fraud clearly. The second one is to make sure that the supervising responsibilities of telecom operators, banks and network platforms are clear. The third one is to strengthen the information security legislation, to define the acts of disclosing and selling citizenship and transaction information as illegal or not. The fourth one is to standardize the selling and use of number changing software, network telephone, SMS group sending, pseudo base stations and other equipment. The last one is to regulate the starting point of punishment and sentencing standards of telecom fraud.

**To implement real name system and perfect the protection**

We should implement the financial accounts real name system, telecom real name system, electricity supplier platform accounts real name system, telecom equipment and financial sector access system, and strengthen accountability mechanisms. Banks and financial institutions should Internetwork with the public security departments to strengthen the implementation of the customer real name system. In addition, the institutions and individuals who do not implement the real name system as required should be accountable. We need to punish the acts included in opening unreal bank accounts and selling bankcards etc., and to eradicate the existence of money laundering tools of telecom fraud. We should clear the main responsibilities of telecom operators, force operators to implement the customer real name system, and seriously deal with the telecom fraud that is caused by illegal operations. We propose that when banks, telecoms, and network platforms have business relationships with the users, such as opening an account, they should sign credit contracts with the users and keep detailed transaction records. At the same time, the government should establish the corresponding personal credit file, put the personal credit information into the department network, and provide information and technical supports for the establishment of an integrity society.

**To strengthen cooperation and mutual assistance and strengthen the investigation effects**

The characteristics of telecom fraud decide that the combating of such crimes should establish multi cooperation, including cross-border cooperation and domestic cooperation. Cross-border cooperation mainly constructs cooperation model by international negotiations and legal documents. In addition, this kind of cooperation unites various departments

to combat the crime, and solves the telecom fraud investigation and prevention problems that are still in the "cross-border legal vacuum zone". Domestic cooperation includes the cooperation among different areas and the cooperation of different kinds of police. The ability of cross regional cooperation determines the quality of case investigation directly, so we should get rid of local protection ideology and weak cooperation consciousness as soon as possible. We should establish the evaluation mechanism of regional cooperation, integrate the strength of public security organizations at all levels, enhance the consciousness of cooperation, and promote the progress of regional investigation cooperation of telecom fraud.

**To strengthen propaganda and improve consciousness**

We should increase preventing propaganda to the whole society, and improve people's awareness of prevention. On the one hand, the public security organizations may make full use of radios, televisions, newspapers, networks, communication tools and other forms to make anti-fraud propaganda. On the other hand, we can organize staffs to go out and propagandize, and increase the preventing propaganda to the whole society in order to make people aware of the crime means and characteristics of telecom fraud, to expose the usual tricks of telecom fraud. Then we can increase public awareness, and warn people not to trust criminals, not to transfer money, not to give criminals any opportunity, in order to reduce the occurrence of telecom fraud.

## CONCLUSION

With the continuous advancement of "Internet +" process, the relationship between people's life and the Internet is more and more close, which also provides more resources for the criminals to implement telecom fraud. The means and media of telecom fraud also presents "Internet +" features, such as means refurbishing fast, involving a wide, more organized, cross regional area etc., which causes many difficulties in the application of the law, investigation, investigation cooperation and the chasing of fraud money, etc.. Therefore, it is necessary to improve legislation, expand the regulation, strengthen the cooperation of the investigation among telecom, finance and other departments, to standardize the behavior of the network operating companies and industries, to improve the safety awareness of the Internet users, and eventually to combat telecom fraud crime efficiently.

## REFERENCES

1. Ning Jiajun. Implementation Background, Connotation and Main Contents of "Internet +" Action Plan [J]. E-Government, 2015(6):32-38.
2. Zhou Kai, TANG Ping. The New Situation and Countermeasures of Network Fraud Crime in "Internet+" Age [J]. Journal of Liaoning Police College, (5):22-27.
3. Hu Xiangyang, Liu Xiangwei, Peng Wei. Research on the prevention and control of Telecom fraud crime [J]. A Journal of People's Public Security University of China (Social Sciences Edition), 2010(5):90-98.
4. Dong Bangjun, Wang Fa. Research on the Investigation and Prevention of Telecom Fraud under the Background of "Internet +" [J]. Theory Monthly, 2016(8):109-156.

# Topic VIII

# INNOVATIVE TECHNIQUES AND EQUIPMENT IN FORENSIC ENGINEERING

# FINGERMARK DETECTION: SHOULD WE TAKE THE RED PILL OR THE BLUE PILL?

**Andy Bécue**
École des Sciences Criminelles, University of Lausanne, Switzerland

**Abstract:** During the last two decades, the progression of research dedicated to fingermark detection has continuously gained speed, as shown by the increasing number of publications in the field. Along with the emergence of new technologies, one can witness a split in the main research interests. First, those who advocate the use of emerging technologies to offer new possibilities in terms of detection and/or gain information about the donor's lifestyle, for example. Second, those who prefer slowing down the pace to strengthen the foundation of the discipline, by gaining a better understanding of some detection mechanisms or interaction schemes between secretion and substrates. These last years have also witnessed the publication of a couple of articles proposing guidelines for people not accustomed with research in the field of fingermark detection. This approach constitutes a step further to promote quality research and strengthened conclusions, especially in regards with emerging technologies. In this context, this paper aims at introducing both trends through critical opinion. As for the title (in reference to a famous movie from the late nineties), this contribution is built to offer the readers a glance to a limitless world in which everything seems possible (blue pill) or to a world in which things are not as easy as expected, with numerous fundamental issuesstill to be addressed (red pill).

**Keywords:** fingerprint, metadetection, profiling, lifestyle, mechanism, guidelines.

## INTRODUCTION

*"You take the blue pill, the story ends. You wake up in your bed and believe whatever you want to believe. You take the red pill, you stay in Wonderland, and I show you how deep the rabbit hole goes."*

*Morpheus [The Matrix, Warner Bros. – 1999]*

One may think what such a citation could have in common with the field of fingermark detection, or how comes a fictional character is cited instead of a forensic scientist having contributed to the field. The reason is quite simple: the field of fingermark detection is currently facing two opposed approaches in terms of research interest. On one side, those who assert that it is time for fingermark detection to "evolve" and step plainly into the 21st century by encompassing the latest technologies and by going beyond the ridge pattern – towards a limitless perspective regarding donor profiling and lifestyle prediction through big data. Blue pill. On the other side, those who decide to mark the pace in favour of casework applicability and take a closer look at the foundation of the discipline – facing a diligent perspective: techniques suddenly not behaving as expected, substrates not fitting into the conventional (empirical) classification, lack of understanding about secretion/substrate interactions, poorly understood detection mechanisms. Red pill. Browsing through a couple of representative papers, this contribution will provide the readers the challenges, advantages, limitations, and perspectives associated with these two approaches. Hopefully it will also promote the consideration about how both approaches could gain from each other and how guidelines could help

optimizing the research efforts. Finally, it will be one's choice to decide which pill(s)should be taken.

Note: an extensive covering of the field is out of the scope of this contribution. Readers interested in getting a thorough view about fingermark detection and its latest developments could refer to the latest Interpol reports[1] as well as to recent monographies in the field.[2]

## FINGERMARK DETECTION

Fingermark detection constitutes a very productive field of forensic science in terms of research interest and publications. This is mostly linked to the role played by fingermarks in an investigative process (Figure 1). It can provide information about its source (an individual), about the activity linked to its deposition (from the position and orientation regarding the item), and can constitute a way to link an individual with an item (direct contact).

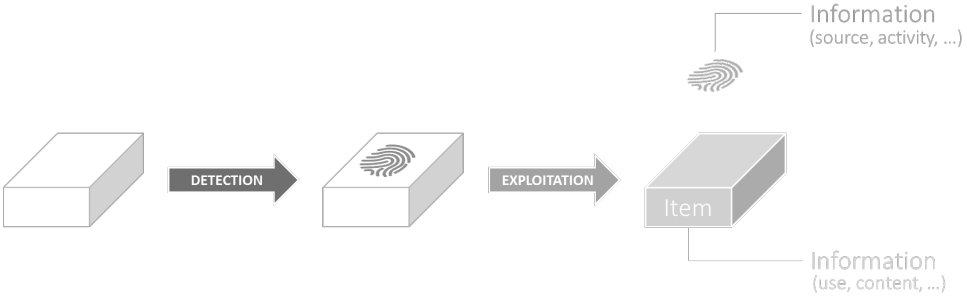



*Figure 1. Schematic representation of the integration of fingermarks in an investigative context.*

Figure 2 illustrates the evolution of the number of citations related tofingermark detection/composition since 1998. From July 2013 to July 2016, the topic associated with the highest number of publications was "powder dusting". Quite surprizing, in a way. The problematics of "contaminated marks" and "chemical imaging" followed. As such, those topics constitute two diametrically opposed approaches to detect fingermarksand reflect the torn interests between casework application, societalcontext and technological developments. At first glance, fingermark detection appears as a field mature enough to provide forensic scientists and investigators with solutions to most of the encountered situations. However, behind all appearances, fundamental issues remain open: (i) daily substrates are still considered as challenging (e.g., banknotes, leather, etc.) or hardly fit in the current categorization system (e.g., "semi-porous"); (ii) the mechanisms behind common techniques remain poorly understood (e.g., cyanoacrylate – CA, physical developer – PD, multi/single-metal deposition – MMD/SMD, vacuum metal deposition – VMD); (iii) the actual efficiency of detection sequences remain hard to assess when considering non-supervised items (about this, it is sometimes claimed that "50% of fingermarks escape detection"[3], a figure difficult to prove but illustrating a known fact regarding the processing of realistic items); (iv) knowledge about the secretion residue, its behaviour, and its interactions with underlying substrates remains incomplete.

1 Bécue&Champod, 2016; Egli*et al.*, 2013; Bécue*et al.*, 2010.
2 Champod*et al.*, 2016.
3 Jaber*et al.*, 2012.

Filling these gaps would assuredly benefit the field, for example through an overall increased efficiency of the detection process.

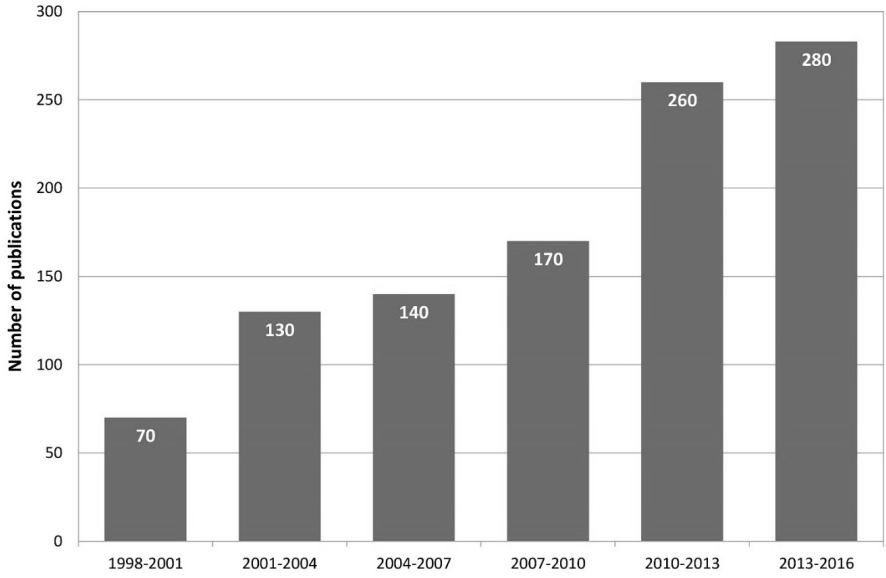



*Figure 2. Evolution of the number of articles in direct link with the detection of fingermarksor with the study of secretion residue reported in the last six Interpol triennial reviews.*[4]

## FINGERMARK-SUBSTRATE INTERACTIONS

Addressing the issue of fingermark detection by ignoring the interaction with the underlying substrate would be like developing a new technique by monitoring reactions in a spectroscopic cell. Unconceivable for most forensic scientists, unless working with solubilized secretions (which appears unrealistic in the frame of fingermark detection). A fingermark is inevitably left on a substrate. From the contact of the fingertip on the substrate and as the mark ages, a series of interaction mechanisms occur between the secretion residue and the underlying surface (e.g., diffusion, affinity, repulsion). Getting a better knowledge about these interactions would provide valuable information about the persistence of marks over time, the (detrimental) impact of some application protocols, and could help develop a more efficient way of characterizing the substrates – to cite some examples. From the early optical observations, technological development such as scanning electron microscopy provided intimate information about fingermarks and ridge morphology[5]. Using a luminescent amino acid reagent and luminescence microscopy, Almog*et al.* showed how amino acids actually penetrate into the paper matrix for 40-60 microns [6]. The amino acid penetration combined with a strong affinity for the cellulosic matrix explains why fingermarks left on paper are highly resistant over time (provided the item is not wetted). More recently, More*et al.* used different optical means to illustrate the difference in behaviour when secretion residue is left on

4 Bécue, 2016.
5 Thomas, 1978; Scruton*et al.*, 1975.
6 Almog *et al.*, 2004.

different transparent and smooth substrates[7] (i.e., glass, poly[vinyl chloride] – PVC, polyethylene – PE, polypropylene – PP). Their study illustrated how fingermarks seem to penetrate/diffuse into coated plastics quite quickly after the deposition. Atomic force microscopy was used to study the minute change of topography along the ridges of fingermarks left on polished silicon and Formica[8]. In both contributions, a dynamic process has been emphasized: the secretion residue first undergoes a transitory mobility from the ridge borders towards the substrate, before receding. Difference in physico-chemical properties can also affect the way a detection technique behaves. For example, $VMD_{Au\text{-}Zn}$ appears to rely on the formation of metal clusters during the vaporization step, whose sizes regulate the deposition of the second metal[9]. Despite these observations, the intimate mechanism of VMD remains poorly understood and application protocols are still mostly based on empirical observations. Finally, the emergence of new substrates (e.g., new series of banknotes, "anti-fingerprint" treatments for digital devices) should trigger the conduction of research projects aiming at exploring the impacts of those substrates on the detection of fingermarks. For example, it has been observed that anti-fingerprint treatments result in fingermarks of better quality compared to unprocessed substrates[10] – in return, it is likely that these marks are more sensitive to friction or shearing movements[11].

## DETECTION TECHNIQUE MECHANISMS

It is well known that several detection techniques have been imported from other scientific fields and modified to fit forensic purposes (e.g., ninhydrin – biology, PD – photography, MMD/SMD – cell staining, VMD – metal deposition). Among the existing techniques, some detection mechanisms are quite well understood. This is the case for amino acid reagents or lipid/blood stains; even if there is still room for discussion regarding molecular intermediates[12]. However, the limits to our current knowledge status are surprisingly quickly reached. One example: cyanoacrylate fuming, one of the most used techniques to detect fingermarks on non-porous substrates. Polymerization occurs through an anionic process. However, it is still hardly known which molecular species trigger the polymerization process regarding fingermarks, despite several studies aiming at identifying these initiators[13]. Similarly, the role of the ambient humidity (i.e., 80%) and the impact of the morphology of polymers on the ridge quality are still unclear[14]. The lack of knowledge becomes more noticeable when dealing with advanced techniques, such as those driven by metal deposition or physico-chemical mechanisms (e.g., PD, MMD/SMD, VMD). In the case of MMD/SMD, attempts to elucidate the interaction mechanism between gold nanoparticles and secretion residue at acidic pH failed so far. The reason is quite simple: if it is relatively easy to characterize gold nanoparticles in solution (colloidal gold), it is extremely complicated to monitor the interactions of gold nanoparticles with fingermarks while the detection is occurring. Post-detection observations are also difficult as they could induce a disturbance in the observed specimen. Up to now, different hypotheses were proposed (encompassing electrostatic interaction, hydrophobic affinity and covalent bonding), but no joint mechanism. The same is observed for PD. Luckily, research efforts were recently invested in these problematics: identification of the molecular

7 Moret *et al.*, 2015.
8 Popov *et al.*, 2017; Dorakumbura *et al.*, 2016.
9 Jones *et al.*, 2001.
10 Forchelet, 2015.
11 Stoehr *et al.*, 2016.
12 Spindler, 2010; Spindler *et al.*, 2009; Wilkinson, 2000.
13 Velthuis & de Puit, 2011; Kupferschmid, 2007; Wargacki *et al.*, 2007.
14 Paine *et al.*, 2011.

species involved in the detection of fingermarks by PD[15] or use of dye-doped functionalized silica nanoparticles to get a better understanding about how citrate-capped gold nanoparticles used in MMD/SMD could interact with the secretion residue[16] – to cite two examples. Finally, it should be noted that the lack of fundamental knowledge does not prevent techniques to evolve[17], but they make things more complicated in case of unexpected failure or imposed changes: replacement of a surfactant for ecological reasons (PD), sudden modification of the water quality (PD), or unreliable results on daily substrates (MMD/SMD).

## METADETECTION

Quite recently, a new trend emerged in the field of fingermark detection: obtaining additional information about the donor and his/her lifestyle. This way of doing can be called "metadetection" for it aims at going beyond the conventional detection purposes (i.e., recording a ridge pattern). Donor profiling can be performed simultaneously to the detection process (as in chemical imaging) or can be implemented subsequently to the detection of the mark (in that case, this could require swabbing the mark for analysis). The main argument behind metadetection is that a fingermark is much more than a ridge pattern and that donor profiling could provide valuable information to investigators (Figure 3).

Hypothetical scenario: a fingermark is detected on the handle of a knife collected in an alley, close to a dead body. Thanks to technological evolutions, a full lifestyle profiling can be obtained in less than a day: male, adult, carnivorous, uses aftershave (XXX by YYY), moisture cream (ZZZ by WWW), presents signs of diabetes, allergic to pollen and smoker. Databases are interrogated (including health insurances, supermarkets and national identity services) and the suspect is identified in a few minutes among the whole population [Note: no criminal record]. The lifestyle prediction is verified at 93% [apparently, the individual has recently stopped smoking and has started a nicotine-based treatment]. The protocol still recommends comparing his fingerprints and his DNA with the few elements of ridge pattern present on the mark and the "touch DNA" collected from it. Check, and check!

Is this scenario plausible? Worthy an Orwell's novel? It certainly raises many questions, as such prospect is already suggested by some. From a chemical point of view, it is true that fingermarks are more than the reproduction of a ridge pattern – in regards with the complex mixture of endogenous and exogenous compounds contained in the secretion residue. However, from a forensic point of view, the introduction of lifestyle information in an investigative context is debatable. It is true that some fingermarks may be slipped in such a way that they contain insufficient dactyloscopic information to reach a conclusion about the source. They are not useless either; and it is too simplistic to think that forensic scientists limit themselves to the ridge pattern (dactyloscopy), as illustrated in Figure 3. Indeed, fingermarks may contain DNA (i.e., "touchDNA"), whose analysis could lead to a source information or at least to the donor's gender. As an example of the growing success of "touch DNA"in investigations, "touch DNA" represented 85% of the DNA profiling requests linked to traces (criminal context), received by the Centre UniversitaireRomand de MédecineLégalein 2016[18](CURML, Lausanne – Switzerland).Several studies also showed that most of the fingermarkdetection techniques do not prevent the recovery of DNA[19]. It is consequently regrettable that DNA contained in fingermarks is not cited/discussed in most of the publications dealing with do-

15 De la Hunty *et al.*, 2015a &2015b.
16 Moret *et al.*, 2014.
17 Bisotti *et al.*, 2016; Moret & Bécue, 2015; Montgomery *et al.*, 2012; Houlgrave *et al.*, 2011.
18 Castella, 2017 (pers. comm.).
19 Norlin *et al.*, 2013;Bhoelai *et al.*, 2011; Raymond *et al.*, 2004.

nor profiling. When cited, DNA is quickly dismissed because it may be degraded, in insufficient amount, contaminated, costly and time-consuming. It should however be noted that all these arguments apply to chemical profiling as well.

Readers interested in the topic of donor profiling can read the following review.[20] Among the reported techniques, chemical imaging using MALDI-MSI is worth being cited as it has been continuously explored and optimized by Bradshaw *et al.* to make it compatible with an investigative process[21]. MALDI-MSI offer the advantage of ridge pattern visualization combined with molecular information. The combination of detection and donor profiling makes it interesting for future developments. More recently, proteomics combined with liquid chromatography has been applied on fingermarks left on users' mobile phones to try predicting their lifestyles.[22]

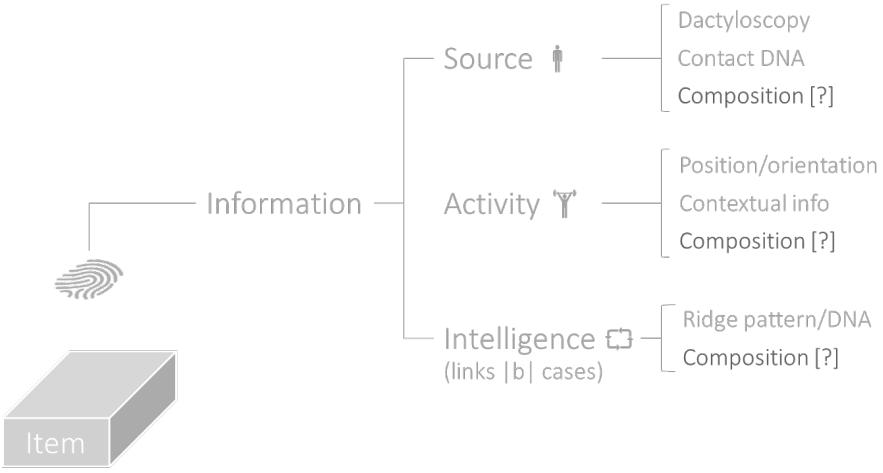



*Figure 3.Schematic representation of the range of information of investigative value that can be gathered from a fingermark. The rightest column refers to the elements that are used (or claimed to be useable) to obtain such information.*

## CHEMICAL SIGNATURE AND LIFESTYLE PROFILING

The recent study of Bouslimani*et al.*illustrates perfectly the philosophy being the metadetection of fingermarks, and more particularly lifestyle profiling[22]. Using high performance liquid chromatography and a metabolomics approach, they showed that fingermarks collected from mobile phones could provide information about the users' lifestyle. As an example, they identified molecules linked to cosmetics (e.g., sunscreen, soap, hair regrowth treatment), medications (e.g., skin anti-inflammatory, antidepressant, antifungal), diet (e.g., caffeine, aspartame, citrus and pepper derivatives) as well as to some activities (e.g., nicotine, anti-mosquito, pet pesticide). By crossing all these information, they could confirm some elements of the volunteers' lifestyle habits (e.g., regular camper, smoker). They also studied intravariability and intervariability in terms of chemical signature distance between specimens collected from phones and hands.

20 Van Dam *et al.*, 2016.
21 Bradshaw *et al.*, 2016 & 2017.
22 Bouslimani *et al.*, 2016.

In their introductive text, the authors claim:

*"Imagine a scenario where personal belongings such as pens, keys, phones, or handbags are found at an investigative site. It is often valuable to the investigative team that is trying to trace back the belongings to an individual to understand their personal habits, even when DNA evidence is also available […] The collective repertoire of molecules found on these objects provides a sketch of the lifestyle of an individual by highlighting the type of hygiene/beauty products the person uses, diet, medical status, and even the location where this person may have been […] Such information could help a criminal investigator narrowing down the owner of an object found at a crime scene, such as a suspect or missing person."*

The last sentence is certainly the one raising most of the questions regarding the usefulness of lifestyle profiling, or its application field. This brings forward the notion of "relevancy" regarding the information that can be obtained from a trace or an item (for an extensive covering of the topic: [23]). What information is to be considered as relevant in an investigation? When does an information become irrelevant or counterproductive to the investigative efforts? The goal of any investigator is indeed to narrow down the number of suspects to a limited pool of individuals, more prone to the investigative process. To reach that goal, an investigator generally relies on contextual information, traditional investigative efforts (e.g., witness interview, suspect audition), and information provided by traces of forensic interests (e.g., fingermarks, DNA, shoemarks, fibers). Currently existing databases (mostly fingerprints and DNA) prove to be extremely helpful as they can actually help investigators to narrow down the pool of suspects in an efficient manner. Such databases are indeed directly linked to an individual (biological identity) and may provide a name quickly if someone is already known to the authorities. Unless expecting a global population surveillance combined with big data analysis, it appears quite unlikely that medication, diet, or daily products – as part of lifestyle habits – could help narrowing down efficiently the pool of suspects. In the same context, the item on which a fingermark is found also constitutes a source of information. In the example of lifestyle profiling obtained from fingermarks left on mobile phones, investigators would certainly have gained valuable information about the identity of the phone's owner and his/her lifestyle by investigating the digital content of the device (digital identities, diary, phone numbers, pictures/videos, etc.). Technological possibilities should consequently not obliterate common sense solutions in regards with the investigative process.

In favour of lifestyle profiling: the technological ability to gain information about secretion residue in terms of a chemical signature certainly constitutes an asset regarding the fundamental study of fingermarks. Indeed, it could help getting a better understanding about donor variability, about its impact on the efficiency of detection techniques, and may eventually provide an evidential tool comparable to DNA. The goal would consequently not consist in predicting someone's lifestyle but rather to get a comprehensive vision of secretion residue as a whole, which would go beyond the conventional "sebum-rich", "eccrine", or "natural" distinction. Further researches on this topic are consequently expected in near future. Additionally, donor profiling could be useful from a healthcare, medico-legal or security perspectives (devices).

## GUIDELINES

Working with fingermarks is certainly not the simplest way of doing research as each fingermark is a specimen. It is consequently impossible to obtain a reproducible set of "identical"fingermarks. Despite its apparent simplicity (asking someone to leave one or several fin-

23 Hazard, 2014.

germarks), the design of a research plan linked to fingermarks requires many questions to be answered: What kind of secretion (natural, sebum-rich, eccrine, artificial)? How many donors? Fresh or aged marks?Unique deposition or depletion series? Which comparison protocol (half marks, pseudo-operational test, etc.)? All these questions must be carefully thought and answered at the early stages of a study as they could strengthen or weaken the conclusions. Willing to increase the quality of research in the field, the forensic community provided hints and guidelines[24]. The underlying aim is to refer to them and discuss any deviation from the proposed recommendations.

In the same context, the use of artificial secretion is still debatable as it is extremely difficult to simulate the complexity of the natural emulsion present on fingertips as well as the variability between donors. However, latest developments showed that complex emulsion could be synthesized and seem to behave similarly to natural ones[25]. It is consequently awaited that additional research in this field may provide a way to obtain reproducible fingermarks. This could become valuable in the early stages of development of a detection technique or for proficiency testing purposes.

## RED PILL?BLUE PILL? – OR BOTH?

The aim of this contribution was not to point out a negative vision of the field. On the contrary. Dozens of efficient detection techniques are currently available to detect fingermarks on a wide range of substrates. Moreover, detection sequences are continuously optimized to increase the success ratio regarding latent marks to be detected on an item. The field has continuously evolved since the mid-50s, even if the main developments occurred in the 1980s-1990s. It is true that some fundamental knowledge is still missing: interaction of the secretion residue with the underlying substrate, intrinsic detection mechanisms, etc. But it is reassuring to see that groups of scientists are currently spending time and efforts to enlighten these shadow areas. The field definitely benefits from strengthening of its foundations: increased rates of success with "difficult" substrates, optimized characterization of substrates, ability to react when facing a sudden modification in a technique efficiency, etc. It also reflects the fact thatfingermark detection is still "young" in a sense and requires the community to spend time on its foundations.Once detected, a fingermark can represent a valuable source of information, but it must be recalled that almost nothing can be done if the mark remains latent.

On the other side of the looking-glass: donor profiling. The main argument behind profiling is the fact that some fingermarks may be of insufficient quality for dactyloscopic purposes. In that context, two visions are opposed: the chemical one and the forensic one. Beyond the proof-of-concept, it is now awaited that donor profiling finds its place in the forensic context. Should it be closely related to the investigative field, then researchers should prove how lifestyle information could actually help an investigator narrowing down the number of suspects. Should it rather constitute a new technological way to strengthen the fundamental knowledge regarding secretion residue, then research should focus on a new way to characterize them. Finally, should it rather be used for healthcare or security purposes, thenfingermarks certainly constitute a non-invasive way of providing valuable information.

To conclude: fingermarks are assuredly a very exciting field for researchers. From the foundations to the emerging technologies, the field has yet to gain from scientific efforts.

So? … Which pill will you take?

24 IFRG, 2014; Sears *et al.*, 2012; Kent, 2010.
25 Sisco *et al.*, 2015.

## REFERENCES


1. Almog, J., Azoury, M., Elmaliah, Y., Berenstein, L., & Zaban, A. (2004). Fingerprint's Third Dimension: The Depth and Shape of Fingerprints Penetration into Paper-Cross Section Examination by Fluorescence Microscopy. *Journal of Forensic Sciences, 49*(5), 981-985.
2. Bécue, A. (2016). Emerging fields in fingermark (meta)detection – A critical review. *Analytical Methods, 8*, 7983-8003.
3. Bécue, A., Champod, C. (2016). *Fingermarks and Other Body Impressions – A Review (July 2013 – July 2016)*. Paper presented at the 18th Interpol Forensic Science Symposium, Lyon (France).
4. Bécue, A., Egli, N., Champod, C., & Margot, P. (2010). *Fingermarks and Other Impressions Left by the Human Body – A Review (August 2007 – July 2010)*. Paper presented at the 16th Interpol Forensic Science Symposium, Lyon (France).
5. Bhoelai, B., de Jong, B. J., de Puit, M., & Sijen, T. (2011). Effect of Common Fingerprint Detection Techniques on Subsequent STR Profiling. *Forensic Science International: Genetics, 3*(1), e429-e430.
6. Bisotti, A., Allain, C., Georges, J.-L., Guichard, F., Audebert, P., Barbosa, I., & Galmiche, L. (2016). New Lumicyano Kit: Comparison Studies with the First Generation and Effectiveness on Nonporous Substrates. *Journal of Forensic Identification, 66*(6), 560-575.
7. Bouslimani, A., Melnik, A. V., Xu, Z., Amir, A., da Silva, R. R., Wang, M., Bandeira, N., Alexandrov, T., Knight, R.,&Dorrestein, P. C. (2016). Lifestyle chemistries from phones for individual profiling. *Proceedings of the National Academy of Sciences, 113*(48), E7645-E7654.
8. Bradshaw, R., Denison, N., & Francese, S. (2016). Development of operational protocols for the analysis of primary and secondary fingermark lifts by MALDI-MS imaging. *Analytical Methods, 8*(37), 6795-6804.
9. Bradshaw, R., Denison, N., & Francese, S. (2017). Implementation of MALDI MS profiling and imaging methods for the analysis of real crime scene fingermarks. *Analyst, 142*(9), 1581-1590.
10. Castella, V. Unit head, in charge of the expertise and research activities of the forensic genetics unities at the Centre Universitaire Romand de Médecine Légale (CURML, Lausanne - Switzerland); personal communication - May 2017.
11. Champod, C., Lennard, C., Margot, P., & Stoilovic, M. (2016). *Fingerprints and Other Ridge Skin Impressions - Second Edition*. Boca Raton, Florida: CRC Press LLC.
12. De la Hunty, M., Moret, S., Chadwick, S., Lennard, C., Spindler, X., & Roux, C. (2015a). Understanding Physical Developer (PD): Part I – Is PD Targeting Lipids? *Forensic Science International, 257*, 481-487.
13. De la Hunty, M., Moret, S., Chadwick, S., Lennard, C., Spindler, X., & Roux, C. (2015b). Understanding Physical Developer (PD): Part II – Is PD targeting eccrine constituents? *Forensic Science International, 257*, 488-495.
14. Dorakumbura, B. N., Becker, T., & Lewis, S. W. (2016). Nanomechanical mapping of latent fingermarks: A preliminary investigation into the changes in surface interactions and topography over time. *Forensic Science International, 267*, 16-24.
15. Egli, N., Moret, S., Bécue, A., & Champod, C. (2013). *Fingermarks and Other Impressions - A Review (August 2010 – June 2013)*. Paper presented at the 17th Interpol Forensic Science Symposium, Lyon (France).

16. Forchelet, S. (2015).*Influence of Anti-Fingerprint Coatings on Fingermark Detection.* Master Degree Thesis;École des Sciences Criminelles, University of Lausanne, Lausanne (Switzerland).
17. Hazard, D. (2014). *La pertinence en science forensique: une (en)quête épistémologique et empirique.* PhD thesis es Science in Forensic science; École des Sciences Criminelles, University of Lausanne, Lausanne (Switzerland).
18. Houlgrave, S., Andress, M., & Ramotowski, R. S. (2011). Comparison of Different Physical Developer Working Solutions - Part I: Longevity Studies. *Journal of Forensic Identification, 61*(6), 621-639.
19. IFRG - International Fingerprint Research Group (2014). Guidelines for the Assessment of Fingermark Detection Techniques. *Journal of Forensic Identification, 64*(2), 174-200.
20. Jaber, N., Lesniewski, A., Gabizon, H., Shenawi, S., Mandler, D., & Almog, J. (2012). Visualization of Latent Fingermarks by Nanotechnology: Reversed Development on Paper - A Remedy to the Variation in Sweat Composition. *Angewandte Chemie, 51*, 12224-12227.
21. Jones, N., Stoilovic, M., Lennard, C., & Roux, C. (2001). Vacuum metal deposition: factors affecting normal and reverse development of latent fingerprints on polyethylene substrates. *Forensic Science International, 115*(1-2), 73-88.
22. Kent, T. (2010). Standardizing protocols for fingerprint reagent testing. *Journal of Forensic Identification, 60*(3), 371-379.
23. Kupferschmid, E. (2007).*Study of the cyanoacrylate polymerization on non-porous substrates.*Bachelor Degree Thesis;École des Sciences Criminelles, University of Lausanne, Lausanne (Switzerland)
24. Montgomery, L., Spindler, X., Maynard, P., Lennard, C., & Roux, C. (2012). Pretreatment Strategies for the Improved Cyanoacrylate Development of Dry Latent Fingerprints on Nonporous Surfaces. *Journal of Forensic Identification, 62*(5), 517-542.
25. Moret, S., & Bécue, A. (2015). Single-Metal Deposition for Fingermark Detection - A Simpler and More Efficient Protocol. *Journal of Forensic Identification, 65*(2), 118-137.
26. Moret, S., Bécue, A., & Champod, C. (2014). Nanoparticles for fingermark detection: an insight into the reaction mechanism. *Nanotechnology, 25*, 425502 (425510 pp).
27. Moret, S., Spindler, X., Lennard, C., & Roux, C. (2015). Microscopic examination of fingermark residues: Opportunities for fundamental studies. *Forensic Science International, 255*, 28-37.
28. Norlin, S., Nilsson, M., Heden, P., & Allen, M. (2013). Evaluation of the Impact of Different Visualization Techniques on DNA in Fingerprints. *Journal of Forensic Identification, 63*(2), 189-204.
29. Paine, M., Bandey, H. L., Bleay, S. M., & Willson, H. (2011). The Effect of Relative Humidity on the Effectiveness of the Cyanoacrylate Fuming Process for Fingermark Development and on the Microstructure of the Developed Marks. *Forensic Science International, 212*, 130-142.
30. Popov, K. T., Sears, V. G., & Jones, B. J. (2017). Migration of latent fingermarks on non-porous surfaces: Observation technique and nanoscale variations. *Forensic Science International, 275*, 44-56.
31. Raymond, J. J., Roux, C., Du Pasquier, E., Sutton, J., & Lennard, C. (2004). The effect of common fingerprint detection techniques on the DNA Typing of fingerprints deposited on different surfaces. *Journal of Forensic Identification, 54*(1), 22-44.

32. Scruton, B., Robins, B. W., & Blott, B. H. (1975). The Deposition of Fingerprint Films. *Journal of Physics D: Applied Physics, 8*, 714-723.

33. Sears, V. G., Bleay, S. M., Bandey, H. L., & Bowman, V. J. (2012). A Methodology for Finger Mark Research. *Science & Justice, 52*, 145-160.

34. Sisco, E., Staymates, J., & Schilling, K. (2015). A chemically relevant artificial fingerprint material for the cross-comparison of mass spectrometry techniques. *Canadian Society of Forensic Science Journal, 48*(4), 200-214.

35. Spindler, X. (2010). *Detection of Latent Fingermarks: Different Approaches to Targeting Amino Acids in the Deposit.*PhD Thesis, Doctor of Philosophy (Applied science), University of Canberra, Australia.

36. Spindler, X., Stoilovic, M., Lennard, C., & Lennard, A. (2009). Spectral Variations for Reaction Products Formed Between Different Amino Acids and Latent Fingermark Detection Reagents on a Range of Cellulose-Based Substrates. *Journal of Forensic Identification, 59*(3), 308-324.

37. Stoehr, B., McClure, S., Höflich, A., Al Kobaisi, M., Hall, C., Murphy, P. J., & Evans, D. (2016). Unusual Nature of Fingerprints and the Implications for Easy-to-Clean Coatings. *Langmuir, 32*(2), 619-625.

38. Thomas, G. L. (1978). The Physics of Fingerprints and their Detection. *Journal of Physics E: Scientific Instruments, 11*, 722-731.

39. Van Dam, A., van Beek, F. T., Aalders, M. C. G., Van Leeuwen, T., & Lambrechts, S. A. G. (2016). Techniques that acquire donor profiling information from fingermarks - A review. *Science and Justice, 56*(2), 143-154.

40. Velthuis, S., & de Puit, M. (2011). Studies Toward the Development of a Positive Control Test for the Cyanoacrylate Fuming Technique Using Artificial Sweat. *Journal of Forensic Identification, 61*(1), 16-29.

41. Wargacki, S. P., Lewis, L. A., & Dadmun, M. D. (2007). Understanding the Chemistry of the Development of Latent Fingerprints by Superglue Fuming. *Journal of Forensic Sciences, 52*(5), 1057-1062.

42. Wilkinson, D. (2000). Study of the reaction mechanism of 1,8-diazafluoren-9-one with the amino acid, L-alanine. *Forensic Science International, 109*, 87-103.

# ANALYSIS OF TURBULENT DIFFUSION MODEL WITH VARIABLE COEFFICIENTS IN CASE OF STATIONARY POINT SOURCES

**Aleksandra Vulović**
Academy of Criminalistic and Police Studies, Belgrade
**Venezija Ilijazi**
Academy of Criminalistic and Police Studies, Belgrade
**Stevo Jaćimovski**[1]
Academy of Criminalistic and Police Studies, Belgrade

**Abstract**: Methods for mathematical modelling provide opportunity for unification of causes and effects of pollution in the atmosphere, i.e. emissions of pollutants in the atmosphere and the level of pollution. Modelling of atmosphere pollution provides a feedback between monitoring of air quality and the number and distribution of pollution sources. Also, modelling allows to monitor efficiency of various projects aimed at reducing environment pollution. As a result of modelling, field of concentration of pollutants in a particular area is obtained allowing us to assess risks to human health in the monitored area.

**Keywords**: turbulent diffusion equation, scattering of impurity in the atmosphere, point source, diffusion coefficient

## INTRODUCTION

There is a growing concern in the world due to constant rise of global pollution. In order to understand the importance of pollution prevention, there is a need for information accessibility regarding pollution and its effect on life. Air pollution is a global problem and it affects every country in the world, regardless of its location or status. For example, the citizens of Africa, Asia and the Middle East breathe in much higher concentrations of pollutants than the rest of the world.

Air pollution is the biggest threat to the environment preservation and it is responsible for a large number of patients with chronic diseases, such as heart and respiratory disease, which affect the quality of people's lives. Air pollution which is dangerous for humans refers to the existence of a prohibited concentration of particulate matter in the air. Particulate matter consists of a mixture of solid and liquid particles of organic and inorganic substances suspended in the air. The most important components of particulate matter are sulphates, nitrates, ammonia, sodium chloride, coal dust, mineral dust and water. Small particles have a major impact on health even at low concentrations. The biggest threat are the particles of less than 10 microns in diameter, which can penetrate deep into the lungs. Among them, particularly important particles are those whose dimensions are less than 2.5 microns.

1 E-mail: stevo.jacimovski@kpa.edu.rs

Modelling of the pollutants dispersion in the air is an important numerical tool. Its application can help us describe current air quality but also provide essential guidance on how to reduce air pollution. By measuring the pollution in a particular location we learn about the current level of pollution and air quality, but based on those measurements we cannot know what the levels of pollution of nearby locations are, or what will happen in the future. Models describing the air pollution allow to visualize the movement of pollutants in the air over time. Use of those models can help us get information on air pollution for a large number of locations without requiring a physical measurement of pollution.[2]

The models describing the air pollution can be divided into regional dispersion models and models for the local dispersion. The first type of model is applied to the range of up to 1000 km, where the Euler or Lagrange dispersion model is used. The second type of models use Gaussian dispersion model and is used for a range of up to 100 km. Gaussian dispersion model considers that emitted particles do not participate in chemical reactions in the atmosphere, they are carried by the wind in a straight line and they mix with the air in the vertical and the horizontal direction.[2]

The concentration of an air pollutant at any given place is a complex function of a number of variables, such as atmospheric stability, source characteristics, as well as terrain and weather conditions (wind direction and wind speed).[3] Vertical temperature structure of the local atmosphere is really an important atmospheric condition. Decreasing of temperature decreases with height at a rate that is lower than the adiabatic lapse rate or if it increases with height, it can lead to high pollution concentrations.[4]

Models describing the air pollution include different characteristics, such as meteorological, terrain, physical characteristics of the source in order to simulate transport of pollutant plumes. Plume rise is very important when trying to determine maximum ground level concentrations. Plume rise can reduce ground level concentration and that is why it is important to calculate it.[5]

Many authors have been publishing papers in this field that is constantly growing. Moreira and Albuquerque[6] have been working on the solution of the atmospheric diffusion equation with a longitudinal wind speed that depends on source distance. Moreira et al.,[7] analysed plume dispersion in low wind conditions in stable and convective boundary layers. Buske et al.,[8] did simulation of pollutant dispersion for low wind conditions. Although number of

2 Lazarević, N. (2012), Računarska vizuelizacija disperzije vazdušnih polutanata, Magistarska teza, Elektrotehnički fakultet Univerziteta Crne Gore, Podgorica.
3 Dragović et al. (2012), Matlab based simulation of dispersion of air pollutants from industrial sources, 17. Naučno stručni skup „Informacione tehnologije 2012“, Žabljak, pp. 108-111.
4 Abdel-Rahman A.A. (2008), On the atmospheric dispersion and Gaussian plume model, 2nd International Conference on waste management, water pollution, air pollution, indoor climate (WWAI'08) Corfu, Greece, October 26-28.
5 Hanna, S.R., Briggs, G.A., Hosker, R.P., (1982), Handbook on Atmospheric Diffusion. DOE/TIC 11223, Department of Energy, 102 pp.
6 Moreira, D.M., Albuquerque, T.T.A. (2016), Solution of the Atmospheric Diffusion Equation with Longitudinal Wind Speed Depending on Source Distance, Revista Brasileira de Meteorologia, v. 31, n. 2, pp. 202-210.
7 Moreira, D.M., Tirabassi, T., Carvalho, J.C. (2005), Plume dispersion simulation in low wind conditions in stable and convective boundary layers. Atmos. Environ., v. 39, pp. 3643-3650.
8 Buske, D., Vilhena, M.T., Moreira, D.M. and Tirabassi, T. (2007), Simulation of pollutant dispersion for low wind conditions in stable and convective planetary boundary layer. Atmos. Environ. 41, pp. 5496–5501.

papers that involve some numerical simulation is growing, there are still lot of papers that are mainly focused on analytical solution.[9],[10]

The objective of the present study was to analyse turbulent diffusion model with variable coefficients in the case of stationary point sources.

## MATHEMATICAL MODEL

When considering this type of problem, the first step is to decide a point in space in which we are trying to analyse pollutant concentration. Problem analysed in this paper is shown in Figure 1. The physical source of pollution is set in the origin of the Cartesian coordinate system (0,0,0). The wind direction is considered to be along the *y* axis, while on the *z* axis we define the height of interest where we will analyze pollutant concentration. The height of the source of pollution is defined with $H_S$.

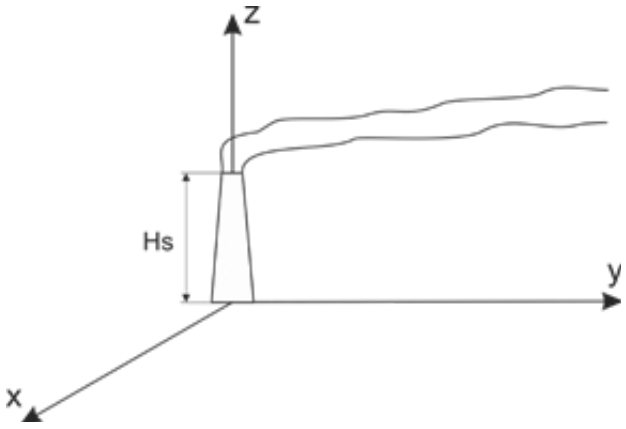



*Figure 1. Schematic representation of the problem*

Equation used to describe stationary, gradient, advection pollutant flow is in the form:

* MERGEFORMAT (1)

$$Q\,u(z)\frac{\partial C(y,z)}{\partial y}=\frac{\partial}{\partial z}\left(K(y,z)\frac{\partial C(y,z)}{\partial z}\right) \tag{2}$$

$$-K(y,z)\frac{\partial C(y,z)}{\partial z}=0 \quad for \quad z\to 0$$

$$-K(y,z)\frac{\partial C(y,z)}{\partial z}=0 \quad for \quad z\to h$$

9 Lin, J.S. and Hildemann, L.M. (1997), A generalized mathematical scheme to analytically solve the atmospheric diffusion equation with dry deposition. Atmos. Environ. 31: 59–71.
10 Vilhena, M.T., Costa, C.P., Moreira, D.M., Tirabassi, T. (2008), A semi-analytical solution for the three-dimensional advection-diffusion equation considering non-local turbulence closure. Atmos. Res. 90, pp. 63–69.

$$u(z)C(0,z) = Q\,\delta(z - H_s)$$

Where $Q$ is the power source, $\delta$ is Dirac delta function, $H_S$ is the height of the source of pollution, and $h$ is the height of the inversion layer of the atmosphere.

Advection speed is changing with the distance from the surface according to the function:

$$u(z) = a\,z^m, \tag{3}$$

where parameter *m* depends on the atmosphere stability.

In the considered model, molecular diffusion coefficient is not a constant value. It is a function of the distance from the Earth's surface:

$$K(y,z) = b\,z^n\,f(y) \tag{4}$$

For the function $f(y)$ we have adopted that value $f(y) = 1$.

Considering the adopted assumptions, equation (1) can be written as:

$$\frac{\partial C(y,z)}{\partial y} = \frac{b}{a} z^{-m} \frac{\partial}{\partial z}\left( z^n \frac{\partial C(y,z)}{\partial z} \right) \tag{5}$$

$$C(y,z) = Y(y)Z(z) \tag{6}$$

After minor transformations, we can write the next equations:

$$\frac{dY(y)}{dy} + \lambda^2 Y(y) = 0 \tag{7}$$

$$\frac{d}{dz}\left( z^n \frac{dZ(z)}{dz} \right) + \lambda^2 \left( \frac{a}{b} \right) z^m Z(z) = 0 \tag{8}$$

where $\lambda$ is arbitrary constant that needs to be determined.

The solution of the first equation (7) of the above system of equations is

$$Y(y) = B_0 e^{-\lambda^2 y},$$

This equation is solved using Fourier method of Separation of Variables:[11]

$$Z(z) = z^{\frac{1-n}{2}} G\left( z^{\frac{m-n+2}{2}} \right)$$

where *G* is an auxiliary function.

11 Kumar, A., Goyal, P. (2012), An Analytical Model for Pollutants dispersion released from different sources in atmospheric boundary layer, Journal of Environmental Research and Development, Vol. 7, No.1., pp. 131-138.

The final solution of the second equation (8) is:

$$Z(z)=z^{\frac{1-n}{2}}\left[B_1 J_\nu\left(\alpha z^{\frac{m-n+2}{2}}\right)+B_2 J_{-\nu}\left(\alpha z^{\frac{m-n+2}{2}}\right)\right] \tag{10}$$

where $J_\nu$ and $J_{-\nu}$ are the Bessel functions of the first kind, $B_1$ and $B_2$ are constants that are determined from the boundary conditions. Also, we have introduced:

$$\alpha^2=\frac{4}{m-n+2}\frac{a}{b}\lambda^2 \qquad \nu=\frac{\quad}{m} \tag{11}$$

With the use of boundary conditions I) and II) we were able to obtain the inherent functions that are orthogonal.[12]

$$Z_\mu(z)=z^{\frac{1-n}{2}}J_{-\nu}\left(\alpha_\mu z^{\frac{m-n+2}{2}}\right) \quad \mu=1,2,3\ldots \tag{12}$$

Values $\alpha_\mu$ are obtained as the roots of the equation:

$$J_{-\nu+1}\left(\alpha h^{\frac{m-n+2}{2}}\right)=0 \tag{13}$$

The expression for the concentration of pollutants is of the form:

$$C(y,z)=A_0+z^{\frac{1-n}{2}}\sum_{\mu=1}^{\infty}A_\mu J_{-\nu}\left(\alpha_\mu z^{\frac{m-n+2}{2}}\right)\mathrm{e}^{-\frac{b(m-n+2)^2\alpha_\mu^2 y}{a}} \tag{14}$$

where $B_0$ is a constant that needs to be determined.

The second equation (8) is solved by introducing substitution:[13],[14]

$$C(y,z)=Q\left[\frac{m+1}{ah^{m+1}}+\frac{m-n+2}{ah^{m-n+2}}(zH_S)^{\frac{1-n}{2}}\sum_{\mu=1}^{\infty}\frac{J_{-\nu}\left[\gamma_\mu\left(\frac{z}{h}\right)^{\frac{m-n+2}{2}}\right]J_{-\nu}\left[\gamma_\mu\left(\frac{H_S}{h}\right)^{\frac{m-n+2}{2}}\right]}{J_{-\nu}^2(\gamma_\mu)}\right]\mathrm{e}^{-\frac{b(m-n+2)^2\gamma_\mu^2 y}{4ah^{m-n+2}}} \tag{15}$$

$$\gamma_\mu=\alpha_\mu h^{\frac{m-n+2}{2}} \tag{16}$$

12 Gradshteyn, I.S., Ryzhik, I.M. (2007), Table of Integrals, Series and Products, Elsevier Academic Press, New York.

13 Abramowitz, M., Stegun, I.A. (1972), Handbook of mathematical functions, National Bureau of Standards, Applied Mathematics Series - 55.

14 Huang, C.H. (1979), Atmospheric Environment, Pergamon Press Ltd.,Vol. 13., pp.453-363.

Unknown coefficients $A_0$ and $A_\mu$ are obtained from the third boundary condition and the fact that the inherent functions $Z_\mu$ are orthogonal. The final expression is:[15],[5]

$$C(y,z)=Q\left\{\frac{2\left(zH_S\right)^{\frac{1-n}{2}}}{b(m-n+2)y}J_{-\nu}\left[\frac{2a\left(zH_S\right)^{\frac{m-n+2}{2}}}{(m-n+2)^2y}\right]\mathrm{e}^{-\frac{a\left(z^{m-n+2}+H_S^{m-n+2}\right)}{b(m-n+2)^2y}}\right\} \tag{17}$$

If the source of pollution is located at the low altitude, close to the surface ( $H_S \to 0$ ), the expression is transformed into:[5,16]

$$C(y,z)=Q\left\{\frac{m-n+2}{a\Gamma\left(\frac{m+1}{m-n+2}\right)}\left[\frac{a}{b(m-n+2)^2y}\right]^{\frac{m+1}{m-n+2}}\mathrm{e}^{-\frac{az^{m-n+2}}{b(m-n+2)^2y}}\right\} \tag{18}$$

If we focus on the analysis of the pollutants concentration in the surface layer of the earth, then the Bessel function in relation to equation (17) can be presented only with the first member.

$$J_{-\nu}(\chi)\approx\frac{2^\nu}{\chi^\nu\Gamma(1+\nu)} \tag{19}$$

For $z$ in range of several meters and for $y>10-20\,\mathrm{m}$, we can use $z=0$. In this case it can be considered that the dependence of the diffusion coefficient is linear ( $n=0$ ). Based on these assumptions and equation (17) we find that the maximum ground pollutants concentrations is at the distance

$$y_{\max}=\frac{aH_s^{m+1}}{b(m+1)^2} \tag{20}$$

and the value is

$$\frac{C_{\max}(\mathrm{y},0)}{Q}=\frac{(m+1)}{a\,e\,H_s^{m+1}} \tag{21}$$

It is evident that the maximum concentrations depend only on the parameters $a, m, H_s$ , while the distance of the maximum concentrations from the source depend on $a, b, m, H_s$ . In other words, the maximum ground pollutants concentration depends on the state of the atmosphere, wind speed and height of the source of pollution.

15 Berlyand, M. E. (1975), Contemporary problems of atmospheric diffusion and air pollution. Hydromet press.

## ANALYTICAL AND NUMERICAL MODEL

In order to calculate pollutant concentration we need to use appropriate parameters.[16] The parameters we have used are shown in Table 1.

**Table 1.** Parameters used for simulation

| Parameter | $m$ | $n$ | $a$ [m/s] | $b$ [m²/s] | [m] | $H_S$ [m] |
|---|---|---|---|---|---|---|
| Value | 0,29 | 0,45 | 1,72 | 3,66 | 150 | 20,50,100 |

The simulations were performed for two different cases, when the inversion layer of the atmosphere is at a high altitude ( $h \to \infty$ ), and when the pollutant source is located at the low altitude ( $\to$ ). In the first case, we were analysing the change in the pollution concentration in the layer of the air which is located 2 m from the surface when the source of the pollution is located at the height of 20, 50 or 100 m. In the second case ( $H_S \to 0$ ) we were analysing the change in the pollution concentration in the layer of the air which is located 2, 10 and 20 m from the ground. The results are visualized using Wolfram Mathematica software.

Figures 2, 3 and 4 show the change of pollutants concentration in the wind direction in the case where the inversion layer of the atmosphere is at a high altitude. Figure 2 shows the results at a height of 2 m from the ground for the case when $h \to \infty$ and the pollution source is located at a height of 20 m.

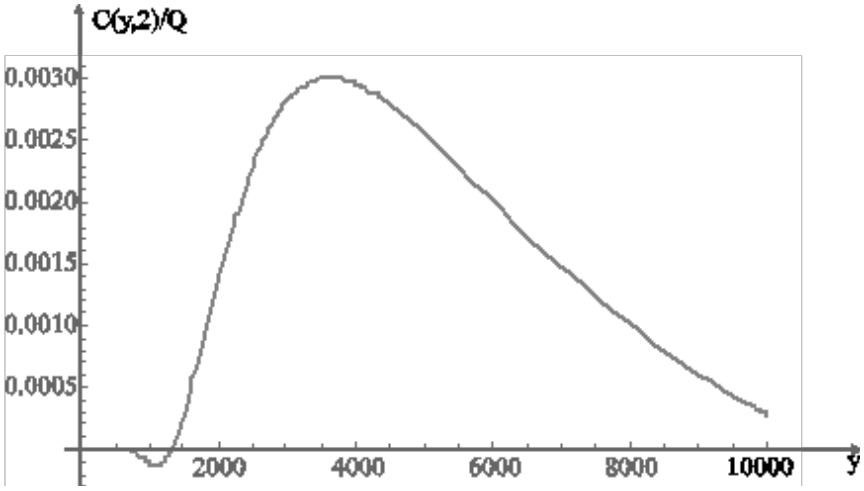



*Figure 2. Dependency of normalized pollutant concentration for z = 2 m, Hs = 20 m*

The dependency of pollutant concentration on a distance from pollution source in the wind direction is shown in Figure 2. Maximum concentration of pollutants is at 3500 m from the pollution source. After this distance concentration almost linearly decreases.

Figure 3 shows the results for the height of 2 m from the ground in the case when a pollution source is located at a height of 50 m.

16 Sharan, M., Yadav, A.K., Sing, M.P. (1995), Comparison of sigma schemes for estimation of air pollutant dispersion in low winds, Atmospheric Environment, Pergamon Press Ltd. Vol. 29, pp. 2051-2059.

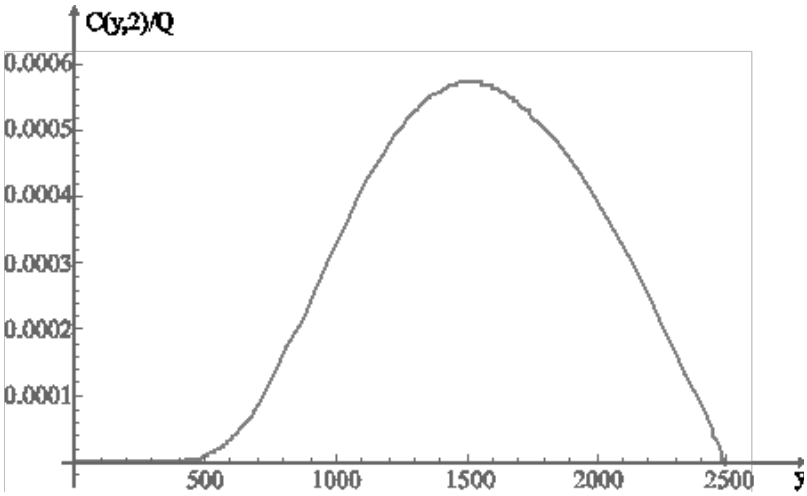



*Figure 3. Dependency of normalized pollutant concentration for z = 2 m, Hs = 50 m*

In this case ($H_s$ = 50 m), maximum concentration of pollutants is at 1600 m from the pollution source. After 1600 m concentration is decreasing until we reach 2500 m from the pollution source. Distribution is in the form of parabola.

The result for the height of 2 m from the ground when the pollutants source is at an altitude of 100 m is shown in Figure 4.

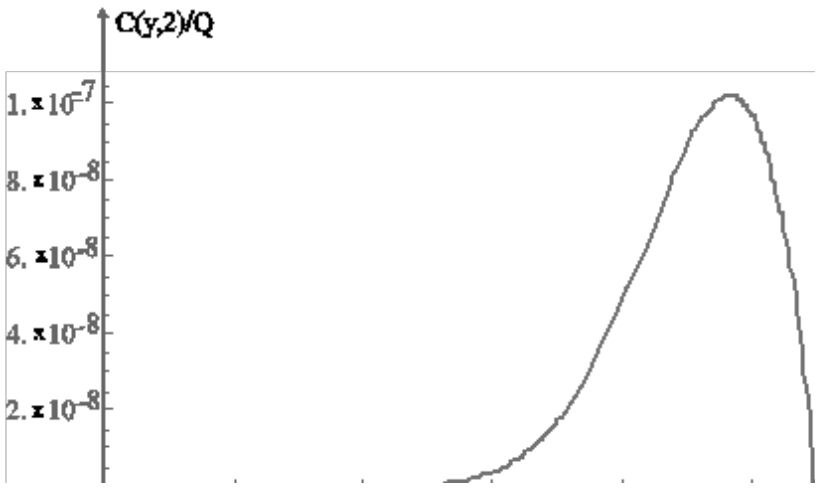



*Figure 4. Dependency of normalized pollutant concentration for z = 2 m, Hs = 100 m*

In this case, when the inversion layer of the atmosphere is at a high altitude and the layer of air we are observing is at 2 m from the surface, the maximum concentration of pollutants is at almost 10000 m from the pollution source. After this distance, concentration is rapidly decreasing.

Figure 5 shows the dependence of the concentration of pollutants at a height 2m from the surface, when a pollution source is located at a height of 50 m.

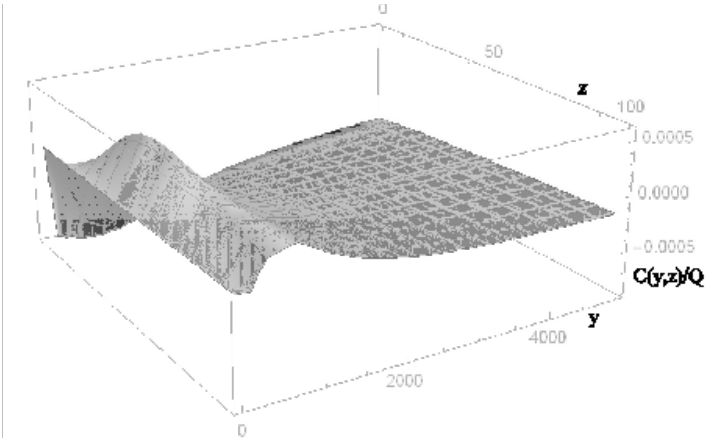



*Figure 5. 3D dependency of normalized pollutant concentration for z = 2 m, Hs = 50 m*

Figures 6, 7 and 8 show the change of pollutant concentration in the wind direction in the case when the pollution source is located at a low altitude.

Figure 6 shows the concentration results for the layer of air 2 m from the surface when $H_S \to 0$.

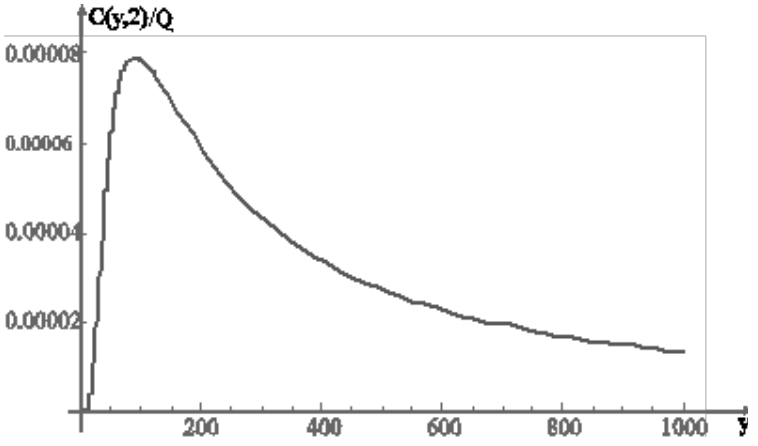



*Figure 6. Dependency of normalized pollutant concentration for z = 2 m*

The dependency of pollutant concentration up to 1000 m from the pollution source is shown. Maximum concentration of pollutants is close to the source (less than 100 m). After reaching the maximum concentration at a distance of almost 100 meters, the concentration decreases exponentially.

Figure 7 shows the concentration results for the layer of air 10 m from the surface when $H_S \to 0$.

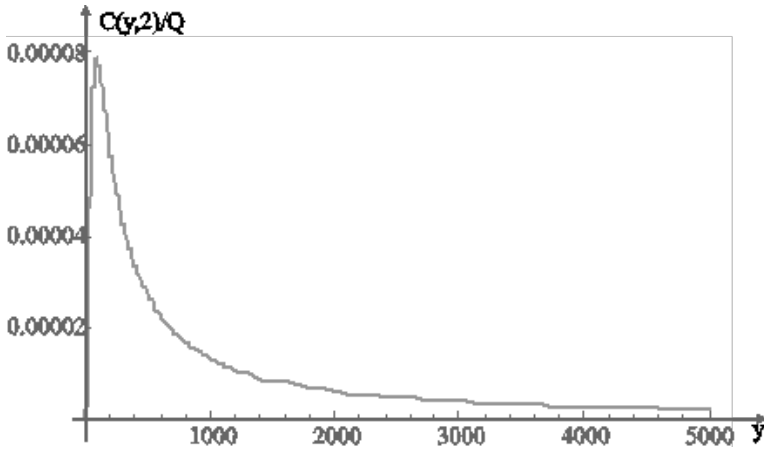



*Figure 7. Dependency of normalized pollutant concentration for z = 10 m*

In case when z = 10 m it is observed that the shape of concentration distribution is similar to the shape shown in Figure 6. The results were similar compared to the results when z = 2 m. The maximum concentration of pollutants is, as in the previous case, close to the source, at a distance less than 100 m. Also, the concentration exponentially decreases after reaching the maximum and it is more pronounced than in the previous case.

Figure 7 shows the concentration results for the layer of air 20 m from the surface when $H_S \to 0$.

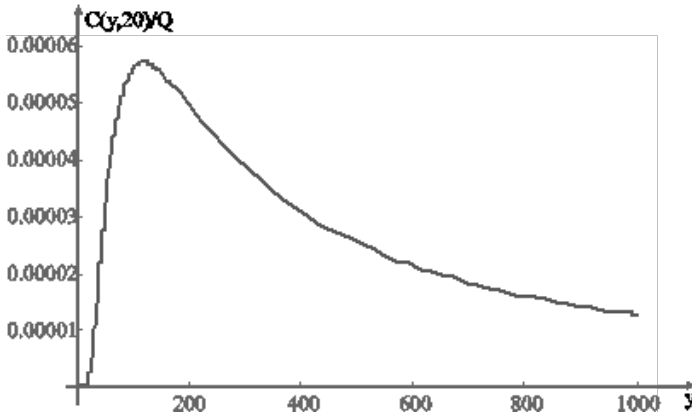



*Figure 8. Dependency of normalized pollutant concentration for z = 20 m*

As in the previous two cases, it shows the distribution of the pollutant concentration at a distance up to 1 km from the source in the wind direction. The shape of the curve that describes the distribution of the concentration is similar to the shape of the curve that describes the distribution at a height of 2 m. The maximum concentration of pollutants is at a distance of approximately 150 m. After this distance the concentration decreases exponentially.

Figure 9 shows a comparative view of pollutant concentration for the heights of 2, 10 and 20 m from the surface in the wind direction for the distance of 1 km from the source of the pollutants.

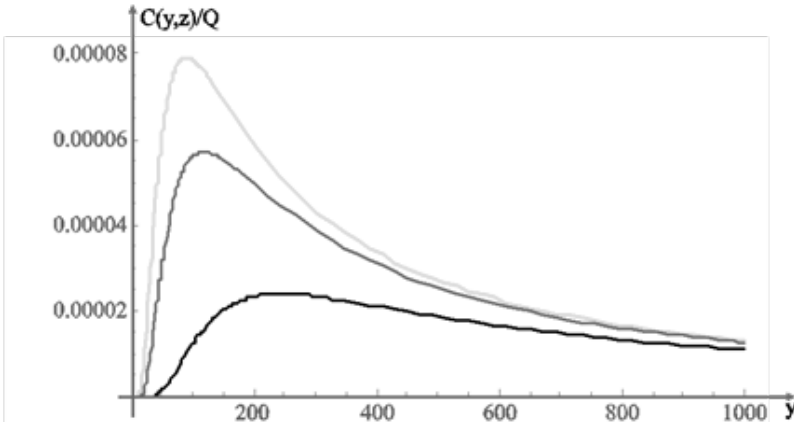



*Figure 9. Comparison of the normalized concentration of pollutant for z = 2 m (green curve), z = 10 m (brown curve) and z = 20 m (black curve) at a distance up to 1000 m*

The maximum pollutant concentration for all three heights (2, 10, and 20 m) is at the distance less than 200 m from pollutants' source. Concentration value is the highest for that of 2 m. Concentration value at 1000 m from the source is almost identical.

Figure 10 shows a comparative view of pollutants' concentration for the heights of 2, 10 and 20 m from the surface in the wind direction for the distance of 5 km from the source of the pollutants.

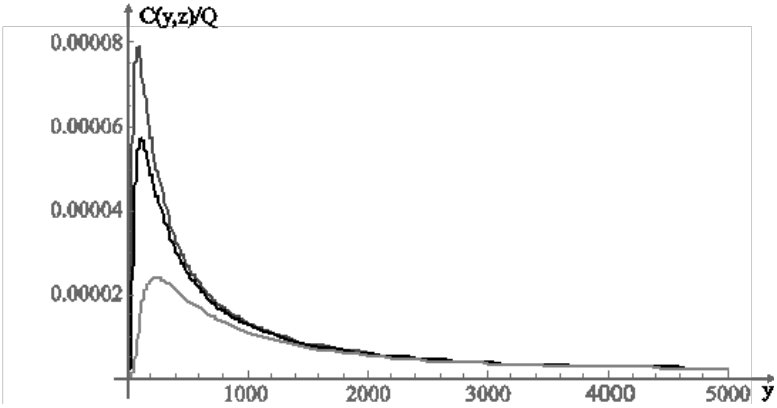



*Figure 10. Comparison of the normalized concentration of pollutant for z = 2 m (blue curve), z = 10 m (black curve) and z = 20 m (red curve) at a distance up to 1000 m*

From the graph we can see that at the distance of about 2000 m from the source, the concentration value for all three heights is the same. After this distance there are no changes in the concentration value until the end of the observed distance.

Figure 11 shows the dependence of the concentration of pollutants at the height of 2 m.

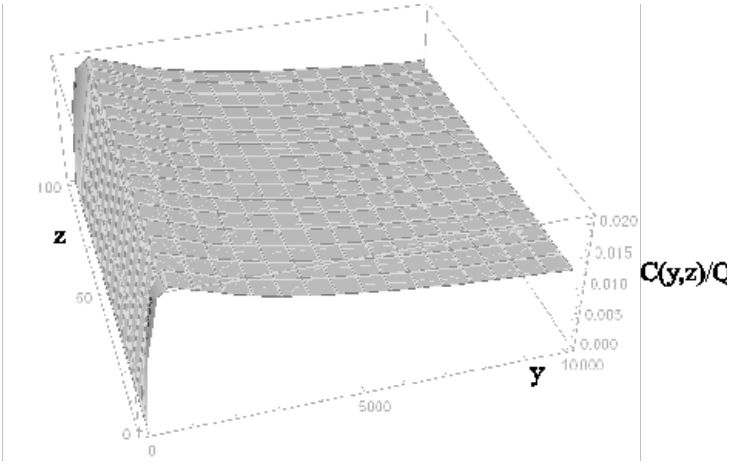



*Figure 11. 3D dependency of normalized pollutant concentration for z = 2 m*

Beside analytical solution to equation that describes pollutant flow, we also did numerical solution for this problem. We numerically solved the equation

$$1.72z^{0.29}\frac{\partial C}{\partial y} = \frac{\partial}{\partial z}\cdot(3.66z^{0.45}\frac{\partial C}{\partial z}) \tag{22}$$

using previously mentioned boundary conditions. The results obtained in this way correspond to the analytical solution presented in Figures 2-11.

## CONCLUSION

Computer modelling and visualization of the air pollutants' dispersion is an important step for the reduction of environmental pollution. In this paper we have shown the mathematical model for turbulent diffusion with variable coefficients in the case of stationary point sources. The normalized concentration was found analytically by solving the two-dimensional turbulent advection diffusion equation.

From the obtained results we can conclude that the concentration change at the distance $y$ depends on the value $z$ to which it relates. On the ground surface at the distance $y_{max}$ from the source it is observed that the maximum normalized concentration $C_{max}(y,0)/Q$ with the increase of $z$ shifts toward the source. At the level of the origin of the impurities ($y=H_s$) the concentration monotonically decreases with the increase of $y$. Observing the vertical profile, it can be seen that the closer the distance to the source, the maximum concentration is more prominent and with the increase of the distance from the origin it lowers and moves to the area of larger distances (in the direction of the wind).

The concentration of impurities is not dependable on $m$ and $n$. Therefore, the effect of stability of the atmosphere (atmospheric stability class) on the distribution of impurities concentration is presented through coefficient $a$ and $b$.

The results obtained by simulations help us get information on air pollution without requiring a physical measurement of pollution, which is very important in critical situations. The future research will include the analysis of specific cases of air pollution in order to compare the measured values with the values obtained using this model.

## ACKNOWLEDGEMENTS

This work was financially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia, Project TR 34019.

## REFERENCE

1. Abdel-Rahman A.A. (2008), On the atmospheric dispersion and Gaussian plume model, 2nd International Conference on waste management, water pollution, air pollution, indoor climate (WWAI'08) Corfu, Greece, October 26-28.
2. Abramowitz, M., Stegun, I.A. (1972), Handbook of mathematical functions, National Bureau of Standards, Applied Mathematics Series - 55.
3. Berlyand, M. E. (1975), Contemporary problems of atmospheric diffusion and air pollution. Hydromet press.
4. Buske, D., Vilhena, M.T., Moreira, D.M. and Tirabassi, T. (2007), Simulation of pollutant dispersion for low wind conditions in stable and convective planetary boundary layer. Atmos. Environ. 41, pp. 5496–5501.
5. Dragović et al. (2012), Matlab based simulation of dispersion of air pollutants from industrial sources, 17. Naučno stručni skup „Informacione tehnologije 2012", Žabljak, pp. 108-111.
6. Gradshteyn, I.S., Ryzhik, I.M. (2007), Table of Integrals, Series and Products, Elsevier Academic Press, New York.
7. Hanna, S.R., Briggs, G.A., Hosker, R.P., (1982), Handbook on Atmospheric Diffusion. DOE/TIC 11223, Department of Energy, 102 pp.
8. Huang, C.H. (1979), Atmospheric Environment, Pergamon Press Ltd., Vol. 13., pp.453-363.
9. Kumar, A., Goyal, P. (2012), An Analytical Model for Pollutants dispersion released from different sources in atmospheric boundary layer, Journal of Environmental Research and Development, Vol. 7, No.1., pp. 131-138.
10. Kumar, P., Sharan, M. (2010), An analytical model for dispersion of pollutants from a continuous source in the atmospheric boundary layer, Proceedings of Royal Society A, vol 466, pp. 383-406.
11. Lazarević, N. (2012), Računarska vizuelizacija disperzije vazdušnih polutanata, Magistarska teza, Elektrotehnički fakultet Univerziteta Crne Gore, Podgorica.
12. Lin, J.S. and Hildemann, L.M. (1997), A generalized mathematical scheme to analytically solve the atmospheric diffusion equation with dry deposition. Atmos. Environ. 31: 59–71.
13. Moreira, D.M., Albuquerque, T.T.A. (2016), Solution of the Atmospheric Diffusion Equation with Longitudinal Wind Speed Depending on Source Distance, Revista Brasileira de Meteorologia, v. 31, n. 2, pp. 202-210.
14. Moreira, D.M., Tirabassi, T., Carvalho, J.C. (2005), Plume dispersion simulation in low wind conditions in stable and convective boundary layers. Atmos. Environ., v. 39, pp. 3643-3650.
15. Sharan, M., Yadav, A.K., Sing, M.P. (1995), Comparison of sigma schemes for estimation of air pollutant dispersion in low winds, Atmospheric Environment, Pergamon Press Ltd. Vol. 29, pp. 2051-2059.

16. Vilhena, M.T., Costa, C.P., Moreira, D.M., Tirabassi, T. (2008), A semi-analytical solution for the three-dimensional advection-diffusion equation considering non-local turbulence closure. Atmos. Res. 90, pp. 63–69.
17. Zauderer, E. (2006), Partial Differential Equations of Applied Mathematics, J. Wiley & Sons, Inc., New Jersey.

# VISUALIZATION OF LATENT FINGERPRINTS BY ELECTROCHEMICAL DEPOSITION OF METALLIC THIN FILMS

**Anka Tutulugdžija**
**Radovan Radovanović**
**Jelena Lamovec**[1]
The Academy of Criminalistic and Police Studies, 196 Cara Dušana Street, 11080 Belgrade-Zemun, Serbia

**Abstract:** A simple and effective approach for visualizing latent fingerprints on different conductive substrates was proposed. The fingerprint residue acted as an insulating mask so it was possible to achieve selective electrochemical deposition of copper and nickel thin films between fingerprint ridges. Thin rectangular pieces of copper, brass and stainless steel foil were chosen for the substrates as materials of relevance to the forensic investigation. Influence of different substrates conditions (roughness, cleanliness) and influence of different deposition parameters (current density, electrodeposition time, concentration of additives) on the film microstructure, adhesion between the film and the substrate and quality of latent fingerprints visualization were investigated. All fingerprints originated from the same donor. The best results were obtained by applying 50 mA/cm$^2$ current density for a period of 30 s, with the mean thickness of the nickel and copper films of about 0.5 μm. The quality of the developed fingerprints was estimated visually and by optical (metallographic) microscopy. It is possible to achieve the satisfactory results of latent fingerprint visualization on rough and dirty surfaces. Electrochemical deposition technique is also applicable for the visualization of latent fingerprints that have been changed by aging.

**Keywords:** latent fingerprints, electrodeposition, thin films, nickel, copper

## INTRODUCTION

Because of their uniqueness, fingerprints are the most commonly used form of physical evidence in criminal investigations. Due to the human glands secretion, impressions of the friction ridge pattern are left after touching a surface. Fingerprints are affected by the substrate that is touched, environmental conditions such as temperature, humidity and light levels and time elapsed since fingerprint deposition.

In the processing of fingerprints, invisible or latent fingerprints (LFP) are the most common and the most problematic type. LFPs need proper treatment to reveal the image. A number of chemical andphysical methods are considered and exploited for LFPs detection and enhancement.

Electrochemical methods have attracted considerable attention in solving the problem of LFPs visualization. Among them, the technique of electrochemical deposition (ED) has great practical significance because it is rapid, low-cost, high-resolution and easy-to-use technique. Thin metal films are used for a variety of applications from machining to microelectronic

1 Corresponding author: jejal@nanosys.ihtm.bg.ac.rs IChTM-Department of Microelectronic Technologies, University of Belgrade, Njegoseva 12, 11000 Belgrade, Serbia

fabrication. For the purpose of LFPs visualization, it is important that the electrodeposition process can occur only on the valleys between fingerprint ridges (spatially selective electrodeposition) and that the colour property of electrodeposited films allows optimization of visual contrast between the fingerprints and substrates.[2,3,4]

Due to the specific relief of the fingerprints, it is crucial to achieve the appropriate fine-grained microstructure of electrodeposited films. With carefully chosen parameters it is possible to obtain the nanocrystalline materials with the grain size less than 100 nm. These materials have good wear-resistance and corrosion-resistance properties.[5,6]

Many different metals and alloys can be electrodeposited whereby different properties can be achieved. It should be noted that this technique is compatible with the integrated-circuit technology as it is low-temperature and high-rate deposition technique. Variation in process parameters, such as current density, deposition temperature or concentration of additives affect many of mechanical and physico-chemical properties of the electrodeposited materials.[7,8,9]

Copper and nickel are well suited metals for different technological applications owing to their low resistivity, low cost and easy-to-grow electrochemically in a well-controlled way.[10,11]

## EXPERIMENTAL DETAILS

The 50 x 10 mm rectangle pieces of brass (260 1/2H, 125 μm-thickness), cold-rolled polycrystalline copper (127 μm-thickness) and stainless steel foils (316L, 125 μm-thickness) were cut and prepared as the substrate material. The samples were mechanically and chemically polished, washed in acetone, isopropyl alcohol, deionized water and dried by a flow of nitrogen. The selected area for electrochemical deposition (20x10mm) was defined by picein wax.

Prior to fingerprint deposition, the donor's hands were washed with soap and dried in the air. Fingerprints were donated by rubbing chosen fingertip over forehead and touching the defined area of substrates surface gently.

2 Gang Qin et al.,*Visualizing latent fingerprints by electrodeposition of metal nanoparticles*, Journal of Electroanalytical Chemistry, Elsevier, 693 (2013) 122-126
3 Meiqin Zhang et al., *Latent fingerprint enhancement on conductive substrates using electrodeposition of copper*, SciChinaChem, Science China Press and Springer-Verlag Berlin Heidelberg, Vol.58, No.7, 2015.
4 Gang Qin et al.,*Visualization of latent fingerprints using Prussian blue thin films*, Chinese Chemical Letters, Elsevier, 24 (2013) 173-176
5 A.S. Ramos, M.T.Vieira, *"An efficient strategy to detect latent fingermarks on metallic surfaces"*, Forensic SciInt (2011), 217, pp.196-203.
6 M.Datta, D.Landolt, *"Fundamental aspects and applications of electrochemical microfabrication"*,ElectrochimicaActa 45 (2000) 2535.
7 J.Lamovec, V.Jović. I.Mladenović, M.Sarajlić, V.Radojević, *"Microindentation hardness testing of different composite systems with thin electrodeposited nickel and copper"*, Proc. 5th International Scientific Conference on Defensive Technologies OTEH 2012, Belgrade,(2012), pp. 570-575.
8 A. A. Rasmussen et al. *"Microstructure and thermal stability of nickel layers electrodeposited from an additive-free sulphamate-based electrolyte"*, Surf. & Coat. Technol. 200 (2006) 6037-6046
9 A. Ibanez, E. Fatas, *"Mechanical and structural properties of electrodeposited copper and their relation with the electrodeposition parameters"*, Surf.&Coat. Techn. 191 (2005), pp.7-16
10 C.Serre, N. Yaakoubi, A. Perez-Rodriguez, J. R. Morante, J. Esteve, J. Montserrat, *"Electrochemical deposition of Cu and Ni/Cu multilayers in Si Microsystem Technologies"*, Sensors and Actuators A, (2005), vol. 123-124, pp. 633-639
11 J.Lamovec, V. Jović, M. Vorkapić, B. Popović, V. Radojević, R. Aleksić, " *Microhardness analysis of thin metallic multilayer composite films on copper substrates*", Journal of Mining and Metallurgy, Section B – Metallurgy 47 (1) B, (2011), 53–61.

Nickel and copper films were electrodeposited from different electrolyte baths. The electrodeposition of copper was performed from a sulphate bath consisting of 240 g/l $CuSO_4 \cdot 5H_2O$, 60 g/l $H_2SO_4$, with and without the additives (polyethylene glycol (PEG 6000)), 1g/l, NaCl 1.5mg/l and sodium 3-mercapto-1-propanesulfonate 0.124 g/l). Nickel films were electrodeposited from the commercial sulphate bath "Slotonik 20" (Schloetter, Germany).

Electrochemical deposition was carried out using direct current (DC) galvanostatic mode. The current density values were maintained at 10 mA/cm$^2$ and 50 mA/cm$^2$. Deposition time was determined in accordance with the plating surface and projected thickness of the films.

After electrodeposition, the samples were rinsed with deionized water and dried by nitrogen. First, the developed fingerprints were evaluated by visual inspection, then by metallographic microscopy (Carl Zeiss microscope "EpivalInterphako") and photographs were taken using a Canon, Power shot SX230HS, 14xIS digital camera.

## RESULTS AND DISCUSSION

Processes of nickel and copper electrodeposition were performed on all the above-mentioned substrates. Due to the complexity of the fingerprint relief and differences in the substrate microstructure, the plating variables such ascurrent density and thickness of the electrodeposited film (deposition time) were chosen for investigation.

For the mentioned experimental parameters, topographic AFM images confirmed the fine-grained columnar structure of electrodeposited Ni and Cu films. The plated structures consist of small substructures as series of very fine submicron grains. These film structures are shown on Figure 1 and Figure 2.

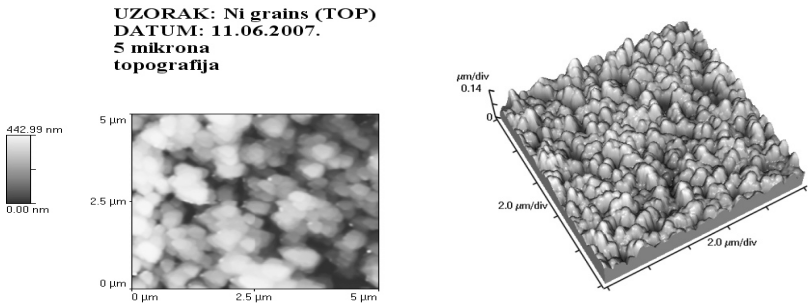



*Figure 1. Topographic AFM image of ED Ni film (10 µm, 10 mA/cm2), chemically etched for 60 s in solution for revealing grain boundaries showing structures of columnar grains*[11]

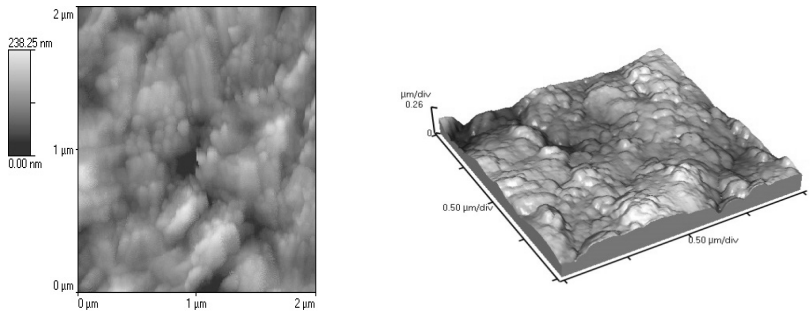



*Figure 2. Topographic AFM image of ED Cu film (10 µm, 50 mA/cm2, chemically etched for 20 s in solution for revealing grain boundaries showing structures of columnar grains*[11]

The microstructure of the electrodeposited Cu and Ni films is influenced by the current density. Increase in the current density leads to decrease in the grain size of deposits. Figure 3 shows AFM topographic scans of two as-deposited Ni films with the same thickness but different current densities. Electrodeposited Ni films thickness is the same in both cases (50 µm) and applied current densities were 10 mA/cm$^2$ for the film topography shown on Figure 3a and 50 mA/cm$^2$for the topography shown on Figure 3b.

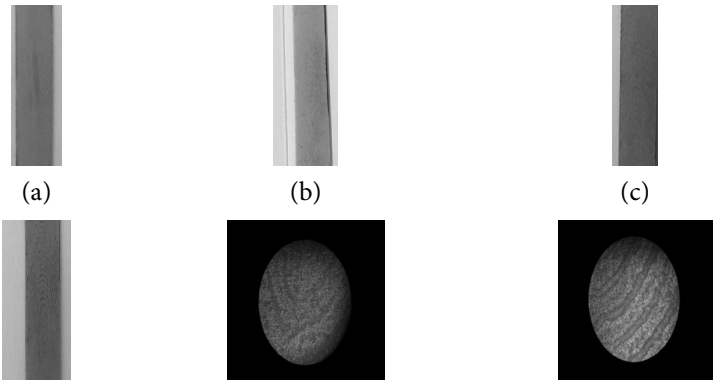
(a) (b)

*Figure 3. Topographic AFM image of ED Ni film (50 µm), electrodeposited with different current densities:*[10] *(a) 10 mA/cm$^2$, (b) 50 mA/cm$^2$*

## VISUALIZATION OF LFPS ON BRASS SUBSTRATES

In order to control the thickness of electrodeposited films on brass, the rates of the electrodeposition process were determined according to the deposition area (20x10mm) and deposited mass as: EDNi(10mA/cm$^2$) = 0.21µm/min, EDNi(50mA/cm$^2$) = 1.03µm/min, EDCu (10mA/cm$^2$) = 0.22 µm/min, EDCu (50mA/cm$^2$) = 1.04µm/min.

Electrochemical deposition of Cu on brass was performed from laboratory-made sulphate electrolyte with and without additives. Deposition time was chosen to be between 30s to 3 min to achieve the film thickness between 0.5 µm and 1 µm and the results are shown in Figure 4. The presence of additives is important for obtaining the bright fine-structured electrodeposited copper films (Figure 4b and Figure 4c). The satisfactory results have been achieved using 50 mA/cm$^2$ current density for a short time of deposition (30s) as shown on Figure 4d. The insulating fingerprint deposit locally covered the substrate and blocked the electrodeposition of copper. The reddish copper film was only deposited on the valleys between fingerprint ridges (Figure 4e and Figure 4f).



(a) (b) (c)

(d) (e) (f)

*Figure 4. Electrodeposited Cu films on brass substrates:(a) without additives, 10mA/cm², 1 min; (b) with additives, 50mA/cm², 1min; (c) with additives, 10mA/cm², 3min; (d) with additives, 50mA/cm², 30s; (e), (f) optical micrographs of (d)*

Latent fingerprints on brass substrates were also developed with the nickel film electrodeposition, with different deposition time and current density values. The best results were obtained with 50 mA/cm² current density for a period of 30s as shown in Figure 5.

(a) (b)

*Figure 5. Electrodeposited Ni films on brass substrates with 50mA/cm² current density and deposition time (a)1min, (b)30s.*

Electrochemical deposition of copper and nickel thin films was also performed on the brass samples with aged fingerprints (13 days of "aging" under ambient conditions). The results of LFPs visualization are shown in Figure 6.

(a) (b) (c)

*Figure 6. Latent fingerprint on brass substrate under ambient conditions for 13 days (a); fingerprint visualization performed with copper electrodeposition, 50mA/cm², 30s (b); visualization performed with electrodeposition of nickel with 50mA/cm² for 30s (c).*

## VISUALIZATION OF LFPS ON COPPER SUBSTRATES

As can be obviously seen from Figure 7, with the copper electrodeposition on copper substrates it is not possible to generate a sharp contrast. The best results were obtained with the use of additives in copper electrolyte bath, applying the 50 mA/cm$^2$ current density for a period of 3 min.

(a) (b) (c)

*Figure 7. LFPs visualization with ED Cu on copper substrates:(a) without additives, 50mA/cm$^2$, 1 min, (b) with additives, 50 mA/cm$^2$, 30s, (c) with additives,10 mA/cm$^2$, 3 min.*

By applying the 10 mA/cm$^2$ current density for nickel electrodeposition on copper substrates, satisfactory results of visualization have not been obtained. Good resultshave been obtained with applying the 50 mA/cm$^2$ current density for deposition times of 1 and 2 min as shown in Figure 8a and Figure 8b. Prolongation of deposition time affects the coverage of the fingerprints (Figure 8c).

(a) (b) (c)

*Figure 8. Electrodeposited nickel films on copper substrates with 50 mA/cm$^2$ current density:(a) 30s, (b) 1 min, (c) 2 min.*

Aging leads to degradation of the latent fingerprints but it is possible to apply the nickel electrodeposition process for their visualization.The results of visualization under different process conditions are shown in Figure 9. Dark lines represent the degraded fingerprints by aging.

(a) (b)

*Figure 9. Electrodeposited Ni films on copper substrates with 13-day old fingerprints: (a) 50 mA/cm², (b)10 mA/cm², for 1 min.*

## VISUALIZATION OF LFPS ON STAINLESS STEEL SUBSTRATES

Due to the weak adhesion of copper films electrodeposited with 50 mA/cm² current density on stainless steel substrates, all tests of fingerprints visualization were performed with 10 mA/cm² current density for a period of 5 min. With deposition rate of 0.2 μm/min, total film thickness of 1 μm was achieved.

Applicability of copper electrodeposition for fingerprint visualization on objects in everyday use was investigated. The objects were uncleaned and unpolished prior to electrodeposition. It should be noted that this method is suitable and applicable to practical cases (Figure 10).

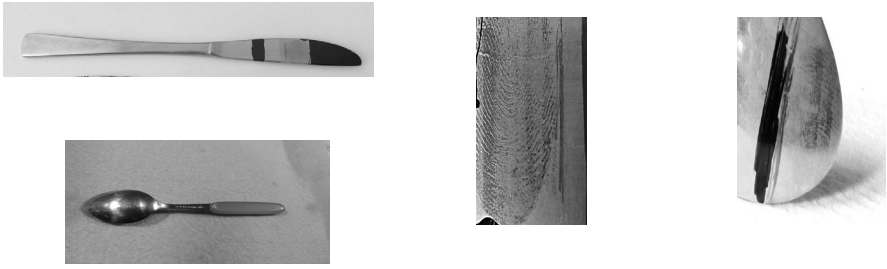


*Figure 10. Electrodeposited Cu films (10 mA/cm2, 5 min) on stainless steel objects in everyday use*

The results of fingerprint visualization with the help of Ni electrodeposited films on stainless steel substrates are shown in Figure 11. Although the film and the substrate are similar in colour and weak contrast is expected, good results may be achieved with 50 mA/cm² current density for deposition time of 30s.

(a) (b)

*Figure 11.Electrodeposited nickel films on stainless steel substrates with 50 mA/cm² current density for: (a) 30 s, (b) 1 min.*

## CONCLUSION

An effective electrochemical approach for visualizing latent fingerprints on conductive substrates was presented. The insulating property of the fingerprint residua as a mask for the spatially selective electrodeposition of copper and nickel films was used on different metal surfaces such as polycrystalline copper, brass and stainless steel. The best results of visualization were obtained with the use of additives in electrolyte baths, with 50 mA/cm$^2$ current density and deposition time of 30s. The similar colour of the film and of the substrate reduces the contrast and makes fingerprint visualization difficult. Thus, the good results were achieved with copper electrodeposition onstainless steel substrates and nickel electrodeposition on brass and copper substrates. Latent fingerprints were successfully developed with the use of copper electrodeposition on objects in everyday use (knife and teaspoon) without their initial cleaning and polishing. Electrochemical deposition is fast, sensitive and significant technique for latent fingerprint visualization on the samples from the real circumstances.

**Acknowledgement**

This work was funded by Ministry of Education, science and Technological Development of Republic of Serbia through the projects TR 32008 and TR 34019.

## REFERENCES

1. A. A. Rasmussen et al. *"Microstructure and thermal stability of nickel layers electrodeposited from an additive-free sulphamate-based electrolyte"*, Surf. & Coat. Technol. 200 (2006) 6037-6046
2. A. Ibanez, E. Fatas, *"Mechanical and structural properties of electrodeposited copper and their relation with the electrodeposition parameters"*, Surf.&Coat. Techn. 191 (2005), pp.7-16
3. A.S. Ramos, M.T.Vieira, *"An efficient strategy to detect latent fingermarks on metallic surfaces",* Forensic SciInt (2011), 217, pp.196-203.
4. C.Serre, N. Yaakoubi, A. Perez-Rodriguez, J. R. Morante, J. Esteve, J. Montserrat, *"Electrochemical deposition of Cu and Ni/Cu multilayers in Si Microsystem Technologies"*, Sensors and Actuators A, (2005), vol. 123-124, pp. 633-639
5. Gang Qin et al., " *Visualization of latent fingerprints using Prussian blue thin films",* Chinese Chemical Letters, Elsevier, 24 (2013) 173-176
6. Gang Qin et al., " *Visualizing latent fingerprints by electrodeposition of metal nanoparticles",* Journal of Electroanalytical Chemistry, Elsevier, 693 (2013) 122-126
7. J.Lamovec, V. Jović, M. Vorkapić, B. Popović, V. Radojević, R. Aleksić, " *Microhardness analysis of thin metallic multilayer composite films on copper substrates*", Journal of Mining and Metallurgy, Section B – Metallurgy 47 (1) B, (2011), 53–61.
8. J.Lamovec, V.Jović. I.Mladenović, M.Sarajlić, V.Radojević, *"Microindentation hardness testing of different composite systems with thin electrodeposited nickel and copper"*, Proc. 5th International Scientific Conference on Defensive Technologies OTEH 2012, Belgrade,(2012), pp. 570-575.
9. M.Datta, D.Landolt, *"Fundamental aspects and applications of electrochemical microfabrication"*,ElectrochimicaActa 45 (2000) 2535.
10. Meiqin Zhang et al., *"Latent fingerprint enhancement on conductive substrates using electrodeposition of copper"*, SciChinaChem, Science China Press and Springer-Verlag Berlin Heidelberg, Vol.58, No.7, 2015.

# THE ROLE OF MICROORGANISMS AS CRIME-FIGHTING TOOLS IN MODERN DAY FORENSIC SCIENCE

**Smilja Teodorović**[1]
Forensics Department, Academy of Criminalistic and Police Studies
**Dejan Jović**
Department of Microbial Ecology, Faculty of Agriculture, University of Belgrade
**Vera Raičević**
Department of Microbial Ecology, Faculty of Agriculture, University of Belgrade

**Abstract:** An increasing body of evidence in the recent years calls attention to the shortcomings of the forensic science system, specifically questionable forensic evidence based on unreliable or unvalidated methods and their invalid interpretations, unsupported by science. The obvious consequence of such flaws is the necessity for the development of rigorous standards and protocols for analyzing and reporting forensic evidence. Further, such deficiencies also indirectly point out to the importance of expanding the repertoire of forensic methods, given that the current ones (with the exception of human nuclear DNA analysis) at the moment lack consistency and high degree of certainty.

Since the 2001anthrax attacks in the United States, a new discipline, microbial forensics, has emerged to provide analysis and interpretation of viruses, fungi, bacteria and their toxins in bioterrorism and biocrimes. However, since then, this field has significantly expanded to include the putative use of microbial evidence in a variety of forensic investigations. This paper focuses on exploiting the possibility of utilizing microbial evidence in criminal prosecutions and civil litigations, such as the use of microbiome to determine postmortem interval and draw conclusions about individualizations, as well as the potential of soil microbial profiling in order to connect people to objects and places and solve environmental crimes. Finally, the feasibility of using microorganisms in court as crime scene evidence and future directions in the field are discussed.

**Keywords**: forensic microbiology, microbiome, soil profiling, environmental forensics.

## INTRODUCTION

The development of forensic science disciplines hasinevitably had a profound influence on criminal investigations, both in terms of conviction of offenders and exoneration of innocent suspects. Advances in DNA technologies have particularly added notable value to personal identification of perpetrators. Since the establishment of "The Innocence Project" in the United States, aimed to exonerate wrongfully convicted individuals through DNA profiling, this approached has led to 351 exonerations. However, in addition to highlighting the value of forensic genetics, these efforts have had another important consequence – a revelation of shortcomings of several other forensic science disciplines. In their analysis of 89 DNA exoneration cases,Saks et al. reported that initial wrongful convictions were a consequence of forensic science testing errors in 69% of the cases and false or misleading testimony by forensic scientists

1Corresponding author: smilja.teodorovic@kpa.edu.rs.

in 27% of the cases[2]. Misleading testimonies would include overstatement of evidence and testimonies resulting from imperfect testing and analyses[3]. Some identification approaches have particularly been recognized as inadequate in the past decade, such as hair, bitemark and shoeprint analyses. For instance, a large review on individualization based on hair samples in forensic science, conducted by the FBI, revealed that 26 out of 28 examiners"overstated forensic matches in a way that favored prosecutors in more than 95 percent"of cases[4]. It has been argued that, if subjected to rigorous testing such as the one conducted for hair analysis, other identification approaches routinely used in forensic work would likelydemonstrate similar flaws[5], due to a lack of standardization of operating procedures, certification of forensic practitioners and accreditation of forensic laboratories. In 2009, National Research Council in the US published a report which emphasized that, aside from the nuclear DNA analysis, none of the employed forensic methods,aimed at individualization in criminal prosecutions and civil litigations, has been able to accurately and consistently demonstrate a "match" between evidence and a specific individual or a source[6].

While aforementioned findings motivate further rigorous experimentation and validation, encouraging results in nuclear DNA forensic analyses, together with advances in DNA technologies, have also opened a possibility for the use of non-human DNA in forensic investigations, microbial being of interest in this paper. Microorganisms represent the most abundant and diverse organisms on the planet and, as such, have gained increasing recognition in the field of forensic science. Forensic microbiology has been defined as "a scientific discipline dedicated to analyzing evidence from a bioterrorism act, biocrime, or inadvertent microorganism/toxin release for attribution purposes"[7]. It is a broad field of interest with numerous applications, with a common goal being identification of origins of pathogens or their toxins. Initially, instances of dentists who have reportedly purposefully infected their patients with an HIV, hepatitis B or hepatitis C virus and other medical negligence cases in which patients have contracted hospital-acquired infections as a result of inadequate hygiene,have received much public attention[8],[9]. Similarly, tracking individuals or companies who have negligently or intentionally caused outbreaks of foodborne diseases has been a traditional aspect of forensic microbiology. Yet, 2001 anthrax attacks in the United States have undoubtedly had a prominent influence on the increased interest, research efforts and expansion of the microbial forensics as a field. Further, development of molecular microbiology techniques and their employment in the environmental forensics have greatly enhanced reconstruction of contaminant release events.

This paper will discuss the emerging applications and techniques of microbiology in forensic investigations, including the role of microorganisms as trace evidence, determination of postmortem intervals and the role of human microbiome.

Soil is found as trace evidence in a wide variety of crimes on clothing, materials and equipment. Given that it is ubiquitous, heterogeneous and transferable, soils evidentiary value has been considered in uncovering the origin of forensic samples and establishing a link between

2 Saks et al., 2005.
3 National Research Council, 2009.
4 https://www.washingtonpost.com/local/crime/fbi-overstated-forensic-hair-matches-in-nearly-all-criminal-trials-for-decades/2015/04/18/39c8d8c6-e515-11e4-b510-962fcfabc310_story.html.
5 https://theintercept.com/2015/04/24/badforensics/.
6 National Research Council, 2009.
7 Budowle et al., 2003.
8 http://abcnews.go.com/Health/rogue-dentist-exposed-7000-patients-hiv-hepatitis/story?id=18834611.
9 http://www.nytimes.com/1993/06/06/weekinreview/aids-and-a-dentist-s-secrets.html?pagewanted=all&mcubz=0.

a crime scene and objects, such as suspect's shoes[10],[11] or care tires. Soils are a complex matrix formed by both organic and inorganic compounds, plant debris, microorganisms and other living organisms. It has been established that soil composition varies with induced stresses, including weather conditions and anthropogenic manipulations, and it has been demonstrated that these variations can be detected and measured (Moreno et al, 2011). Traditional approaches to soil analyses in forensic investigations includedmorphological, chemical and mineralogical examination (i.e. color, particle size, chemical characteristics, such as pH, organic content), as well as biological (i.e. pollen and plant wax)[12],[13],[14],[15],[16].

It has been estimated that $10^9$ bacterial cells inhabit a gram of soil, representing 10 000 to 1 000 000 species, but only approximately 1% of these can be cultured in laboratories. Importantly, bacteria can generate a highly site-specific DNA profile, as the community structure can be influenced by soil type, seasonal variation, site management, vegetation cover and environmental conditions. Therefore, the focus of soil DNA fingerprinting analysis for forensic applications has been microorganisms, specifically targeting the bacterial 16S ribosomal RNA (rRNA) gene region (Young et al, 2015). Specifically, a pilot study of soil samplecomparisons from three ecosystems using Terminal Restriction Fragment Length Polymorphism (T-RFLP) of 16S ribosomal DNA, offered promising results: within sample similarity was higher compared to between sample and unique ecosystem features were uncovered[17]. T-RFLP was also employed in a more comprehensive analysis of soils collected from five distinct habitats over one year, in order to examine bacterial profile uniqueness of individual habitats, level of diversity within each habitat, as well as temporal changes[18]. While the results were encouraging in term of the first two criteria for bacterial profiling of soil, considerable temporal variation was observed. In order to address this issue, as well as putative bacterial heterogeneity over small distances (given that the reference sample would not be collected from the exact same location from which the unknown sample originates), the authors utilized T-RFLP profiles of a recombination protein A gene (*recA*) from nitrogen fixing bacteria, thus simplifying the bacterial profile. The results demonstrated potential for soil habitat differentiation in forensic analyses, given that the soil in question has not undergone significant anthropogenic manipulation[19]. Researchers have also determined that both bacterial and fungal T-RFLP profiles, from ten sites in New Zealand, can be beneficial in determining the origin of questioned soil sample and site-specific matching, emphasizing the importance of further examination of microbial communities' spatial distribution[20]. More recently, next generation sequencing of the bacterial 16S rRNA gene was employed to compare soils from ten different and nine similar habitats. In this study, 94.5% of soil bacterial profiles were correctly matched to their soil of origin[21], thus demonstrating the potential of this method in determining the origin of unknown soil samples.

As mentioned above, often a temporary gap exists between the time of a crime and retrieval of a forensic soil sample, so the effects of seasonal variation, drying, and sample transfer, i.e. removal of soil from the crime scene, must be considered before forensic soil analysis

10 http://cordis.europa.eu/result/rcn/184018_en.html.
11 Quaak and Kuiper, 2011.
12 http://cordis.europa.eu/result/rcn/184018_en.pdf.
13 Pye et al., 2007.
14 Horrocks, 2004.
15 Dawson et al., 2003.
16 Fitzpatrick et al., 2012.
17 Heath et al., 2006.
18 Meyers et al., 2008.
19 Lenz et al., 2010.
20 Macdonald et al., 2011.
21 Jesmok et al., 2016.

can be robustly utilized in court. Seasonal variation is not regarded as an issue for mineralogical analysis as the underlying geology is not affected; however, the soil DNA profile can potentially be considerably altered. Initial studies using 16S rRNA T-RFLP showed monthly fluctuations in bacterial community structure (Lenz and Foran, 2010). These issues clearly require further investigation. Soil removed from the environment during the crime event, as a result of contact with materials, will also be subjected to varying conditions (e.g. temperature, sunlight, humidity, moisture) depending on the circumstances of a case and relocation. For example, soils adhering to shoes or shovels often dry out during storage, potentially altering the DNA profile. Transfer of soil to an object can also be biased according to particle size, which is dependent upon soil properties, mineralogy, and the type of contact, e.g. footwear (Young et al, 2015).

One team of scientists specifically examined shoe soles from 89 randomly selected individuals and different surface types, demonstrating distinct microbial community structure in each sample and strong and immediate impact of the floor microbial profile on the shoe, indicating that suspects could be traced in such a way based on where they have been before the sampling[22]. Some have even contemplated the idea that banks could spread rare, harmless bacterial species on their floors, presumably to be transferred to the perpetrator's shoe soles, demonstrating that they (or their shoes) have at some point visited the bank[23]. However, shoe microbiome usually changes throughout the day, making identification challenging when people have walked significantly; also, floor microbiome will be altered by numerous people who have walked on it.

## THE ROLE OF MICROORGANISMS IN DETERMINING POST-MORTEM INTERVAL

Determination of time of death in cases when a corpse is found at some stage of decomposition still remains one of the notable challenges in forensics work. One of the traditional approaches entails determining Post Mortem Interval (PMI) as a function of the rectal temperature via Glaister equation. Many other approaches based on physical and chemical changes of the corpse exist, but are dependent on numerous parameters, such as age of the corpse, cause of death, ambient temperature, humidity, etc. Even when these parameters are incorporated into comprehensive models, suchestimations of PMI are very unreliable past 48–80 hours after death has occurred[24].Then, the identification of insect collection present on the corpse, with the particular emphasis on the oldest colonizers, plays a significant role in deciphering PMI. However, these methods are restricted by the lack of information regarding insect developmental rates in various decomposition environments, humidity and state of the corpse[25]. As a result, researchers pondered whether, similarly to the predictable patterns of insect succession, microorganisms also change in waves on the corpse, as it undergoes decomposition. Using pyrosequencing, Pechal et al. analyzednecrobiome, a collection of microorganisms present at the decomposing swine corpse, in order to determine bacterial community abundance and identify taxa associated with discrete time points, which may be useful for estimating minimum PMI[26]. Expanding on the idea, Metcalf et al.[27] conducted experiments on 40 mice, sampling abdominal cavity, skin and associated gravesoil in the period

22 Lax et al., 2015.
23 http://www.ubiomeblog.com/why-bacteria-could-soon-be-playing-a-leading-role-in-crime-busting/.
24 Petrovic, 2012.
25 Harvey et al., 2016.
26 Pechal et al., 2013.
27 Metcalf et al., 2013.

of 48 days, during which mice corpse underwent all decomposition phases. High-throughput DNA sequencing of partial 16S (for bacteria and archea) and 18S (for fungi, nematodes and amoeba) rRNA genes was performed in order to determine structure and diversity of microbial populations from samples. Researchers found that at 9 days, during the rupture stage, inflow of oxygen results in a remarkable shift from predominantly anaerobic and facultatively anaerobic gut bacteria, such as Lactobacillus and Bacteroides, to aerobes from soil and air, such as Alphaproteobacteria, Pseudochrobactrum and Ochrobactrum. Corpse rupturing also results in a change of soil composition, leading to switch from oligotrophic to copiotrophic taxa. At approximately day twenty, changes in eukaryotic diversity resulted in the domination by a nematode, *O. tipulae*. This reproducible pattern of decomposition through time, the "microbial clock", has also been demonstrated on human corpses[28],[29] and enabled researchers to perform precise estimations ofthe PMI.Microbial succession patterns do not appear to be affected by soil type, but are different in the summer and winter[30], demonstrating that the effects of seasonality need to be investigated further in order to evaluate the use of such PMI calculations in forensics work.

Interestingly, one study suggested that bacterial community involved in decomposition mainly comes from the soil[31] and that crucial decomposing microorganisms are ubiquitously present in low abundance. Another study suggested a long persistence of human-associated bacterial taxa indecomposing soil, otherwise quite rarely present in soils[32]. It is precisely this shift in soil community structure, represented by dramatic increase in abundance of otherwise negligent taxa, that holds a potential promise as a biomarker, a predictor of gravesoil. A future development of this method for the search of large areas of land suspected to be clandestine grave sites has also been contemplated[33].

## THE USE OF HUMAN MICROBIOME IN FORENSIC INVESTIGATIONS

It has been estimated that approximately hundred trillion microorganisms inhabit human bodies, primarily skin and saliva, as well as gastrointestinal tract, ears, nose and mouth. By sequencing genetic bacterial material from 250 healthy people, the Human Microbiome Project (http://commonfund.nih.gov/hmp/) has discoveredincredible abundance and diversity of human microbiota–thousands of bacterial species live on the surface of human skin and mucosal surfaces, and, within each habitat, there exist significant differences in microbial abundance and composition even among healthy individuals[34]. The latter represents the basis for the microbial forensics approach, that is, the attempt to utilize human microbiome in order to identify individual microbial signatures and apply them in future forensic investigations.

Density of bacteria inhabiting human skin has been estimated to reach approximately 10 $^{7}$ cells per square centimeter[35], while over a 150 unique bacterial speciesare thought to exist on human palms[36]. Interestingly, researchers have reported significant differences between

28 Cobaugh et al., 2015.
29 Metcalf et al., 2016.
30 Carter et al., 2015.
31 Metcalf et al., 2016.
32 Cobaugh et al., 2015.
33 https://www.americanscientist.org/blog/macroscope/how-forensic-scientists-find-a-dead-body%E2%80%94and-how-microbes-can-help.
34 The Human Microbiome Project Consortium.
35 Fierer et al., 2010.
36 Fierer et al., 2008.

male and female hands, both in terms of residingbacterial populations and their diversity, which was higher in females[37]. The fact that only about 13% of bacterial species and subspecies appeared to be shared between any two individuals served as a motivation to examine the existence of individual microbial profiles, as well as their transfer and subsequent survival on surfaces touched by hands. Indeed, latent touch samples left by perpetrator's casual contact with objects are often recovered on crime scenes (Nishi et al, 2015), but in most cases inspection of fingerprints, as well as human DNA typing based on STR analysis from a latent print, cannot provide sufficient information to identify a suspect in a criminal investigation. For instance, a previous study has reported low success rates in obtaining profiles from touch DNA on glass surfaces (ca. 9 %), fabric (23 %), and wood (36 %) (Daly, 2012). Notably, Fierer et al. raised the possibility of personal identification using the bacterial flora of human skin, with an idea that the contact of the palms with numerous surfaces leads to the transfer of bacterial species to the objects we touch, and the bacteria resistant to environmental influences (humidity, temperature, UV rays, etc.) can survive on touch surfaces and for several weeks[38]; thus, it can be assumed that people in their daily lives leave behind a bacterial trace in their surroundings. In this study, the authors exploited a high-throughput pyrosequencing-based approach to quantitatively compare bacterial flora from user's computer keypads and their palms. In fact, the bacteria in the phyla Actinobacteria, Firmicutes, Proteobacteria, and Bacteroidetes are found on all surfaces of the human body, and the human hand sometimes harbors more complex bacterial flora than the gut or oral cavity. Analyzing the DNA of bacterial populations,Fierer and colleagues showed a very high degree of match between bacterial species and subtypes from the user's fingertip and its computer keyboard[39]. Also, it was found that the bacterial populations of the keyboard, that is, the finger bristle, of two users are far more different than the bacterial population of the computer keyboard and the fingerprint of the same user[40]. These results can be reliably reproduced even two weeks after touching the surface. Although this study needs to be developed and examined for the effect on surface type on the results, for example, metal or glass substrates, it is clear that the personal bacteria we all carry on our palms have a very attractive potential in forensics. The use of this method in forensics would allow the identification of persons in cases where this cannot be achieved by standard methods (for example, due to incomplete or smudged fingerprints), as well as a new, independent way of confirming results obtained from fingerprints or DNA. Similar analysis in another study was able to differentiate between individuals, using swabs taken from personal cell phones[41].

Similarly, microorganisms colonizing the pubic region have been analyzed in studies in an attempt to identify individuals, given that mammalian hairs are a frequent type of trace evidence encountered at crime scenes, but often lack roots, thus nuclear DNA, necessary for performing human DNA profiling based on STR markers. Tridico and colleagues analyzedDNA extracts from pubic hairs, demonstrating unique combinations of microbial taxa in individuals, as well as pubic hair signature taxa[42]. By investigating a couple, researchers suggested that an intercourse can result in the transfer of bacterial populations, sustainable for at least 18 hours, leading to a change in pubic microbiome. This could be a potentially important tool in sexual assault cases, when no human DNA has been recovered, to possibly provide association between an offender and the victim, based on a similar bacterial profile of pubic hairs. Storage time and temperature, important factors in forensic scenarios, did not appear to play

37 Fierer et al., 2008.
38 Fierer et al., 2008.
39 Fierer et al., 2008.
40 Fierer et al., 2008.
41 Lax et al., 2015.
42 Tridico et al., 2014.

a role in bacterial taxonomic profiles[43], although generally more targeted experiments with larger sample sizes are needed in the future in order to provide a clearer understanding of the feasibility of pubic bacteria in the courtroom.

## CONCLUSIONS

Microbial forensics is an emerging discipline with very promising results. Numerous research avenues, some not discussed in this paper, are being pursued in this arena. For instance, a research team from Clarkson University in the US is researching the link between spores of toxic molds found in very old buildings and development of health problems in tenants, such as irrational anger and cognitive impairment[44]. However, more studies are necessary in order to ascertain the potency of microbial forensics, as well as the feasibility of microorganisms as evidence in forensic investigations. Microbial genetic analysis have proven to be a valuable tool in this regard, yet future experiments require drastic increase in sample sizes and testing reproducibility of results with high precision. For instance, consideration of the use of "bacterial fingerprints" in the courtroom, dictates research on many unknowns, such as its duration on touched objects, role of surface types, the amount of contact between the surface and the object, the outcome of mixing bacterial populations from different individuals, etc.[45]In addition, there exists a gap between application of microbial approaches in controlled experiments and routine forensic work and introduction of any new scientific approach requires undertaking necessary validations, which will be accepted by scientists and key personnel in the criminal justice system, as well as policy makers[46]. Therefore, implementation of microbial forensics in investigations will need prior rigorous quality assurance, in order to define robustness, reliability, sensitivity and limitations[47]. Level of uncertainty in measurements estimated from scientific studies, standardization of operating principles and procedures would also be needed[48]. Further, appropriate training and mandatory certification of crime scene investigators andlaboratory analysts[49],[50],accreditationof programs and laboratories, as well as effective oversight are necessary steps on the road of admissibility of microbiology evidence in every day forensic science and the court of law.

## REFERENCES

1. Executive Summary of the National Academies of Science Reports, Strengthening Forensic Science in the United States: A Path Forward. (2009). *Forensic Science Policy & Management: An International Journal, 1*(2), 106–122.
2. MISAFE (The Development and Validation of Microbial Soil Community Analyses for Forensics Purposes). (2017).

43 Williams et al., 2017.
44 http://www.dailymail.co.uk/sciencetech/article-3022735/Seen-ghost-inhaled-toxic-mould-Poor-air-quality-old-buildings-lead-haunting-hallucinations.html.
45 http://www.nbcsandiego.com/news/local/Researchers-To-Test-Feasibility-of-Microbial-Cells-as-Crime-Scene-Evidence--328455771.html.
46 Saylers, 2004.
47 Saylers, 2004.
48 National Academies of Science, 2009.
49 http://www.newsweek.com/2016/01/08/using-human-microbiome-predict-time-death-403513.html.
50 https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf.

3. Altman, L. (1993). AIDS and a Dentist's Secrets (http://www.nytimes.com/1993/06/06/weekinreview/aids-and-a-dentist-s-secrets.html?pagewanted=all&mcubz=0).

4. Budowle, B., Schutzer, S. E., Einseln, A., Kelley, L. C., Walsh, A. C., Smith, J. A., Campos, J. (2003). Public health. Building microbial forensics as a response to bioterrorism. *Science, 301*(5641), 1852–1853.

5. Burks, R. (2015). How Forensic Scientists Find a Dead Body – And How Microbes Can Help (https://www.americanscientist.org/blog/macroscope/how-forensic-scientists-find-a-dead-body%E2%80%94and-how-microbes-can-help).

6. Carmichael, A. (2015). Why Bacteria Could Soon Be Playing a Leading Role in Crime Busting (http://www.ubiomeblog.com/why-bacteria-could-soon-be-playing-a-leading-role-in-crime-busting/).

7. Carter, D. O., Metcalf, J. L., Bibat, A., & Knight, R. (2015). Seasonal variation of postmortem microbial communities. *Forensic Science, Medicine and Pathology, 11*(2), 202–207.

8. Christian, S. (2015). Using The Human MicrobiomeTo Predict Time Of Death (http://www.newsweek.com/2016/01/08/using-human-microbiome-predict-time-death-403513.html).

9. Cobaugh, K. L., Schaeffer, S. M., &DeBruyn, J. M. (2015). Functional and Structural Succession of Soil Microbial Communities below Decomposing Human Cadavers. *PLoS One, 10*(6), e0130201.

10. Community, C. o. I. t. N. o. t. F. S., & Council, N. R. (2009). *Strengthening Forensic Science in the United States A Path Forward* (pp. 1 online resource (349 p.)).

11. Dawson, L. A., Towers, W., Mayes, R. W., Craig, J., Väisänen, R. K., & Waterhouse, E. C. (2004). The use of plant hydrocarbon signatures in characterizing soil organic matter. *Geological Society, London, Special Publications, 232*(1), 269–276.

12. Fierer, N., Hamady, M., Lauber, C. L., & Knight, R. (2008). The influence of sex, handedness, and washing on the diversity of hand surface bacteria. *Proceedings of the National Academy of Sciences, 105*(46), 17994–17999.

13. Fierer, N., Lauber, C. L., Zhou, N., McDonald, D., Costello, E. K., & Knight, R. (2010). Forensic identification using skin bacterial communities. *Proceedings of the National Academy of Sciences, 107*(14), 6477–6481.

14. Fitzpatrick, R. W., & Raven, M. D. (2012). How Pedology and Mineralogy Helped Solve a Double Murder Case: Using Forensics to Inspire Future Generations of Soil Scientists. *Soil Horizons, 53*(5), 14.

15. Freeman, S. (2015). Seen a ghost? Then you may have inhaled toxic mould: Poor air quality in old buildings may lead to haunting hallucinations (http://www.dailymail.co.uk/sciencetech/article-3022735/Seen-ghost-inhaled-toxic-mould-Poor-air-quality-old-buildings-lead-haunting-hallucinations.html).

16. Harvey, M., Gasz, N., & Voss, S. (2016). Entomology-based methods for estimation of postmortem interval. *Research and Reports in Forensic Medical Science*, 1.

17. Heath, L. E., & Saunders, V. A. (2006). Assessing the potential of bacterial DNA profiling for forensic soil comparisons. *J Forensic Sci, 51*(5), 1062–1068.

18. Horrocks, M. (2004). Sub-sampling and Preparing Forensic Samples for Pollen Analysis. *Journal of Forensic Sciences, 49*(5), 1–4.

19. Hsu, S. S. (2015). FBI Admits Flaws in Hair Analysis Over Decades (https://www.washingtonpost.com/local/crime/fbi-overstated-forensic-hair-matches-in-nearly-all-crimi-

nal-trials-for-decades/2015/04/18/39c8d8c6-e515-11e4-b510-962fcfabc310_story.html?utm_term=.6c4db5a10059).

20. Human Microbiome Project, C. (2012). Structure, function and diversity of the healthy human microbiome. *Nature, 486*(7402), 207–214.
21. Jesmok, E. M., Hopkins, J. M., &Foran, D. R. (2016). Next-Generation Sequencing of the Bacterial 16S rRNA Gene for Forensic Soil Comparison: A Feasibility Study. *Journal of Forensic Sciences, 61*(3), 607–617.
22. Lax, S., Hampton-Marcell, J. T., Gibbons, S. M., Colares, G. B., Smith, D., Eisen, J. A., & Gilbert, J. A. (2015). Forensic analysis of the microbiome of phones and shoes. *Microbiome, 3*, 21.
23. Lenz, E. J., &Foran, D. R. (2010). Bacterial profiling of soil using genus-specific markers and multidimensional scaling. *Journal of Forensic Sciences, 55*(6), 1437–1442.
24. Lupkin, S. (2013). Rogue Dentist May Have Exposed 7,000 Patients to HIV, Hepatitis (http://abcnews.go.com/Health/rogue-dentist-exposed-7000-patients-hiv-hepatitis/story?id=18834611).
25. Macdonald, C. A., Ang, R., Cordiner, S. J., &Horswell, J. (2011). Discrimination of soils at regional and local levels using bacterial and fungal T-RFLP profiling. *Journal of Forensic Sciences, 56*(1), 61–69.
26. Metcalf, J. L., Wegener Parfrey, L., Gonzalez, A., Lauber, C. L., Knights, D., Ackermann, G., Knight, R. (2013). A microbial clock provides an accurate estimate of the postmortem interval in a mouse model system. *Elife, 2*, e01104.
27. Metcalf, J. L., Xu, Z. Z., Weiss, S., Lax, S., Van Treuren, W., Hyde, E. R., Knight, R. (2016). Microbial community assembly and metabolic function during mammalian corpse decomposition. *Science, 351*(6269), 158–162.
28. Meyers, M. S., &Foran, D. R. (2008). Spatial and temporal influences on bacterial profiling of forensic soil samples. *Journal of Forensic Sciences, 53*(3), 652–660.
29. Pechal, J. L., Crippen, T. L., Benbow, M. E., Tarone, A. M., Dowd, S., &Tomberlin, J. K. (2014). The potential use of bacterial community succession in forensics as described by high throughput metagenomic sequencing. *International Journal of Legal Medicine, 128*(1), 193–205.
30. Petrovic, A., (2012). Forenzickaentomologija, radnaskripta (http://www.bio.bg.ac.rs/materijali_korisnika/Forenzicka%20entomologija_skripta_2012_5828_1381328930.pdf).
31. Pye, K., Blott, S. J., Croft, D. J., &Witton, S. J. (2007). Discrimination between sediment and soil samples for forensic purposes using elemental data: an investigation of particle size effects. *Forensic Science International, 167*(1), 30–42.
32. Quaak, F. C., & Kuiper, I. (2011). Statistical data analysis of bacterial t-RFLP profiles in forensic soil comparisons. *Forensic Science International, 210*(1-3), 96–101.
33. Saks, M. J., & Koehler, J. J. (2005). The coming paradigm shift in forensic identification science. *Science, 309*(5736), 892–895.
34. Salyers, A. A. (2004). Microbes in Court: The Emerging Field of Microbial Forensics (http://www.actionbioscience.org/genomics/salyersarticle.html).
35. Smith, J. (2015). Five Disturbing Things You Didn't Know About Forensic "Science" (https://theintercept.com/2015/04/24/badforensics/).
36. Stimson, B. (2015). Researchers To Test Feasibility of Microbial Cells as Crime Scene Evidence (http://www.nbcsandiego.com/news/local/Researchers-To-Test-Feasibility-of-Microbial-Cells-as-Crime-Scene-Evidence--328455771.html).

37. Tridico, S. R., Murray, D. C., Addison, J., Kirkbride, K. P., &Bunce, M. (2014). Metagenomic analyses of bacteria on human hairs: a qualitative assessment for applications in forensic science. *Investigative Genetics, 5*(1), 16.

38. Williams, D. W., & Gibson, G. (2017). Individualization of pubic hair bacterial communities and the effects of storage time and temperature. *Forensic Science International: Genetics, 26*, 12–20.

# CHROMATOGRAPHIC TECHNIQUES AS RELIABLE TOOLS FOR AUTHENTICATION AND ADULTERATION OF DIETARY SUPPLEMENTS

**Nikola Milašinović**[1]
Academy of Criminalistic and Police Studies, Belgrade
**Bojana Vidović**
University of Belgrade, Faculty of Pharmacy, Department of Bromatology
**Bojan Čalija**
University of Belgrade, Faculty of Pharmacy, Department of Pharmaceutical Technology and Cosmetology

**Abstract:** Being aware that labels do not provide sufficient guarantees regarding the true contents of a product, the application of accurate and reliable methods to identify and/or authenticate the components of dietary supplements, has steadily increased during the past decades. Another aspect that should be considered as part of the safety of these products is adulteration by the illegal addition of pharmaceutical substances or their analogs. Therefore, to protect consumers from illegal substitutions or adulterations, numerous analytical procedures were developed in order to detect counterfeits and illegal preparations. The choice of analytical instrumentation and methodology should be selected based on the intended purpose and scope of the analytical method, together with specificity, linearity, limits of detection and the limits of quantification, range, accuracy, as well as its precision. This mini-review highlights the utilization of chromatography techniques, alone or coupled with some spectroscopic methods, applied in the dietary supplement analysis as well as the authentication and the illegal impurity identification.

**Keywords:** chromatographic techniques, authentication, adulterations, dietary supplements.

## INTRODUCTION

In recent years, the public confidence in the ability of manufacturers as well as governments to assure the safety of food and health products has been shaken[2], and the adulteration of these products in the market is an increasingly serious global issue[3]. Many of the food products targeted for adulteration are of high commercial value and/or produced in high tonnage around the world presenting the economic and public health concerns[4],[5].Adulteration often involves substitution of the materials with cheaper or low(er) quality material, dilution of the

1 nikola.milasinovic@kpa.edu.rs.
2 Gallup, A.M., 2008. The Gallup Poll Cumulative Index: Public Opinion, 1998–2007. Rowman and Littlefield, Lantham, Maryland.
3 Wheatley, V. M. and Spink, J. (2013), Defining the Public Health Threat of Dietary Supplement Fraud. Comprehensive Reviews in Food Science and Food Safety, 12: 599–613.
4 http://www.searo.who.int/entity/world_health_day/2015/whd-what-you-should-know/en/.
5 Blackstone, E. A., Fuhr, J. P., &Pociask, S. (2014). The Health and Economic Effects of Counterfeit Drugs. American Health & Drug Benefits, 7(4), 216–224.

original product, and mislabeling of age and origin of the material used[6].In recent years, the increased global dietary supplements market has been accompanied by an increased frequency of economically motivated adulteration of these products[7]. Concerns have included too little or none of the active ingredient in a supplement, substitution of claimed naturally derived material with a synthetic substance and products adulterated with drugs or drug analogs[8]. Authentication of dietary supplements is important to avoid adverse toxic effects, provide consumer protection, as well as for certification purpose[9].Many sophisticated techniques or protocols provide means for verification of foodstuff origin[10] and detection and precise quantification of the adulterants in various products[11,12,13,14,15,16]. However, no single methodology is generally applicable for adulteration detection[17].

Many techniques could be employed for detection and identification of counterfeit products[18], among which different chromatographic techniques[19,20,21], coupled or alone, might be applied in the dietary supplement analysis. This mini-review aims at providing an overview of the chromatographic techniques currently used for the identification and quantification of

6 Vemireddy, L. R., Satyavathi, V. V., Siddiq, E. A., &Nagaraju, J. (2015). Review of methods for the detection and quantification of adulteration of rice: Basmati as a case study. Journal of Food Science and Technology, 52(6), 3187–3202.
7 Liu, Y. and Lu, F. (2017), Adulterated pharmaceutical chemicals in botanical dietary supplements: novel screening approaches. Reviews in Analytical Chemistry, 36(3), pp. -. doi:10.1515/revac-2016-003.
8 http://www.usp.org/sites/default/files/usp/document/about/public-policy/public-policy-dietary-supplements.pdf.
9 Lo, Y.T., Shaw, P.C. (2018), DNA-based techniques for authentication of processed food and food supplements. Food Chemistry, 240:767–774.
10 Georgiou, C.A.,Danezis, G.P., (2015), Elemental and isotopic mass spectrometry, in: Advanced mass spectrometry for food safety and quality, Ed. Y. Pico, Comprehensive Analytical Chemistry, Elsevier, 2015, pp. 131–243.
11 Vemireddy, L. R., Satyavathi, V. V., Siddiq, E. A., &Nagaraju, J. (2015). Review of methods for the detection and quantification of adulteration of rice: Basmati as a case study. Journal of Food Science and Technology, 52(6), 3187–3202.
12 Ambrose, A., Cho, B.-K., (2014). A Review of Technologies for Detection and Measurement of Adulterants in Cereals and Cereal Products. Journal of Biosystems Engineering, 39(4):357–365.
13 Azad, T. & Ahmed, S. (2016) International Journal of Food Contamination 3(22). doi:10.1186/s40550-016-0045-3.
14 Iammarino, M., Marino, R. and Albenzio, M. (2017), How meaty? Detection and quantification of adulterants, foreign proteins and food additives in meat products. Int J Food Sci Technol, 52: 851–863. doi:10.1111/ijfs.13350.
15 Haneef, J., Shaharyar, M., Husain, A., Rashid, M., Mishra, R., Siddique, N. A. and Pal, M. (2013), Analytical methods for the detection of undeclared synthetic drugs in traditional herbal medicines as adulterants. Drug Test. Analysis, 5: 607–613. doi:10.1002/dta.1482.
16 Brown, P.N., Paley, L.A., Roman, M.C., Chan, M., (2008), Single-Laboratory Validation of a Method for the Detection and/or Quantification of Select Alkaloids in Goldenseal Supplements and Raw Materials by Reversed-Phase High-Performance Liquid Chromatography. Pharmaceutical Biology, 46(1-2):135–144.
17 Sarma, N., Giancaspro, G., Venema, J. (2016), Dietary supplements quality analysis tools from the United States Pharmacopeia. Drug Testing and Analysis, 8(3-4):418–423.
18 Jelena Đuriš, BojanaVidović, BojanČalija, Nikola Milašinović, (2016) "Anti-counterfeiting Food and Drug Packaging Technologies and Forensic Tools: Present State and Future Trends", International Scientific Conference "Archibald Reiss Days", 3–4 March 2016, Belgrade, Serbia, pp. 237–251.
19 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.
20 Sherma, J., Analysis of counterfeit drugs by thin layer chromatography. Acta Chromatographica, 19:5–20, 2007.
21 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.

adulterants in dietary supplements, with the special focus on different synthetic drugs and theiranalogs.

## ADULTERATION OF DIETARY SUPPLEMENTS

Dietary supplements (also called food supplements) are concentrated sources of nutrients or other substances with a nutritional or physiological effect, whose purpose is to supplement the normal diet.The active ingredients in dietary supplements include: vitamins, minerals, herbs, or other botanicals, amino acids, and substances such as enzymes, metabolites and other. The quality of these products, especially plant food supplements is defined by ingredient authenticity, absence of impurities, content ofdesirable marker, and active compounds or profiles of these constituents[22]. Despite the current regulations and standards, there are significant risks associated with the use of dietary supplements including the absence of active ingredients, the presence of contaminants (including heavy metals and microbiological agents), toxic agents, and intentional adulteration with pharmaceuticals in order to develop an immediate action or to intensify a claimed effect[23].These adulterants may include approved prescription drugs, theiranalogs, patented drugs not undergoing clinical trials, or pharmaceuticals withdrawn because of their serious side effects[24].

The pharmaceutical adulterants include a number ofanalogs such as appetite suppressors, stimulants, antidepressants, anxiolytics, diuretics, anabolic steroids and prohormones in supplements for muscle building/sports performance enhancement, while analogs of those substances of suspicious quality, and without available pharmacological studies[25],[26],[27]are of a major concern.For instance, the European Medicines Agency and the *United States Food and Drug Administration*(FDA) removed the appetite suppressant drug sibutramine from the market for safety reasons in 2010, as it was confirmed that it can increase blood pressure and pulse rate, causing coronary artery disease, heart failure, arrhythmias, stroke, and even death. On contrary to thesewarnings, the fraudulent addition of sibutraminehas been detected in many slimming supplements[28].

Since the introduction of Meditag authentication hologramin 2005, there has been a significant increase in the identification and confiscation of illegal items from the market and prevention of their entry into distribution channels. The reason for adulteration ofsome products with analogs by manufacturerslies in the fact that it might be easier to evade interception by regulatory authorities, but since analogs are structurally modified, they might not be

22 Mudge, E.M., Betz, J.M., Brown, P.N., (2016), The Importance of Method Selection in Determining Product Integrity for Nutrition Research. Advances in Nutrition, 7(2):390–398.
23 Maughan, R.J., (2013), Quality assurance issues in the use of dietary supplements, with special reference to protein supplements. Journal of Nutrition, 143(11):1843S–1847S.
24 Vaclavik, L., Krynitsky, A.J., Rader, J.I., (2014), Mass spectrometric analysis of pharmaceutical adulterants in products labeled as botanical dietary supplements or herbal remedies: a review. Analytical and Bioanalytical Chemistry, 406: 6767–90.
25 Rocha, T., Amaral, J.S., Oliveira, M.B.P.P.,(2016), Adulteration of Dietary Supplements by the Illegal Addition of Synthetic Drugs: A Review. Comprehensive Reviews in Food Science and Food Safety, 15(1):43–62.
26 Khazan, M., Hedayati, M., Kobarfard, F., Askari, S., Azizi, F., (2014), Identification and Determination of Synthetic Pharmaceuticals as Adulterants in Eight Common Herbal Weight Loss Supplements. Iranian Red Crescent Medical Journal, 16(3):e15344.
27 http://www.psychiatrictimes.com/articles/dietary-supplement-adulteration-erectile-dysfunction-weight-loss-and-sports.
28 Mathon, C., Ankli, A., Reich, E., Bieri, S., Christen, P., (2014), Screening and determination of sibutramine in adulterated herbal slimming supplements by HPTLC-UV densitometry. Food Additives & Contaminants: Part A, 31:15–20.

detected by ordinary laboratory methods. This has become evident by the number of toxicity cases and adverse reactions (with casualties) reported via analytical techniques that detected the presence of chemical adulterants in market products, being responsible for their toxicity.

An overview of commonly used pharmaceutical adulterants in dietary supplementsreported by FDA is given in Table 1[29]. Based on the information available in the interactive online Rapid Alert System for Food and Feed (RASFF) database the most frequent pharmacological adulterants in dietetic foods, food supplements, fortified foods in the European Union from 2013 to 2016 were 1,3-dimethylamylamine (DMAA), sildenafil and its analogues (thiosildenafil, homosildenafil, thiodimethylsildenafil, desmethylcarbodenafil and dithiodesmethylcarbodenafil), yohimbine, phenethylamine and sibutramine[30].

*Table 1. Patterns of contamination observed in dietary supplement recall notices issued by the FDA*[31]

| Product category | Undeclared ingredients | Examples |
|---|---|---|
| Muscle building | Anabolic androgenic agents | Methandienone, desoxymethyltestosterone, 4-chlorodehydromethyltestosterone |
| Tonics | Stimulants | Ephedrine, amphetamine analogs |
| Weight loss | Anorectic agents | Sibutramine, fenfluramine, ephedrine, phenteramine |
| Sexual enhancement | Phosphodiesterase type 5 inhibitors | Sildenafil, tadalafil, aminotadalafil inhibitors |

The growing problem of dietary supplements adulteration has been recognized by the United States Pharmacopeial (USP) Convention. To support identification of adulterated products and prevent them from reaching consumers USP Expert Group prepared General Chapter <2251>*Adulteration of Dietary Supplements with Drugs and Drug Analogs*[32]. This chapter identifies three major categories of adulterated dietary supplements: erectile dysfunction, weight loss and sports performance enhancement supplements. The first version of the chapter focuses on erectile dysfunction supplements adulterated with phosphodiesterase type 5 (PDE-5) inhibitors and it is expected that the following revisions will include methods for detection of adulteration in the other two commonly adulterated categories. As no individual technique is capable of addressing all potential analytes, the use of various screening techniques is highly recommended to maximize probability for adulteration detection.

According to this chapter, two types of techniques for adulteration can be distinguished: *targeted* and *nontargeted*, depending on whether the analytes are known or not. Targeted analysis relies on pre-existing knowledge of the analyte and allows optimization of methodology for its reliable detection, while nontargeted screening aims at wideningthe detection scope. Therefore, it is advisable to apply a nontargeted methodology first, followed by a targeted procedure. Nontargeted methods should be also applied if the presence of various adulterants is suspected. Appendix of this chapter contains description of screening methodologies recommended for PDE-5 inhibitors, including high-performance liquid chromatography coupled with photodiode array or mass-spectrometric detection and high-performance thin-layer

29 Maughan, R.J., (2013), Quality assurance issues in the use of dietary supplements, with special reference to protein supplements. Journal of Nutrition, 143(11):1843S–1847S.
30 https://webgate.ec.europa.eu/rasff-window/portal/.
31 Maughan, R.J., (2013), Quality assurance issues in the use of dietary supplements, with special reference to protein supplements. Journal of Nutrition, 143(11):1843S–1847S.
32 Adulteration of dietary supplements with drugs and drug analogs. Pharmacopeial Forum, 2014, 41(3). United States Pharmacopeial Convention, Rockville, MD.

chromatography coupled with visual, ultraviolet (UV), and/or mass spectrometry (MS)detection. This chapter will be updated regularly in response to the new adulterants and analytical tools improvements. It should be highlighted that the USP is developing an open access Dietary Supplements Adulteration Database intended to provide information on the incidences of dietary supplements adulteration and available methods for adulteration detection[33].

## OVERVIEW OF RELIABLE TECHNIQUES IN DIETARY SUPPLEMENTSAUTHENTICATION

The analytical methods chosen for detection, identification and, eventually, quantification of the substances of interest, depend on several factors including the number of targeted compounds and different chemical families, required sensitivity, formulation type (e.g., tablets, oily capsules, liquids) and the complexity of the matrix (e.g., some samples are consisted of a large number of different botanicals). This section gives an overview of chromatographic methods used for detecting synthetic adulterants in dietary supplements, focusing onthe most frequently adulteratedsupplementsused for weight loss, muscle building/sport performance, and sexual enhancement performance.

## CHROMATOGRAPHIC TECHNIQUES IN DIETARY SUPPLEMENTS ANALYSIS/AUTHENTICATION

Spectroscopic techniques such as near-infrared, infrared and Raman spectroscopy are fast, simple, and cost-effective techniques regularly used for the detection of counterfeits[34]. Due to the complexity of dietary supplements content, especially by presence of herbal ingredients and lack of selectivity towards these species,chromatographic methods are becoming more important in this domain.[35]

There are several chromatographic techniques that could be applied for detection of adulterantsindietary supplements:thin-layer chromatography, high-performance liquid chromatography andgas chromatography, alone or coupled with other techniques such as photodiode array, visual, UV or mass-spectrometric detection.

In order to enhance sample reproducibility, a correct sampling procedure is of a great importance. Namely, sample collection and preliminary sample processing as well as weighing or dilution, are all part of an important sample preparation procedures. Other steps include alternative sample processing methods (solvent exchange, evaporation, etc.), removal of particulates by filtration, centrifugation or solid phase extraction, sample extraction (for liquid/solid samples) and derivatization, mainly to enhance analyte detection. Microencapsulated ingredients required to break a shell material[36]. Sample preparation and detection of adulter-

33 Sarma, N., Giancaspro, G., Venema. J., (2016), Dietary supplements quality analysis tools from the United States Pharmacopeia. Drug testing and analysis. 8(3-4):418–23.
34 Liu, Y. and Lu, F. (2017), Adulterated pharmaceutical chemicals in botanical dietary supplements: novel screening approaches. Reviews in Analytical Chemistry, 36(3), pp. -. doi:10.1515/revac-2016-0032.
35 Deconinck, E., Sacré, P.Y., Courselle, P., De Beer, J.O., (2013), Chromatography in the Detection and Characterization of Illegal Pharmaceutical Preparations. Journal of Chromatographic Science, 51(8):791–806.
36 Curtis, J.M., Berrigan, N., Dauphinee, P., (2008), The determination of n-3 fatty acid levels in food products containing microencapsulated fish oil using the one-step extraction method. Part 1: measurements in the raw ingredient and in dry powdered foods. Journal of the American Oil Chemists' Society, 85:297–305.

ants in dietary supplements can be complicated by characteristics such as analyte solubility, type of excipients, the presence of colors and complex formulation[37].

*Thin-layerchromatography (TLC)*. TLC is considered to be a simple, easy, rapid, and inexpensive technique for the quality control of food, drugs, dietary supplements and other health products in order to preliminary screening the ingredients, purity evaluations and testing the stabilityof products[38]. All identifications in the TLC are based on the migration distances ($R_f$) values and the color of the spots between the samples and standards when the spots of separated compounds on TLC plate are detected with UV light or sprayed with specific chromogenic reagents[39]. This analytical method has been widely used for the quality of control of medical plants, but also for the analysis of herbalpreparations[40]. However, the main *disadvantages ofTLCinclude lack of* sufficient specificity and low sensitivity to identify the nature of separated compounds[41]. Also, based on the fact that TLC is an open system, dependent on environmental factors, results cannot be fully controlled and analyses are not totally reproducible[42]. Moreover, the sensitivity of TLC could be improved by using high-performance thin layer chromatography(HPTLC).[43]As a consequence of the use of higher quality of TLC plates with finer particle sizes in the stationary phase, HPTLC offers better results with regard to speed, efficiency and separation (Figure 1.),and allows quantitative analysis of compounds. A comparison of the physical properties of TLC and HPTLC plates is given in Table 2.

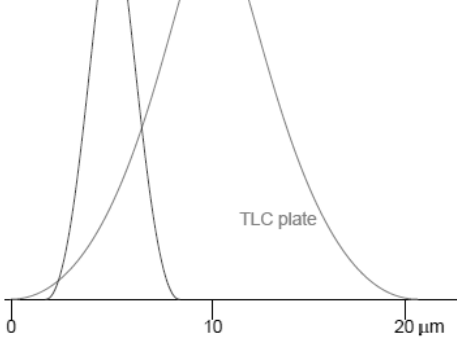



*Figure 1. Comparison of particle size distribution for the same sample used in TLC and HPTLC plates*

37 Mudge, E.M., Betz, J.M., Brown, P.N., (2016), The Importance of Method Selection in Determining Product Integrity for Nutrition Research. Advances in Nutrition, 7(2):390–398.
38 Cimpoiu, C. and Hosu, A. (2007), Thin layer chromatography for the analysis of vitamins and their derivatives. Journal of Liquid Chromatography & Related Technologies, 30, 701–728.
39 Liu, Y. and Lu, F. (2017), Adulterated pharmaceutical chemicals in botanical dietary supplements: novel screening approaches. Reviews in Analytical Chemistry, 36(3), pp. -. doi:10.1515/revac-2016-0032.
40 Duron, R.R., Almaguer, L. C., Garza-Juárez, A. De J., De La Luz, Ma., Cavazos, Salazar, Waksman-De-Torres, N., (2009), Development and Validation of Thin-Layer Chromatographic Methods for Quality Control of Herbal Products. Acta Chromatographica 21:203–215.
41 Ariburnu E, Mehmet FU, Huseyin Y, Erdem Y., (2012), Comparative determination of sibutramine as an adulterant in natural slimming products by HPLC and HPTLC densitometry. Journal of Pharmaceutical and Biomedical Analysis, 64–65:77–81.
42 Nicoletti, M., (2011), HPTLC fingerprint: a modern approach for the analytical determination of botanicals. RevistaBrasileira de Farmacognosia, 21(5), 818–823.
43 Attimarad, M., Ahmed, K. K. M., Aldhubaib, B. E., & Harsha, S. (2011). High-performance thin layer chromatography: A powerful analytical technique in pharmaceutical drug discovery. Pharmaceutical Methods, 2(2), 71–75. http://doi.org/10.4103/2229-4708.84436.

The recent HPTLC instrumentation allows obtaining fingerprints, as specific tracks useful to ascertain the identity of raw material and constituents of products, such as herbal supplements or herbal remedies[44]. HPTLC is also widely used as screening tool for dietary supplements adulterated with pharmaceutical chemicals including PDE-5inhibitors[45] and anorectic drugs[46]. The HPTLC-UV densitometry method was applied for the identification and quantification of sibutramine in adulterated herbal slimming supplements[47].Although appropriate for detection of adulterants present in weight loss, muscle building, or sexualenhancement supplements, both TLC and HPTLC methods require reference standards for a positive identification, therefore being inappropriate for screening adulterations with new pharmacological drugs, designer drugs.[48]

*Table 2. Features of HPTLC versus classical TLC*

| | **Classical TLC** | **HPTLC** |
|---|---|---|
| Average particle size | 10-12 μm | 5-6 μm |
| Particle size distribution | 5-20 μm | 4-8 μm |
| Layer thickness | 250 μm | 200 μm (100 μm) |
| Plate height | 30 μm | 12 μm |
| Typical migration distance | 10-15 cm | 3-6 cm |
| Typical separation time | 20-200 min | 3-20 min |
| Number of samples most often allied to plate | < 10 | < 36 (72) |
| Range sample volume | 1-5 μl | 0.1-0.5 μl |
| Detection limits: absorption | 1-5 ng | 100-500 pg |
| Detection limits: fluorescence | 50-100 pg | 5-10 pg |

*Source: adapted from Merck Millipore website*

*High-performance liquid chromatography (HPLC).* HPLC is a well-established and widespread separation method that can be applied to analyzedifferentcompounds with a wide range of molecular weights[49],[50]. The main advantage of HPLC regarding authenticity is its abilityto separate, identify and quantitate the minor and specific compoundsbased on the

44 Toniolo, C., Nicoletti, M., Maggi, F., Venditti, A., (2014), HPTLC determination of chemical composition variability in raw materials used in botanicals. Natural Product Research, 28(2):119–26.
45 Singh, S., Prasad, B., Savaliya, A.A., Shah, R.P., Gohil, V.M., Kaur, A., (2009), Strategies for characterizing sildenafil, vardenafil, tadalafil and their analogues in herbal dietary supplements, and detecting counterfeit products containing these drugs. Trends in Analytical Chemistry, 28:13–28.
46 Ariburnu E, Mehmet FU, Huseyin Y, Erdem Y., (2012), Comparative determination of sibutramine as an adulterant in natural slimming products by HPLC and HPTLC densitometry. Journal of Pharmaceutical and Biomedical Analysis, 64–65:77–81.
47 Mathon, C., Ankli, A., Reich, E., Bieri, S., Christen, P., (2014), Screening and determination of sibutramine in adulterated herbal slimming supplements by HPTLC-UV densitometry. Food Additives & Contaminants: Part A, 31:15–20.
48 Namera, A., Kawamura, M., Nakamoto, A., Saito, T., & Nagao, M. (2015). Comprehensive review of the detection methods for synthetic cannabinoids and cathinones. Forensic Toxicology, 33(2), 175–194. http://doi.org/10.1007/s11419-015-0270-0.
49 Sass-Kiss. A., Chromatographic Technique: Highperformance Liquid Chromatography (HPLC), in: Modern Techniques for Food Authentication. Sun, D.-W. (ed.), Elsevier, 2008.
50 De Carvalho, L.M., Martini, M., Moreira, A.P., De Lima, A.P., Correia, D., Falcão, T., Garcia, S.C., De Bairros, A.V., do Nascimento, P.C., Bohrer, D., (2011), Presence of synthetic pharmaceuticals as adulterants in slimming phytotherapeutic formulations and their analytical determination. Forensic Science International, 204(1):6–12.

spectral peak and retention time compared to those obtained for standards[51]. HPLC and ultra-high performance liquid chromatography (UHPLC) coupled to UV or diode array detectors are applied for the analysis of pharmaceutical adulterants in dietary supplements, in particular those used for weight control and sexual performance enhancement. However, in the absence of appropriate standards, especially in the case of new analogs/designer drugs, these simple and cost-effectivetechniques, have limited applicability[52]. Nevertheless, in some cases, HPLC can beused as screening toolfor the detection of such adulterants, especially those analogs structurally similar to the native compound, as they will present different retention times but identical UV spectra[53].HPLC methods used for analysis of the common adulterants are usually based on the use of octadecylsilane (C-18) as stationary and acetonitrile as mobile phaseand coupled to MS detector[54].As can be seen in Figure 2, liquid chromatography-tandem mass spectrometry (LC-MS) has recently become the method of choice in analysis of adulterants in food supplements[55],[56]including anorexics, diuretics, benzodiazepines, antidepressants, analgesics, hypoglycemics and other[57]. This system combines the separation power of LC with the ability of an MS to selectively detect and confirm molecular identity[58].

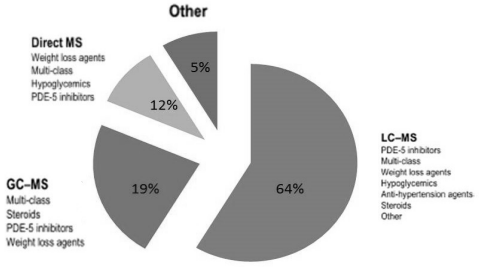



*Figure2. The percentage of qualitative and quantitative MS analysis of pharmaceuticals adulterations in dietary supplements and herbal remedies published between 1997 and 2014 (adapted from Vaclavik, 2014)*

Depending on the level of selectivity required, various MS systems with different types of mass analyzers included triple quadrupole (QqQ), single quadrupole (Q), ion trap (IT) andtime-of-flight (TOF) mass spectrometers and different data acquisition modeshavebeen

51 Ibid.
52 Rocha, T., Amaral, J. S. and Oliveira, M. B. P.P., (2016), Adulteration of Dietary Supplements by the Illegal Addition of Synthetic Drugs: A Review. Comprehensive Reviews in Food Science and Food Safety, 15:43–62.
53 Hou, P., Zou, P., Low, M.Y., Chan, E., Koh, H.L., (2006), Structural identification of a new acetildenafil analogue from pre-mixed bulk powder intended as a dietary supplement. Food Additives & Contaminants: Part A, 23:870–5.
54 Walker, M.J., Naughton, D.P., Deshmukh, N., Burns, D.T., (2016), A review of methods for the simultaneous detection of illegal ingredients in food supplements. Journal of the Association of Public Analysts. 44:51–66.
55 Vaclavik, L., Krynitsky, A.J., Rader, J.I., (2014), Mass spectrometric analysis of pharmaceutical adulterants in products labeled as botanical dietary supplements or herbal remedies: a review. Analytical and Bioanalytical Chemistry, 406: 6767–90.
56 Liu, Y. and Lu, F. (2017), Adulterated pharmaceutical chemicals in botanical dietary supplements: novel screening approaches. Reviews in Analytical Chemistry, 36(3), pp. -. doi:10.1515/revac-2016-0032.
57 Deconinck, E., Sacré, P.Y., Courselle, P., De Beer, J.O., (2013), Chromatography in the detection and characterization of illegal pharmaceutical preparations. Journal of Chromatographic Science, 51(8):791–806.
58 Patel, D.N., Lin, L., Kee, C., Ge, X., Low, M., Koh, H., (2014), Screening of synthetic PDE-5 inhibitors and their analogues as adulterants: analytical techniques and challenges. Journal of Pharmaceutical and Biomedical Analysis, 87:176–90.

usedto provide information about the molecular weight, structure, identity and quantity of wide range of individual components[59].

LC-MS is more generally applicable method than GC-MS for the analysis of large, polar, ionic, thermally unstable and involatile compounds without chemical derivatization, which significantly shortens thetime required for analysis[60,61]. However, general searchable mass spectral librariesare not applicable for LC-MS analysis[62,63].

*Gas chromatography-mass spectrometry (GC-MS).* Despite being a sensitive, reproducible, accurate, and quantitative technique, well suited for the analysis of mixtures, the applicability of the use of GC-MS for analysis of the pharmaceutical adulterants in dietary supplementsis largely determined by the volatility and thermal stability of target compounds[64,65].GC-MShas been proved as a sensitive screening method for the detection of anabolics in sportssupplements[66]and cost saving and rapid method for identification of the sildenafil and its analogs in herbal preparations and food products[67]. Also, a simple and rapid procedure based on GC-MS is described for determination of synephrine, active principle of *Citrus aurantium* plant in different dietary supplements promoted to control the weight[68]. Besides its lipolytic activities, synephrine is structurally similar to endogenous neurotransmitters (epinephrine and norepinephrine) and ephedrine, andcan produce adverse cardiovascular effects[69].

## CONCLUSION

Counterfeiting of dietary supplements represents a global issue raising the economic and public health concerns. The authentication of these products in order to avoid undesirable, harmful side effects and to provide consumer protection is in high demands, becoming a serious problem worldwide. Among many techniques that could serve to ensure the safety of

59 Vaclavik, L., Krynitsky, A.J., Rader, J.I., (2014), Mass spectrometric analysis of pharmaceutical adulterants in products labeled as botanical dietary supplements or herbal remedies: a review. Analytical and Bioanalytical Chemistry, 406: 6767–90.

60 Becue, I., Van Poucke, C., Van Peteghem, C., (2011), An LC-MS screening method with library identification for the detection of steroids in dietary supplements. Journal of Mass Spectrometry, 46(3):327–35.

61 Popescu, A.M., Radu, G.L., Onisel, T., Raducanu, A.E., Niculae, C.G., (2014), Detection by gas chromatography-mass spectrometry of adulterated food supplements. Romanian Biotechnological Letters, 19(4):9485–9492.

62 Becue, I., Van Poucke, C., Van Peteghem, C., (2011), An LC-MS screening method with library identification for the detection of steroids in dietary supplements. Journal of Mass Spectrometry, 46(3):327–35.

63 Peters, R.J., Rijk, J.C., Bovee, T.F., Nijrolder, A.W., Lommen, A., Nielen, M.W., (2010), Identification of anabolic steroids and derivatives using bioassay-guided fractionation, UHPLC/TOFMS analysis and accurate mass database searching. AnalyticaChimica Acta, 664:77–88.

64 Vaclavik, L., Krynitsky, A.J., Rader, J.I., (2014), Mass spectrometric analysis of pharmaceutical adulterants in products labeled as botanical dietary supplements or herbal remedies: a review. Analytical and Bioanalytical Chemistry, 406: 6767–90.

65 Rocha, T., Amaral, J. S. and Oliveira, M. B. P.P., (2016), Adulteration of Dietary Supplements by the Illegal Addition of Synthetic Drugs: A Review. Comprehensive Reviews in Food Science and Food Safety, 15:43–62.

66 Van Thuyne, W., Delbeke, F.T., (2004), Validation of a GC-MS screening method for anabolizing agents in solid nutritional supplements. Biomedical Chromatography, 18(3):155–9.

67 Man, C.N., Nor, N.M., Lajis, R., Harn, G.L., (2009), Identification of sildenafil, tadalafil and vardenafil by gas chromatography-mass spectrometry on short capillary column. 121Journal of Chromatography A, 6:8426–30.

68 Marchei, E., Pellegrini, M., Pacifici, R., Zuccaro, P., Pichini, S., (2006), A rapid and simple procedure for the determination of ephedrine alkaloids in dietary supplements by gas chromatography-mass spectrometry. Journal of Pharmaceutical and Biomedical Analysis, 41:1633–41.

69 Jordan, S., Murty, M., Pilon, K., (2004), Products containing bitter orange or synephrine: suspected cardiovascular adverse reactions. Canadian Medical Association Journal, 12;171(8):993-4.

these products available in the market, chromatographic methods could be applied for separation of minute product quantities enabling the cope with tremendously complex and extremely dilute samples. These methods include the combinations of gaseous or liquid phases, giving rise to the types of chromatography used in analysis, such are gas or liquid chromatography (coupled with mass spectrometry or alone), thin-layer chromatography and (ultra) high-performance thin-layer chromatography, generally considered as easy, reliable and accurate techniques in determination of adulterated compounds. In order to avoid possible drug interactions and harmful health effects and to ensure the quality of dietary supplements, besides using already available techniques, the need to develop innovative methodologies or improved analytical techniques for the detection of adulterant compounds from different pharmaceutical substances and their analogs is of a great importance.

## REFERENCES

1. Adulteration of dietary supplements with drugs and drug analogs. Pharmacopeial Forum, 2014, 41(3). United States Pharmacopeial Convention, Rockville, MD.
2. Ambrose, A., Cho, B.-K., (2014). A Review of Technologies for Detection and Measurement of Adulterants in Cereals and Cereal Products. Journal of Biosystems Engineering, 39(4):357–365.
3. Ariburnu E, Mehmet FU, Huseyin Y, Erdem Y., (2012), Comparative determination of sibutramine as an adulterant in natural slimming products by HPLC and HPTLC densitometry. Journal of Pharmaceutical and Biomedical Analysis, 64–65:77–81.
4. Attimarad, M., Ahmed, K. K. M., Aldhubaib, B. E., & Harsha, S. (2011). High-performance thin layer chromatography: A powerful analytical technique in pharmaceutical drug discovery. Pharmaceutical Methods, 2(2), 71–75. http://doi.org/10.4103/2229-4708.84436.
5. Azad, T. & Ahmed, S. (2016) International Journal of Food Contamination 3(22). doi:10.1186/s40550-016-0045-3.
6. Becue, I., Van Poucke, C., Van Peteghem, C., (2011), An LC-MS screening method with library identification for the detection of steroids in dietary supplements. Journal of Mass Spectrometry, 46(3):327–35.
7. Blackstone, E. A., Fuhr, J. P., &Pociask, S., (2014). The Health and Economic Effects of Counterfeit Drugs. American Health & Drug Benefits, 7(4), 216–224.
8. Brown, P.N., Paley, L.A., Roman, M.C., Chan, M., (2008), Single-Laboratory Validation of a Method for the Detection and/or Quantification of Select Alkaloids in Goldenseal Supplements and Raw Materials by Reversed-Phase High-Performance Liquid Chromatography. Pharmaceutical Biology, 46(1–2):135–144.
9. Cimpoiu, C. and Hosu, A. (2007), Thin layer chromatography for the analysis of vitamins and their derivatives. Journal of Liquid Chromatography & Related Technologies, 30, 701–728.
10. Curtis, J.M., Berrigan, N., Dauphinee, P., (2008), The determination of n-3 fatty acid levels in food products containing microencapsulated fish oil using the one-step extraction method. Part 1: measurements in the raw ingredient and in dry powdered foods. Journal of the American Oil Chemists' Society, 85:297–305.
11. De Carvalho, L.M., Martini, M., Moreira, A.P., De Lima, A.P., Correia, D., Falcão, T., Garcia, S.C., De Bairros, A.V., do Nascimento, P.C., Bohrer, D., (2011), Presence of synthetic

pharmaceuticals as adulterants in slimming phytotherapeutic formulations and their analytical determination. Forensic Science International, 204(1):6–12.

12. Deconinck, E., Sacré, P.Y., Courselle, P., De Beer, J.O., (2013), Chromatography in the detection and characterization of illegal pharmaceutical preparations. Journal of Chromatographic Science, 51(8):791–806.
13. Duron, R.R., Almaguer, L. C., Garza-Juárez, A. De J., De La Luz, Ma., Cavazos, Salazar, Waksman-De-Torres, N., (2009), Development and Validation of Thin-Layer Chromatographic Methods for Quality Control of Herbal Products. Acta Chromatographica 21:203–215.
14. Gallup, A.M., 2008. The Gallup Poll Cumulative Index: Public Opinion, 1998-2007. Rowman and Littlefield, Lantham, Maryland.
15. Georgiou, C.A., Danezis, G.P., (2015), Elemental and isotopic mass spectrometry, in: Advanced mass spectrometry for food safety and quality, Ed. Y. Pico, Comprehensive Analytical Chemistry, Elsevier, 2015, pp. 131–243.
16. Haneef, J., Shaharyar, M., Husain, A., Rashid, M., Mishra, R., Siddique, N. A. and Pal, M. (2013), Analytical methods for the detection of undeclared synthetic drugs in traditional herbal medicines as adulterants. Drug Test. Analysis, 5: 607–613. doi:10.1002/dta.1482.
17. Hou, P., Zou, P., Low, M.Y., Chan, E., Koh, H.L., (2006), Structural identification of a new acetildenafil analogue from pre-mixed bulk powder intended as a dietary supplement. Food Additives & Contaminants: Part A, 23:870–5.
18. http://www.psychiatrictimes.com/articles/dietary-supplement-adulteration-erectile-dysfunction-weight-loss-and-sports.
19. http://www.searo.who.int/entity/world_health_day/2015/whd-what-you-should-know/en/.
20. http://www.usp.org/sites/default/files/usp/document/about/public-policy/public-policy-dietary-supplements.pdf.
21. https://webgate.ec.europa.eu/rasff-window/portal/.
22. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3632147/pdf/S114.pdf.
23. Iammarino, M., Marino, R. and Albenzio, M., (2017), How meaty? Detection and quantification of adulterants, foreign proteins and food additives in meat products. Int J Food Sci Technol, 52: 851–863. doi:10.1111/ijfs.13350.
24. Đuriš, J.,Vidović, B.,Čalija, B., Milašinović, N., (2016), Anti-counterfeiting Food and Drug Packaging Technologies and Forensic Tools: Present State and Future Trends, International Scientific Conference "Archibald Reiss Days", 3–4. March, Belgrade, Serbia, 237–251.
25. Jordan, S., Murty, M., Pilon, K., (2004), Products containing bitter orange or synephrine: suspected cardiovascular adverse reactions. Canadian Medical Association Journal, 12;171(8):993–4.
26. Khazan, M., Hedayati, M., Kobarfard, F., Askari, S., Azizi, F., (2014), Identification and Determination of Synthetic Pharmaceuticals as Adulterants in Eight Common Herbal Weight Loss Supplements. Iranian Red Crescent Medical Journal, 16(3):e15344.
27. Liu, Y. and Lu, F., (2017), Adulterated pharmaceutical chemicals in botanical dietary supplements: novel screening approaches. Reviews in Analytical Chemistry, 36(3):1–14. doi:10.1515/revac-2016-003.
28. Lo, Y.T., Shaw, P.C., (2018), DNA-based techniques for authentication of processed food and food supplements. Food Chemistry, 240:767–774.

29. Man, C.N., Nor, N.M., Lajis, R., Harn, G.L., (2009), Identification of sildenafil, tadalafil and vardenafil by gas chromatography-mass spectrometry on short capillary column. 121 Journal of Chromatography A, 6:8426–30.
30. Marchei, E., Pellegrini, M., Pacifici, R., Zuccaro, P., Pichini, S., (2006), A rapid and simple procedure for the determination of ephedrine alkaloids in dietary supplements by gas chromatography-mass spectrometry. Journal of Pharmaceutical and Biomedical Analysis, 41:1633–41.
31. Mathon, C., Ankli, A., Reich, E., Bieri, S., Christen, P., (2014), Screening and determination of sibutramine in adulterated herbal slimming supplements by HPTLC-UV densitometry. Food Additives & Contaminants: Part A, 31:15–20.
32. Maughan, R.J., (2013), Quality assurance issues in the use of dietary supplements, with special reference to protein supplements. Journal of Nutrition, 143(11):1843S–1847S.
33. Mudge, E.M., Betz, J.M., Brown, P.N., (2016), The Importance of Method Selection in Determining Product Integrity for Nutrition Research. Advances in Nutrition, 7(2):390–398.
34. Namera, A., Kawamura, M., Nakamoto, A., Saito, T., & Nagao, M. (2015). Comprehensive review of the detection methods for synthetic cannabinoids and cathinones. Forensic Toxicology, 33(2), 175–194. http://doi.org/10.1007/s11419-015-0270-0.
35. Nicoletti, M., (2011), HPTLC fingerprint: a modern approach for the analytical determination of botanicals. RevistaBrasileira de Farmacognosia, 21(5), 818–823.
36. 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.
37. Patel, D.N., Lin, L., Kee, C., Ge, X., Low, M., Koh, H., (2014), Screening of synthetic PDE-5 inhibitors and their analogues as adulterants: analytical techniques and challenges. Journal of Pharmaceutical and Biomedical Analysis, 87:176–90.
38. Peters, R.J., Rijk, J.C., Bovee, T.F., Nijrolder, A.W., Lommen, A., Nielen, M.W., (2010), Identification of anabolic steroids and derivatives using bioassay-guided fractionation, UHPLC/TOFMS analysis and accurate mass database searching. AnalyticaChimica Acta, 664:77–88.
39. Rocha, T., Amaral, J. S. and Oliveira, M. B. P.P., (2016), Adulteration of Dietary Supplements by the Illegal Addition of Synthetic Drugs: A Review. Comprehensive Reviews in Food Science and Food Safety, 15:43–62.
40. Popescu, A.M., Radu, G.L., Onisel, T., Raducanu, A.E., Niculae, C.G., (2014), Detection by gas chromatography-mass spectrometry of adulterated food supplements. Romanian Biotechnological Letters, 19(4):9485–9492.
41. Sarma, N., Giancaspro, G., Venema, J. (2016), Dietary supplements quality analysis tools from the United States Pharmacopeia. Drug Testing and Analysis, 8(3-4):418–423.
42. Sass-Kiss. A., Chromatographic Technique: Highperformance Liquid Chromatography (HPLC), in: Modern Techniques for Food Authentication. Sun, D.-W. (ed.), Elsevier, 2008.
43. Sherma, J., Analysis of counterfeit drugs by thin layer chromatography. Acta Chromatographica, 19:5–20, 2007.
44. Singh, S., Prasad, B., Savaliya, A.A., Shah, R.P., Gohil, V.M., Kaur, A., (2009), Strategies for characterizing sildenafil, vardenafil, tadalafil and their analogues in herbal dietary supplements, and detecting counterfeit products containing these drugs. Trends in Analytical Chemistry, 28:13–28.

45. Toniolo, C., Nicoletti, M., Maggi, F., Venditti, A., (2014), HPTLC determination of chemical composition variability in raw materials used in botanicals. Natural Product Research, 28(2):119–26.

46. Vaclavik, L., Krynitsky, A.J., Rader, J.I., (2014), Mass spectrometric analysis of pharmaceutical adulterants in products labeled as botanical dietary supplements or herbal remedies: a review. Analytical and Bioanalytical Chemistry, 406: 6767–90.

47. Van Thuyne, W., Delbeke, F.T., (2004), Validation of a GC-MS screening method for anabolizing agents in solid nutritional supplements. Biomedical Chromatography, 18(3):155–9.

48. Vemireddy, L.R., Satyavathi, V.V., Siddiq, E.A., Nagaraju, J., (2015). Review of methods for the detection and quantification of adulteration of rice: Basmati as a case study. Journal of Food Science and Technology, 52(6), 3187–3202.

49. Walker, M.J., Naughton, D.P., Deshmukh, N., Burns, D.T., (2016), A review of methods for the simultaneous detection of illegal ingredients in food supplements. Journal of the Association of Public Analysts. 44:51–66.

50. Wheatley, V.M. and Spink, J., (2013), Defining the Public Health Threat of Dietary Supplement Fraud. Comprehensive Reviews in Food Science and Food Safety, 12: 599–613.

# MODERN TECHNOLOGIES OF FORENSIC BALLISTICS EXAMINATIONS

**Dmitry Sergeevich Korovkin**,
Head of the Department of Forensic Examinations and Studies of the Federal State Treasury Educational Institution of Higher Education "Saint-Petersburg University of the Ministry of Internal Affairs of the Russian Federation",
Candidate of Juridical Sciences, Associate Professor, Police Colonel.

**Abstract:** In modern Russian forensic examinations, the technology of producing forensic examination in most cases is understood as a set of methods and instruments applied during production examinations or a set of scientific knowledge applied to solve specific expert tasks. Thus, when we talk about modern technologies for the production of forensic ballistics, we talk about new methods of research, modern technical means used in the production of examinations and specific methodological recommendations for the production of studies of certain types of forensic ballistics. Diagnostic testing is traditionally understood as the researches directed at determining group accessory of objects (for example, relevancy to the category of "firearms"), definition of technical conditions (suitability to produce shots and "serviceability"); determination of cause and effect relationships within clarification of circumstances of firearms using.Considering the production technology of forensic and ballistic examinations as a set of methodical recommendations about production of concrete researches, we should talk about the relevance of developing and improving research methods new to the Russian forensic ballistics objects, such as: main parts of firearms, the written-off firearms, copies and remarks of ancient and antique weapons. No less relevant is the technology of production of situational complex medical and criminalistic examinations aimed at establishing the circumstances of the use of firearms. In the field of identification studies of firearms, technology of using electron-raster, scanning and confocal microscopes is gaining importance.

**Key words:** forensic-ballistic examination, firearms, parts of weapons, microscopy.

## INTRODUCTION

In modern Russian forensic examination the technology of production of forensic examination, in most cases, means a set of methods and tools used in the manufacture of forensic examinations or a set of scientific knowledge used to solve specific expert tasks. Thus, when we talk about modern technologies for the production of forensic ballistics, we talk about new methods of research, modern technical means used in the production of examinations and specific methodological recommendations for the production of researches of certain types of forensic ballistics.

## FORMATION OF A SINGLE DEPARTMENTAL APPROACH TO THE PRODUCTION OF FORENSIC BALLISTICS

In the opinion of many experts, the existence of clearly defined procedures for the production of examinations, which have clearly prescribed the procedure in normative documents and bylaws, will help avoid the "departmental" approach to the production of examinations. This will exclude the possibility of excessive expert initiative, arbitrary interpretations of individual methods, as well as the detrimental influence of expert non-competence, which mostlydepends on the personal qualities of the expert. It is believed that the introduction of expert technology is a direct way to the uniformity of research on a certain category of objects, since it will contain a certain list of compulsory technical means, the sequence of actions of the expert, as well as formalized conclusions that depend on one or another result of the study.

At the moment, the research methods of individual objects developed within the Ministry of Internal Affairs of the Russian Federation have approximately one structure and include the following elements: tasks; objects of research; the essence of the methodology; characteristics of the object under research; subject to investigation; the necessity to consider the materials of the criminal case; equipment; instruments; materials; sequence of actions of the expert; formulation of conclusions. Particular attention in the development of new or improvement of old techniques is given to the sequence of action of the expert and the projected impact of the results obtained, regarding compliance with the logic of cause and effect relationships.

## STRUCTURE OF FORENSIC BALLISTICS EXAMINATION

Several independent types of research are singled out in the Russian forensic-ballistic examination, which form a forensic ballistic examination structure, and they include: a diagnostic examination of factory firearms; diagnostic examination of factory-made cartridges; diagnostic examination of the main parts of factory-made firearms; diagnostic examination of self-made firearms; diagnostic research of pneumatic and gas weapons, limited firearms; diagnostic examination of products constructively similar to firearms; identification research of traces of firearms on liners; situational researches of establishing the circumstances of the use of gunshot and the reasons and conditions for the production of the shot.

The diagnostic examinationis traditionally understood as anexamination aimed at: establishing the group belonging of objects (for example, relevance to the category of "firearms"), determining the technical state (suitability for the production of shots and "serviceability"); establishing cause and effect relationships in the context of clarifying the circumstances of the use of firearms.

## THE PROBLEMATIC ISSUES OF RESEARCH ON DECOMMISSIONED FIREARMS AND THE MAIN PARTS OF FIREARMS

Considering the technology of production of forensic ballistics as a set of methodological recommendations for the production of specific studies, one should speak of the urgency of developing and improving research methods in relation to new objects for the Russian foren-

sic ballistics, such as, the written-off firearms; the main parts of firearms; copies and replicas of antique weapons.

Deactivated firearms as the object of forensic ballistics examination came into force in Russia as a result of changes introduced on July 10, 2012 in Article 1 of the Russian Federal Law № 150 "On Arms" of November 13, 1996.

In accordance with the provisions of Article 1 of the aforementioned law, deactivated firearms should be understood as written-off firearms, in each major part of which the technical changes are made, excluding the possibility of a shot from it or using its basic parts of ammunition, including throwing equipment, and which is intended for use in the implementation of cultural and educational activities with the ability to simulate a shot from a cartridge light and sound action (inert weapons) or without the possibility of simulating a shot from it (training weapons), or to study the processes of interaction of parts and mechanisms of weapons (split weapons);

- old (antique) weapons are weapons, missile and air weapons manufactured prior to the end of 1899 (except for firearms manufactured to fire cartridges), and bladed weapons manufactured before the end of 1945;

- a copy of the old (antique) weapons are weapons manufactured to original drawings or sample vintage (antique) weapons, provided of exact or large-scale reproduction of its design, appearance and artistic design that does not include genuine parts of antique or other weapons;

- a replica of the old (antique) weapons are weapons made according to the original drawings or description of a sample vintage (antique) weapons with a creative variation of design, appearance, or artistic decoration of cultural value as a model of artistic and decorative-applied art;

All the terms and definitions introduced in the Law are newto date; therefore, their place in the conceptual framework of forensic ballistics is not fully determined. Accordingly, there are no methodological recommendations for researching this category of objects. It is also noted that the definitions of certain concepts are rather controversial from the standpoint of the modern theory of the Russian weapons science.So the term "deactivated weapon" in the context in which it is used does not at all reflect the characteristics of objects falling under its definition. Especially it concerns such a version of it as a written-off firearm with the ability to simulate a shot from it with a cartridge of light-and-sound action (inert weapons).For a long time, these objectswere manufacturedhere in Russia and were sold as signalling devices manufactured from weapons that were removed from service. In addition, models (the mass and dimensions of firearms) specified as "deactivated" firearms are produced from dismantled military firearms abroad. In Russia, these objects were, until 2005, produced as equipment for theatrical and entertainment enterprises on the basis of specially designed specifications exactly as mass-size models. At the same time, often in the course of their forensic research, they are in violation of the current methodology for resolving the issue of the object belonging to firearms (approved by the Federal Interdepartmental Coordination and Methodological Council on the problems of expert research and recommended for use in expert institutions of the Russian Federation, Minutes № 8 of 29.02. 2000) were recognized as defective firearms.[1]

It should be noted that, in accordance with the provisions of the above-mentioned methodology, antique (antiquarian) weapons, a copy of antique (antique) weapons and replica of antique (antiquarian) weapons are nothing more than a firearm if it is capable of firing a shell with a directed movement and possessing a specific kinetic energy not less than 0.5 J/mm$^2$

1 The methodology of establishing the belonging of the object to firearms. Moscow: FEC of the MIA of Russia, 2000.

(50 J/cm$^2$). However, it is necessary that their turnover is determined not by the certification bodies, but based on the conclusion of a certified expert of the Ministry of Culture of the Russian Federation.

Deactivated firearms in accordance with the provisions of Art. 2 of the Law on Arms, belongs to the category of civilian weapons and in accordance with the provisions of Art. 9 these objects are sold to citizens who have reached the age of 18 without permission (licensing). Accordingly, the written-off weapons belong to the category of civilian weapons, but since there is no danger, criminal responsibility for their turnover does not apply.

These objects are allowed for civilian circulation based on the decision of the certification body, which in their work are guided by the relevant state standards and forensic requirements.

In addition to such products that passed through the certification body, the population in circulation has products made from firearm knots and parts of the Second World War period. In Russia, these objects are confiscated primarily from members of military historical clubs engaged in the reconstruction of representatives of the opposing sides of the period. Units and parts (formerly parts of combat firearms) used in the manufacture of such products were derived from weapons found in the territories on which the fighting took place during the Second World War and parts of the "deactivated" weapons.

Despite the fact that these objects directly fall under the influence of the method of solving the question of the components of a firearm (approved by the Federal Interdepartmental Coordination and Methodological Council on the problems of expert studies and recommended for use in expert institutions of the Russian Federation, Minutes № 8 of 29.02.2000), the decision of the expert question on the serviceability of firearms and its suitability for shooting (approved by the Methodical Council of Expert Forensic Centre of the Ministry of Internal Affairs of the Russian Federation, Minutes № 1 dated May 30, 2013), the questions of their forensic expert research require additional methodological support.

In accordance with the current methodology for resolving the issue of the components of firearms, all objects of self-made production, regardless of whether they are assembled from parts or assemblies of industrial production or from self-made fabrication, and also their combinations fall under the category of weapons. In the event that they have a complex of features of the material part of the object that determine its intended purpose, as well as energy characteristics that ensure the possibility of using the object for its intended purpose.Additionally, it is determined by the presence of three main groups of characteristics: constructive; energy characteristics of the projectile; reliability. The structural features of the material part of the object characterize its intended purpose and, with reference to firearms, presupposes at a minimum the presence of the following constructional elements: a device for dispersing the missile and giving it a directed movement (barrel); barrel channel locking device; device for ignition of propellant charge.

Shooting devices that are structurally similar to "decommissioned firearms" and have the ability to simulate shots, which have not been certified by the State, in the opinion of some experts, do not belong to the category of "deactivated weapons"and to the group of self-made products. In all these cases, there is no trunk, as a device for dispersing the projectile and giving it a directional movement, since it contains not retrievable bushings, pins or spreader plates. Under the circumstance, everything is extremely clear that the product is self-made, according to its origin, despite the industrial parts used for its assembly. However, since very often the appearance of the product does not differ much from an industrial product, it is regarded by the expert as defective firearms but not as an item of self-made manufacturing and unsuitable for shooting by a cartridge the structure of which has a missile.

Unfortunately, in the fundamental method that we are considering, it is said that in the frames of solving the problem of the object's relevance to the category of firearms, the fact of a possible malfunction and unsuitable for firing (production of shots) of factory firearms does not matter. The purpose of the object will not change from its state. These issues are closely interrelated, but their consideration is beyond the frames of this method. In connection with the fact that at the moment there are no interdepartmental methodological recommendations for assessing the boundaries and the limits of malfunctions of factory-made weapons (in the case of self-made products, this issue is not solved, since in relation to them the issue's solution of relevance to the category of firearms directly depends on the specific kinetic energy of missile shot from it) and the causes and conditions of their occurrence and the logical patterns of the conclusions about the malfunction of weapons. The lack of expert technology for determining the malfunction of factory-made weapons and the availability of objects assembled from factory-made parts, but not in compliance with all technological processes, processing and joining parts, and debugging and alignment, leads to a number of expert collisions. With regard to self-made assemblies or parts of firearms that have been constructed or reconstructed, which are structurally similar to legally fixed and admitted to circulation by the state certification bodies.

The expert, depending on the level of his training, competencies, skills and abilities, interpreting the methodology's provisions of the decisions on the issue of belonging to a firearm can come to the following conclusions: the object presented to the study is a firearm, manufactured industrially, unsuitable for the production of shots; the object presented to the study is a firearm, industrial manufacture, defective and unsuitable for the production of shots; the object presented to the study is a self-made firing device that is structurally similar to a firearm and designed to simulate shots.

The criminal liability for the illegal turnover of firearms is a threat to the owner, in the event of availability the first conclusion in the expert evidence. In the other two cases, liability is excluded, however, it is only in the event that the composition of the product does not contain the main parts of firearms that remain when assembling or manufacturing without modification.

At this moment, the analysis of expert practice shows that experts use two basic methods of solving the question of relevance of the investigated object to the category of the main parts of firearms. These methods have significant influence to the conclusion, but at the same time, nowhere and in any way not fixed, in the framework of officially accepted methods:

- Comparison of the design features of the object under study (shape, dimensions, availability of certain parts, assemblies, elements, and marking symbols) with information about the main parts of firearms contained in special reference literature.

- The installation of the main parts in place of similar details in known good-quality firearms, with the subsequent production of shots.

Both of the above methods have disadvantages.

The first way is speculative and so cannot be confirmed by effective experiment. More so, in most cases, the special reference literature does not contain structural elements' size characteristics. In the best-case scenario, there are detailed schemes of the main firearms' installation. The Russian literature, unfortunately, allows for relatively detailed analysis of firearms of exclusively domestic production, or the firearms of the Second World War period.

In the second case, the production of shots certainly indicates not only the relevance of the objects to the category of the main parts, but also their technical suitability for ensuring the functioning of the weapon in the production of the shot. However, in most cases, experts do not have the necessary copies of firearms. It is not always possible in the conditions of an

expert forensic laboratory to replace certain parts with others. For example, replacement of the trunk is not always possible without special tools and proper gunsmith skills.

In addition to the lack of methodology and methodological recommendations aimed at addressing the issue of the objects' relevance to the category of the main parts of firearms, the question of the range of objects, which must be researched in the examination of the main parts of firearms, remains uncertain. It is also necessary to determine the forensic requirements and criteria for this category of objects, as the main parts of firearms.

From the above, the main details of improvised shooting devices cannot be classified as main detail of factory-made firearms, because we cannot fully know by what the person who produced it was guided. Criminal liability connected by self-made firearms comes only if their construction provides the possibility of producing shots in the course of which the missile which left the bore has a specific kinetic energy of not less than 0.5 J/mm2 (50 J/cm2). Accordingly, with regard to self-made firearms, we can talk about it as an integral system which is not subject to sweeping expert evaluation. This expert evaluation influences the criminal-legal qualification of the acts related to it.

By analogy with the self-made firearms, the details of factory manufacturing subjected to changes introduced by a self-made way, due to which they changed their initial technical parameters and construction, cannot be attributed to the main parts of firearms.

In our opinion, during the research process of the firearms, the main parts are exposed to adverse factors, as a result they were subjected to corroding of different degrees. It is necessary to indicate in expert evidence how much the state of its surfaces has changed, whether the small details ensuring the regular functioning of the main parts are not lost and whether the condition of the object allows them to be used for the intended purpose of the main parts of the firearm. These conclusions, in a number of cases, can be made without installing the details in standard samples and experimental shooting.

It should be noted that recently, one more point of view appeared on the questions connected with expert research of the main parts of firearms. It is the fact that an expert who is a specialist in the field of judicial ballistics and forensic ballistics expertise and who has received the relevant training is not entitled to resolve this issue. Firstly, this issue is to some extent juridical (this view seems to us not entirely correct). Secondly, none of the programs of judicial ballistics and forensic ballistics expertise, which carried out the training of forensic experts, either in full-time form of training or in retraining or advanced training, does not contain topics related to the study of the firearms' main parts.

Not in one specialized publication these questions have not found their complete reflection.[2] Approved methodologies or guidelines on this issue are also missing. In this regard, the question arises: what kind of person then will be competent in resolving this issue, because the variety of firearms is so great that neither military engineers, firearm specialists, nor persons trained in firearms design engineers will not possess all knowledge of the design of the main parts of the entire variety of firearms.

2 Forensic investigation of weapons and traces of its use: Part 1: textbook / ed. V.A. Ruchkin, I.A. Chulkov. 2nd ed. Volgograd: VA of the MIA of Russia, 2011; Kokin M.V., Yarmak K.V. Forensic ballistics and forensic ballistics expert examination: textbook. Moscow: Unity-Dana, 2014; Chulkov I.A. , Latyshev I.A. The material part of shooting firearms. Forensic aspects: study guide, 2nd ed. corrected and additional. Volgograd: VA of the MIA of Russia, 2010; The methodology of establishing the belonging of the object to firearms. Moscow: FEC of the MIA of Russia, 2000.

# PROBLEMS OF IMPROVING THE PRODUCTION OF SITUATIONAL FORENSIC-BALLISTIC AND COMPLEX MEDICAL-FORENSIC EXAMINATIONS

Problems of improving the production of situational forensic-ballistic and complex medical-criminalistics examinations aimed at establishing the circumstances of the use of firearms remain topical. Topicality of improving the methodological support of these examinations is due to a number of factors which arenot only objective but also subjective.

Diversity and different characters of the researchable objects can be attributed to the factors of objective nature that affect the necessity to improve the methodological support of the type of expert research under consideration. Proceeding from the data of the established practice of conducting forensic ballistic situational examinations (on the example of St. Petersburg and the Leningrad region), the objects of this type of expertise include:

- firearms (including limited firearms);
- air weapon;
- shooting devices (power-actuated fastening tool, starting pistols, devices for slaughtering, etc.);
- ammunition and cartridges for firearms and other shooting devices;
- fired bullets and shot cartridges, as well as traces associated with their use;
- the procedural documents contained in the materials of a criminal case (the protocols of the crime scene inspection, interrogation, the investigative experiment, verification of the testimony on the spot, expert opinions, etc.);
- crime scene material condition;
- the processes and developments accompanying the use of firearms.

It should be noted that in most cases a few different objects were subjected to expert research at the same time based on the content of the questions posed for resolution. For example, objects of firearms, traces on obstacles and a set of procedural documents (protocols of inspections, interrogations and investigative experiments).

The second group of factors of an objective nature results from a variety of objects and their combination within the framework of one research, which causes the existence of a variety of methods and their combinations, which are not only difficult to adopt, but there is necessity to improve them, taking into account specific expert tasks. Separately, there are situations when it is necessary to investigate, in the context of solving situational problems, not only different obstacles (the situation of the scene), but also objects of biological origin (living persons and corpses). Conducting research on the totality of these objects within a purely forensic-ballistic examination is impossible, because it requires the involvement of a specialist in forensic medicine. With rare exceptions, this specialist hasno special knowledge in the field of judicial ballistics. This gives rise to difficulties of subjective nature, caused by the necessity for a comprehensive and, as a rule, commission research of objects and, as a consequence, the necessity for competent selection of specialists, which do not exist in some regions.

The solution of the situational problems is aimed at establishing the following: the possibility of a shot from a firearm without pressing the trigger, under certain conditions; distance, direction and location of shot production; the relative position of the shooter and the victim at the time of the shot; sequence and number of shots; the possibility of causing gunshot injuries in a particular situation and conditions is directly related. In most cases, to expertly verify

versions of the elements of the method of committing a crime or establishing an instrument of crime.

It should be noted that assessing of forensic-ballistic situational expertise current state is based on the current practice of assessing evidence in court. This examination, especially if necessary, is a parallel study of biological and non-biological objects of damage (corpses, living persons, clothing and other non-biological barriers), it is immediately expedient to entrust specialists in the field of forensic ballistics, forensic medicine, and often specialists in the field of physical and chemical research. The urgency of improving the methodological foundations and production technologies of this expertise is becoming increasingly urgent if taking into account the variety of tasks to be performed and the differences of the facilities.

## USING THE ACHIEVEMENTS OF MODERN MICROSCOPY IN FORENSIC-BALLISTIC IDENTIFICATION RESEARCHES

Using technologies of electron raster, scanning confocal microscopes are becoming increasingly important in the field of identification research of firearms. Using of these tools allows us tosolve the problems of identification of tracks on firing shells and shot bullets, which leaves the weapon with a slight wear of the following forming details (striker hammer, barrel rifling field). Using of these tools allows for observing the displayed signs of wear and tear on the metalworking equipment used in the manufacture of firearms at the completely different level of trace micro-reliefincrease. For example, the operated optical comparative microscopes used today do not reveal differences of the traces on the bullets produced which are produced successively, in the enterprise, from the copies of one model of firearms. This is due to the fact that the working parts of modern equipment used in weapons production acquire new signs of wear only after processing 3-8 parts. Accordingly, from 3 to 8 barrels of firearms of the same model, successively released on the same equipment, will have a common micro-relief and a complex of introduced features. Individual differences in trace micro-relief due to low wear of production equipment, or the negligible impact of operational factors cannot be detected in the study of objects using modern comparative microscopes, the increase of which exceeds more than 400x. Scanning confocal and electron-raster microscopes make it possible to observe the object with a much larger increase, especially with regard to the increase in electron-raster microscopes. The increase in the latter can reach up to 4000x. The use of scanning probe microscopes is possible, but it is still the most acceptable of all scanning microscopes, the use of modern confocal scanning microscopes (NS-3000, Leica TCS-SP.8, Leica DSM 3D) to solve the problem of "little informative traces", receive a 3D image, but also measure the elements of the microrelief. Despite the positive examples of the use of scanning confocal microscopes on the increase in the altitudes of 800x, for the identification of firearms in the tracks on shot bullets and shot cartridges, the use of electron-raster microscopes is more preferable. During the long-term discussion supported by applied research, within the framework of the "School-Seminar on Forensic Weapons Science", operating on the basis of the Saratov National Research State University named after N.G. Chernyshevskyit was found that the increase in scanning confocal microscopes was not always sufficient, the resulting image, despite the possibility of obtaining, a pseudo 3D image was not always clear, and the observation field and the scanned surface had undesirably small dimensions. It is precisely with the use of electron-raster microscopes on an increase in the limits of 1000-1300x that it is possible to detect coincident or different traces in the tracks of the striker and the rifling fields that cannot be observed in optical comparative microscopes and with the use of scan-

ning confocal microscopes.[3] With foreign experience, the use of electron-raster microscopes and scanning confocal microscopes in the field of identification of firearms in the footsteps of shot bullets and shot cartridges can be found in the materials published in the AFTE Journal, published in the United States of America.[4]

## CONCLUSION

Summarizing all of the above, one can say that one of priority tasks facing the Russian forensic-ballistics is the task of developing unified interdepartmental approaches to the study of forensic-ballistic objects, especially such as decommissioned firearms and the main parts of firearms, and the introduction of more wide scale of modern electron-raster microscopes, which proved their effectiveness in solving identification problems, with regard to "little informative" traces of firearms on shot bullets and shot cartridges.

## REFERENCES

1. Chulkov I.A., Latyshev I.A. The material part of shooting firearms. Forensic aspects: study guide, 2nd ed. corrected and additional. Volgograd: VA of the MIA of Russia, 2010.
2. Forensic investigation of weapons and traces of its use: Part 1: textbook/ed. V.A. Ruchkin, I.A. Chulkov. 2nd ed. Volgograd: VA of the MIA of Russia, 2011.
3. Kokin M.V., Yarmak K.V. Forensic ballistics and forensic ballistics expert examination: textbook. Moscow: Unity-Dana, 2014.
4. The methodology of establishing the belonging of the object to firearms. Moscow: FEC of the MIA of Russia, 2000.
5. http://firearm-expert.sgu.ru.
6. AFTE Journal--Volume 45 Number 1-winter 2013.

3 http://firearm-expert.sgu.ru.
4 AFTE Journal--Volume 45 Number 1- winter 2013.

# TESTING OF FIRE EXTINGUISHERS – BETWEEN EUROPEAN AND NATIONAL REGULATIONS

**Aleksandar Mićović, PhD**[1]
**Stevan Jovičić, PhD**
**Nenko Brkljač, PhD**
Technical Test Centre, Belgrade

**Abstract:** Methods and procedures used to test portable and mobile fire extinguishers are defined by European standards EN 3 and EN 1866. The mentioned standards are in force in all EU member states, while in the Republic of Serbia the corresponding SRPS standards are applied, which are referred to by the order on mandatory attestation of fire extinguishers from as late as 1983.[2] The said standards were withdrawn from use in 2012, but they are still used as an integral part of the order on mandatory testing of fire extinguishers which is still in force. This has caused quite an unusual situation: the standards which are in force are not applied, and instead of them the standards which are officially withdrawn from use are actually applied in the process of fire extinguisher certification.[3]

The procedure of fire extinguisher testing defined by European Standards EN 3 and EN 1866 is essentially very similar to a series of the SRPS standards, but far more comprehensive and functionally more complex, requiring far longer period of testing and it is also several times more expensive than testing carried out in the Republic of Serbia. EN3 standard pays far more attention to certificates for materials applied in manufacturing of fire extinguishers as well as training of manufacturing personnel.[4],[5] Quality and reliability of pressure indicators as well as the quality of surface protection of fire extinguisher body are particularly taken care of. These quality requirements demand also better equipment in laboratories accredited to perform testing according to the European standards. There is still not a single laboratory in Serbia which has been accredited to perform testing according to EN3 standards.

**Key words:** test methods, fire extinguishers, EN 3, EN 1866, certification

## INTRODUCTION

In addition to domestic manufacturers there is a large number of importers and distributors of fire extinguishers manufactured in other countries present in the market of the Republic of Serbia. It should point out that it is necessary to conduct testing – control of conformity for each new batch from import, while domestic manufacturers are obliged as a part of regular supervision to submit to an accredited laboratory the extinguishers from their manufacture for control testing. It is clear that this is quite an extensive work and it can be concluded that state institutions, particularly the Ministry of Interior – Fire Department have their interest

1 amicovic1@gmail.com
2 Службени лист СФРЈ бр. 16/83, Наредба о обавезном атестирању ручних и превозних апарата за гашење пожара
3 SRPS Z.C2.022, *Ručni i prevozni aparati za gašenje požara, metode ispitivanja*
4 EN 1418 Welding personnel - Approval testing of welding operators for fusion welding and resistance weld setters for fully mechanised and automatic welding of metallic materials
5 EN 287-1 Qualification test of welders - Fusion welding - Part 1

in covering this field both through legislation and practical implementation of relevant regulations.

According to the legal provisions in force all residential and office buildings are obliged to be equipped with either fire hydrants or corresponding fire extinguishers. In case of sky scrapers a fire extinguisher should be placed at every second floor. On the other hand, according to the surveys of 2010 and 2013 conducted by the Belgrade Housing Enterprise at the sample of 14,000 residential buildings almost 90% did not have the required fire-fighting installations. Only about 3,200 fire extinguishers are available in the staircase area. About 20,000 fire extinguishers are still needed.

It can be concluded from the above said that the institutions of the Republic of Serbia, which are in charge of fire protection, must urgently decide how to act in order to solve the current situation. The logical direction is to start certifying fire extinguishers according to the European standards, but the question is what should be done with thousands of fire extinguishers which are currently in use with previously obtained certificates and which do not meet the test requirements according to EN3 and EN 1866 standards. It should also mentioned that there is not a single laboratory for such testing accredited in Serbia.

## CERTIFICATION TESTS OF FIRE EXTINGUISHERS

Fire extinguisher testing defined by the European Standards EN3 and EN 1866 in terms of duration of testing are significantly longer and financially several times more expensive than those applied in the Republic of Serbia, which would create additional burden to domestic manufacturers.

As an illustrative example of what was previously stated, we shall use a description of the procedure of subjecting plastic components of fire extinguishers to artificial ageing test. The prescribed time interval of exposure is 500 hours (paragraphs 11.2.3 and 11.2.4 of EN3-3 standard), which converted into work days amounts to approximately one month of conditioning just for the parts made of plastic.

Certification tests of fire extinguishers according to the EN 3 standard imply testing of functional characteristics of fire extinguishers, which correspond to the requirements of the following standards:

- *EN 3-3 Portable fire extinguishers, Part 3 Construction, resistance to pressure, mechanical tests*;

- *EN 3-6 Provisions for the attestation of conformity of portable fire extinguishers in accordance with EN 3-1 to 3-5* (*the mentioned standards have been replaced with EN 3-7);*

- *EN 3-7 Characteristics, performance requirements and test methods;*

- *EN 3-8 Additional requirements to EN-7 for construction, resistance to pressure and mechanical tests for extinguishers with maximum allowable pressure equal to or lower than 30 bar*;

- *EN 3-9 Additional requirements to EN 3-7 for pressure resistance of $CO_2$ extinguishers*;

- *EN ISO 1866 Mobile fire extinguishers.*

Testing of fire extinguishers in accordance with EN 3 standards means also the introduction of many novelties in the testing procedure. Further in the text we shall present the most important differences in comparison with the currently valid scope of testing for extinguisher certification.

When applying for testing of certain characteristics or certification of a fire extinguisher, the entity requiring such testing is obliged to submit to an authorized certification body an application and the following accompanying design and technical documentation:

- Complete book with construction documentation which defines clearly and undoubtedly the construction of fire extinguisher;
- Complete list of extinguisher parts (components) with identification or catalogue numbers;
- Excerpt from the register of fire extinguishers;
- Certificate of harmlessness of extinguishing agent (safety data sheet);
- Technological report on thermal processing and technology of extinguisher manufacturing and welding procedure applied on extinguisher body;
- Certificates on materials used for extinguisher manufacturing;
- Attestations for built-in extinguisher parts, certified by an accredited body, and
- Reports with the results of internal tests.

If compared with the scope of technical documentation which is currently submitted when requesting certification, the EN 3 standards include new documents such as: excerpt from the register of manufacturers and technological report on thermal processing and welding procedure applied.[6]

Together with the design and technical documentation the entity applying for testing is obliged to submit a minimum number of fire extinguishers to be tested (the number of extinguishers submitted with the design and technical documentation is given in Table 1).

*Table 1. Number of extinguishers submitted for testing.*

| Type of extinguisher | Water based | Foam based | $CO_2$ | Halon | ABC powder | BC powder |
|---|---|---|---|---|---|---|
| Number of extinguishers | ≥ 19 | ≥ 21 | ≥ 16 | ≥ 16 | ≥ 19 | ≥ 17 |

The accredited institution based on testing results gives assessment on conformity of portable and mobile fire extinguishers with the requirements set out in the EN 3 and EN 1866 standards. It is necessary to mention that according to the Order on mandatory testing of portable and mobile fire extinguishers (paragraph 5) the number of samples for mandatory testing of a certain type is 3.

According to the requirement stated in paragraph 6.1 of EN 3-8 standard, the minimum allowable temperature range declared of the body must be -30 °C to +60 °C. Maximum value of operating pressure is measured at the temperature of +60 °C, 30 seconds after the activation of the cylinder (if it is a fire extinguisher with a cylinder), or immediately upon taking extinguisher from temperature conditioning at +60 °C. Unlike these requirements SRPS Z.C2.035 in paragraph 5.6 sets out that according to this standard extinguishers must be operational at temperatures ranging from -20 °C to +45 °C, which represents a milder criterion of temperature range for extinguisher functioning.[7]

Mechanical tests of cylinders in accordance with the requirements set out in paragraphs 6.3.2 and 6.3.3 of EN 3-8 standard should be performed at the ambient temperature of (20 ± 5)°C. The number of specimens tested is: 5 samples for burst test and 5 samples for mechanical strength test (crushing test). All test samples should be in their finished state, in other

6 *EN 1320 Destructive tests on welds in metallic materials - fracture test*
7 SRPS Z.C2.035, *Ručni i prevozni aparati za gašenje požara, ručni aparati za gašenje prahom*

words painted[8] and marked. The mechanical strength test shall be carried out at the sample of at least 5 extinguishers. This kind of testing shall be carried out in order to confirm quality of the extinguisher body. Tests are performed to check out strength or ductility under the impact of external load on extinguisher body. Testing is conducted with an empty tank. The standard prescribes two types of bodies – long and short bodies.[9]

**Testing extinguisher body (long bodies)**

If the subject extinguisher body length is greater than 1.5 x D, the extinguishers are considered long or extinguishers with long bodies, where D is external diameter of the body. In that case the body is put into the testing tools as shown in Figure 1. The body is crushed perpendicularly to the longitudinal axis of an extinguisher at approximately ½ of its length. The crushing tool should be made of the material that would not get deformed during the test. The tool should be shaped as a cylindrical mandrel which would perform kneading. Mandrel diameter is $D_B = (D \pm 20)$ mm, and the length should be sufficient to overlap the crushed body. The body shall be crushed to dimension corresponding to 10% of its external diameter within a period of 30 to 60 s (Figure 1).

For bodies with a longitudinal weld, the weld seam shall be at an angle of 90° to the support line. For bodies with a transverse weld, testing is carried out at an angle of 45° to the weld.

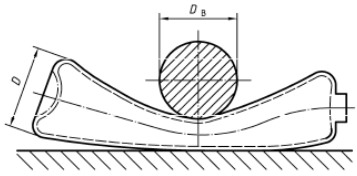



*Figure 1. Positioning of extinguishers with long bodies, L ³ 1.5 x D*

Following the crushing test, the body shall be subjected to the test pressure *PT*. The body shall not have any cracks or leaks, according to the requirements stated in paragraph 6.3.3.2 of EN 3-8 standard.[10]

**Testing extinguisher body (short bodies)**

If the tested extinguisher body length is less than 1.5 x D, the extinguishers are considered to be short or extinguishers with short bodies, where D is external body diameter. In this case the extinguisher is crushed by means of a tool presented in the following sketch.

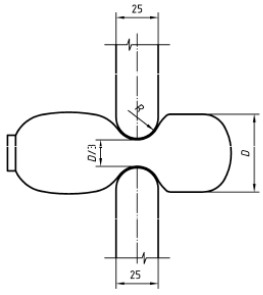



*Figure 2. Positioning of extinguishers with short bodies*

8 Farbregister RAL-841-GL
9 *EN 3-3 Portable fire extinguishers, Part 3 - Construction, resistance to pressure, mechanical tests*
10 *EN 3-8 Additional requirements to EN-7 for construction, resistance to pressure and mechanical tests for extinguishers with maximum allowable pressure equal to or lower than 30 bar*

The crushing tools is 25 mm thick. The tool radius should be R = 12.5 mm, and of sufficient length to extend beyond the sides of the crushed body (Figure 2). Crushing shall be made to the dimensions which correspond to 10% of external diameter of the body tested within a period of 30 to 60 s. For bodies with a longitudinal weld, the weld seam shall be at an angle of 90° to the tool. For bodies with a transverse weld, the testing is carried out at an angle of 45° to the weld. After the crushing test, the body is filled and subjected to cold water pressure up to the value of test pressure PT. There must not be any leakage during this type of testing according to the requirements stated in paragraph 6.3.3.3 of EN3-8 standard.

These tests represent a novelty and they are not set forth in the Order on mandatory attestation of portable and mobile fire extinguishers.

According to EN 3 standards temperature conditioning at $TS_{max}$ (maximum operational temperature) is carried out at three components of a fire extinguisher which are normally subject to pressure in operating condition for 500 hours. The samples are then conditioned in an atmosphere of 50% relative humidity and at an ambient temperature of (20 ± 3)°C until their weight stabilises. Then they are checked in detail to see if they comply with the data given in construction documentation. These tests also represent a novelty and are not set forth in the Order on mandatory attestation of portable and mobile fire extinguishers. The reference standard for this type of testing SRPS Z.C2.035 prescribes limit temperatures of -20°C to +45°C and includes just a functional trial run of the extinguisher at these temperatures. The conditioning of extinguishers in conditioning chambers is carried out within a time interval of 4 hours at an average, depending on the size of the extinguisher.

One of the greatest changes in testing of extinguishers refers to testing of fire extinguishing efficiency. Fire classes are defined in EN2 standard and Annex I to EN3-7 standard. Minimum sizes of test fires are defined in tables according to extinguishing medium with which the extinguishers are filled. The following tables contain sizes of test fires that certain type of extinguisher with a set quantity of extinguishing medium must extinguish.[11] The approach to testing differs from the SRPS standard which defines this field. The testing is completed when two test fires are extinguished, but within one size of test fire. There are no limits regarding the number of attempts at extinguishing. If only one of three attempts has been successful, it is allowed to go the first smaller test fire. If it is also extinguished, it is acknowledged that that extinguisher can extinguish this smaller size of test fire.

*Table 2. Minimum requirements regarding assessment of extinguishing efficiency of powder extinguishers.*

| Powder fire extinguisher | | |
|---|---|---|
| Test fire rating | Minimum duration of operation [s] | Nominal permitted charges[kg] |
| 5A | 6 | 1 |
| 8A | 6 | 1,2 |
| 13A | 9 | 1,2,3,4 |
| 21A | 9 | 1,2,3,4,6 |
| 27A | 9 | 1,2,3,4,6,9 |
| 34A | 12 | 1,2,3,4,6,9 |
| 43A | 15 | 1,2,3,4,6,9,12 |
| 55A | 15 | 1,2,3,4,6,9,12 |

11 *EN 3-7 Characteristics, performance requirements and test methods*

*Table 3. Minimum requirements regarding assessment of extinguishing efficiency of water-based and foam extinguishers*

| Water-based and foam fire extinguishers | | |
|---|---|---|
| Test fire rating | Minimum duration of operation[s] | Nominal permitted charges[l] |
| 5A | 6 | 2,3 |
| 8A | 9 | 2,3,6 |
| 13A | 9 | 2,3,6,9 |
| 21A | 9 | 2,3,6,9 |
| 27A | 12 | 2,3,6,9 |
| 34A | 15 | 2,3,6,9 |
| 43A | 15 | 2,3,6,9 |
| 55A | 15 | 2,3,6,9 |

*Table 4. Minimum requirements regarding assessment of extinguishing efficiency of CO2 extinguishers*

| CO2 fire extinguishers | | |
|---|---|---|
| Test fire rating | Minimum duration of operation[s] | Nominal permitted charges[kg] |
| 21B | 6 | 2 |
| 34B | 6 | 2 |
| 55B | 9 | 2,5 |
| 70B | 9 | 2,5 |
| 89B | 9 | 2,5 |
| 113B | 12 | 2,5 |
| 144B | 15 | 2,5 |
| 183B | 15 | 2,5 |
| 233B | 15 | 2,5 |

*Table 5. Minimum requirements regarding assessment of extinguishing efficiency of halon extinguishers*

| Halon extinguishers | | |
|---|---|---|
| Test fire rating | Minimum duration of operation[s] | Nominal permitted charge[kg] |
| 21B | 6 | 1 |
| 34B | 6 | 1,2 |
| 55B | 9 | 1,2,4 |
| 70B | 9 | 1,2,4,6 |
| 89B | 9 | 1,2,4,6 |
| 113B | 12 | 1,2,4,6 |
| 144B | 15 | 1,2,4,6 |
| 183B | 15 | 1,2,4,6 |

| | | |
|---|---|---|
| 233B | 15 | 1,2,4,6 |

Testing is carried out by an operator wearing a protective suit. The use of protective helmet, gloves and certified visor is allowed, which differs from the instructions in paragraph 3.2.3 of SRPS Z.C2.022,[12] which prescribes that an operator conducting a test must wear a civil or work suit and must not use any protective means (mask, goggles, gloves and similar). The EN 3 standard prescribes only that the person extinguishing test fire must not wear an aluminium-faced suit. Test fires must be prepared according to the requirements of the reference standard or these instructions. The requirements are set forth in Annex I, paragraph I. 1 of the EN3-7 standard.

The EN 3-7 standard defines the fire size which must be extinguished by a certain size of extinguisher, i.e. with nominal quantity of extinguishing charge. The smallest size of standard test fires that an extinguisher can efficiently extinguish is taken from the table. For instance, C6 extinguisher must extinguish class A fire, 8A size of fire and class B fire, 113 B in size. Testing if the extinguisher can extinguish even larger test fires is carried out by going to the next size of test fire. In this way the procedure is repeated until the extinguisher is efficient in extinguishing (two test fires of a series of three should be extinguished or two consecutive ones have been extinguished). Testing is carried out as agreed with the entity requiring the test or if it is satisfied with testing of only one size of test fire. In that case the extinguisher is marked with the label of only the test fire that it had extinguished. It is in the interest of the entity applying for testing to have the extinguishers tested for larger test fires, which would suggest the quality of extinguisher.

**Class A fires (test fires)**

Test fires for Class A fires are made of wooden sticks set as shown in the figure below. The sticks are supported on a metal frame 250 mm high, 900 mm wide and 500 mm long (Figures 3 and 4).

The moisture of sticks is determined according to ISO 4470 standard.[13] At least five stick samples are taken, (500 ± 10) mm long. The requirements are set out in Annex J to EN 3-7 standard.

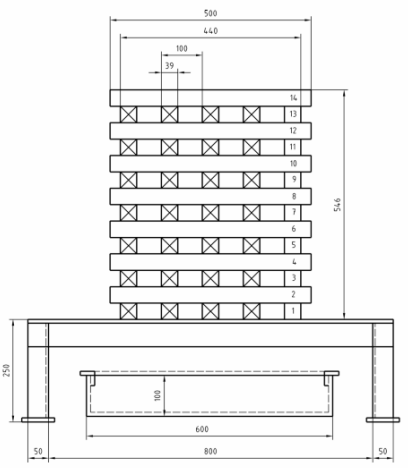



*Figure 3. Class A test fire, side view*

12 SRPS Z.C2.020, *Ručni i prevozni aparati za gašenje požara, opšte odredbe*
13 *ISO 4470, Sawn timber - Determination of average moisture content of a lot*

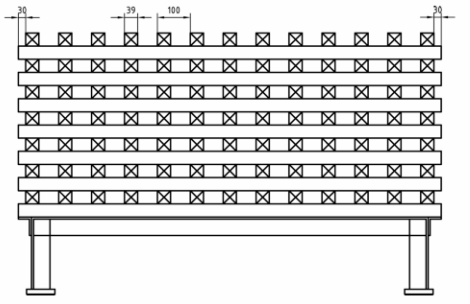



*Figure 4. Class A test fire, front view*

The sizes of class A test fires are given in Table 4.

*Table 4. Sizes of Class A test fires*

| Designation of test fire | Number of 500 mm wooden sticks in each transverse layer | Length of test fire in [m], longitudinal layers, 5 rows of sticks in a layer |
|---|---|---|
| 5A | 5 | 0,5 |
| 8A | 8 | 0,8 |
| 13A | 13 | 2,3 |
| 21A | 21 | 2,1 |
| 27A | 27 | 2,7 |
| 34A | 34 | 3,4 |
| 43A | 43 | 4,3 |
| 55A | 55 | 5,5 |

The test fire is constructed indoors in a test chamber sheltered from draughts. The test chamber must be minimum 8 m high. The area around the test fire must be free, and the test fire must be at a minimum distance of 3 m from the wall. The test fire can be made outside as well on condition that there is no wind during the test. The ambient temperature must be between 0 °C and 30 °C when the efficiency is tested for Class A fires. The measurement of air speed or airflow must be taken before the crib is ignited.

The lighting tray size should allow for the test fire to be completely covered by the source of flame burning from below the stacked sticks. The tray dimensions are 600 mm x 100 mm x L mm, where L is the dimension which varies depending on the size of test fire. The lighting tray is set symmetrically below the test fire. If larger test fires are ignited, it is allowed to use multiple lighting trays. The lighting tray is first filled with water to a depth of 30 mm, and then fuel (diesel fuel + petrol). The quantity of fuel should allow to create a flame that would burn for 2.5 minutes. The requirement is set out in Annex I paragraph I. 2.2 of EN 3-7 standard.

The test fire is approached by only one operator who will ignite the test fire. After the fire has burnt for 2 min, the tray shall be withdrawn from beneath the crib. The crib shall then be permitted to burn for further 6 min (stacked wooden sticks are in flame for 8 min). The operator shall then bring the extinguisher into use, and direct the jet onto the test fire. The entire contents of the extinguisher may be discharged either continuously or in successive bursts. The maximum extinguishing time shall not exceed 5 min for fires up to and including 21A and 7 min for fires of a greater size. After the extinguisher is fully discharged the fire shall be observed for 3 min from that point. For the test to be deemed successful, all flames

shall be extinguished and there shall be no recurrence of flames during the 3 min observation period. The extinguishing is deemed successful if the test fire is extinguished in two of three attempts or in two successive attempts. The requirement is set out in paragraph 6.4.2 of EN 3-7 standard.

**Class B fires**

Testing is performed in a range of welded sheet steel circular trays, the dimensions of which are given in Table 5. The minimum allowed height from the surface of the fuel to the rim of the tray shall be 100 mm for fires up and including 70B and 140 mm for fires of larger sizes. After each test, a minimum of 5 mm of fuel shall remain on the surface of the "water mirror". The tray should be placed on the surface of the ground or on a special support but in such a way as to prevent the flow of air under the tray. It is also not allowed for the tray to be dug into the ground which would enable sand or earth to get into the tray, i.e. into the fire which is extinguished during the test. The requirement is set out in paragraph I.3.1 of Annex I to EN3/7 standard.

*Table 5. Sizes of Class B test fires*

| Designation of test fire | Volume of liquid (1/3 water + 2/3 fuel) in l | Dimensions of a test fire (tray) | | | | |
|---|---|---|---|---|---|---|
| | | Internal diameter at rim in [mm] | Height in [mm] | Thickness of walls in [mm] | Area of fire in [$m^2$] | Duration of operation in [s] |
| 21B | 21 | 920±10 | 150±5 | 2,0 | 0,66 | 6 |
| 34B | 34 | 1170±10 | 150±5 | 2,5 | 1,07 | 6 |
| 55B | 55 | 1480±15 | 150±5 | 2,5 | 1,73 | 9 |
| 70B | 70 | 1670±15 | 150±5 | 2,5 | 2,20 | 9 |
| 89B | 89 | 1890±20 | 200±5 | 2,5 | 2,80 | 9 |
| 113B | 113 | 2130±20 | 200±5 | 2,5 | 3,55 | 12 |
| 144B | 144 | 2400±25 | 200±5 | 2,5 | 4,52 | 15 |
| 183B | 183 | 2710±25 | 200±5 | 2,5 | 5,75 | 15 |
| 233B | 233 | 3000±30 | 200±5 | 2,5 | 7,32 | 15 |

The fuel for the class B test fires shall be industrial heptane which shall have the following characteristics:

- distillation curve: 84°C to 105°C;
- difference between initial and final points of distillation: ≤ 10°C;
- aromatic content (*V*/*V*): ≤ 1 %;
- density at 15°C 0,680 to 0,720.

The test is carried out at the ambient temperature between 0°C and 30°C, while the wind speed shall not be greater than 3 m/s. The requirement is set out in paragraph I.3.2 of Annex I to EN 3-7 standard.

Yet another novelty of EN 3 standard in comparison with the test currently carried out provides for testing of pressure gauges in cycles. The accuracy of pressure gauge is tested at a temperature of (20 ± 5)°C, the pressure gauge being subjected to 1,000 pressure cycles from zero to P (Tmax) at an average rate of pressure change of (20 ± 5) bar/min.

The permitted errors in indication on pressure gauges are: 1 bar maximum at the low pressure end of the green zone; +/- 6% at the high pressure end of the green zone; the ($P$ + 20°C) point shall be indicated and the maximum permitted error is +/- 0.5 bar.

All tests shall be carried out at (20 ± 5)°C.

## CONCLUSION

From all the above said it can be concluded that the relevant institutions in the Republic of Serbia are presented a serious task to regulate the current state-of-affairs in the field of fire protection which refers to certification and testing of fire extinguishers.[14] Test laboratories that would like to get accreditation for the testing scope according to EN3 standards (i.e. SRPS standards in force), must be additionally well-equipped both materially, in terms of purchase of adequate equipment, and in terms of personnel, in order to be capable to carry out this type of testing. Domestic manufacturers of fire extinguishers must be prepared for the fact that certification process would become several times more expensive, which considering modest serial manufacturing puts them into unequal position with far richer manufacturers from Europe (Czech Republic, Greece, Poland, France, etc.) and especially from China, which would become dominant through the network of distributors and importers, but not the exclusive supplier in the market of the Republic of Serbia.

On the other hand, testing methodology and the manufacturing process of fire extinguishers have changed a lot in comparison with the time some 34 years earlier, when the Order on mandatory testing of fire extinguishers was written. Many manufacturers use aluminium as the basic material for production of bodies and all marks on such bodies are made with laser print on the bottom of the body. According to the current regulations these extinguishers do not comply with the requirement of SRPS.Z.C2.020, according to which the factory number and year of manufacture must be impressed into the body material, which in this case is a nonsense. In addition to this, manufacturing becomes increasingly cheaper and use of cheap plastic materials creates preconditions for the operating life of extinguishers to become shorter so that the new ones will have to be bought more often. Contemporary trends do not anticipate the production of extinguishers that would last 35 years or more, as was the case with the extinguishers manufactured at the time of SFR Yugoslavia, in other words when the series of JUS.Z.C2.02 standards were adopted, and which are still present as operational in our environment (offices, services, etc.).

## REFERENCES

1. EN 1320 *Destructive tests on welds in metallic materials - fracture test*
2. EN 1418 *Welding personnel - Approval testing of welding operators for fusion welding and resistance weld setters for fully mechanised and automatic welding of metallic materials*
3. EN 287-1 *Qualification test of welders-Fusion welding-Part 1*
4. EN 3-3 *Portable fire extinguishers, Part 3 Construction, resistance to pressure, mechanical tests*
5. EN 3-7 *Characterises, performance requirements and test methods*
6. EN 3-8 *Additional requirements to EN-7 for construction, resistance to pressure and mechanical tests for extinguishers with maximum allowable pressure equal to or lower than 30 bar*

14 „Službeni glasnik RS“ 74/2009 *Pravilnik o tehničkim i drugim zahtevima za ručne i prevozne aparate za gašenje požara*

7. Farbregister RAL-841-GL
8. ISO 4470*, Sawn timber-Determination of average moisture content of a lot,*
9. „Службени лист СФРЈ“ 16/83, *Наредба о обавезном атестирању ручних и превозних апарата за гашење пожара*
10. „Службени гласник РС“ 74/2009 *Правилник о техничким и другим захтевима за ручне и превозне апарате за гашење пожара*
11. SRPS Z.C2.020, *Ručni i prevozni aparati za gašenje požara, opšte odredbe*
12. SRPS Z.C2.022, *Ručni i prevozni aparati za gašenje požara, metode ispitivanja*
13. SRPS Z.C2.035, *Ručni i prevozni aparati za gašenje požara, ručni aparati za gašenje prahom*

# FORENSIC COURSE DEVELOPMENT. NEW DIRECTIONS IN FORENSIC EDUCATION

**Biljana Koturević**
Academy of Criminalistic and Police Studies
**Ana Branković**
Academy of Criminalistic and Police Studies

**Abstract:** Forensic experts are engaged in the field of fundamental, as well as applied sciences, in order to, by using objective application of scientific knowledge, methods and techniques in the examination of certain clues, substantiate the existence of crime and draw certain conclusions. The role of forensic engineers, according to AAFS, is to resolve criminal or civil regulatory issues using scientific/engineering techniques. Forensic engineer also investigates accidents, defects of industry products, environment contamination, buildings and bridges collapses, cars, plane and train accidents, blasts, etc. Due to the existence of a clear need for education and training of new generations of forensic engineers, the Academy of Criminalistic and Police Studies accredited new studies program named Forensic Engineering. This paper will present the curriculum of forensic engineering bachelor studies, the objectives, tasks, features of courses, opportunities for further education and employment. Also, it will point out possible modifications of curriculum in order to meet the needs of the Ministry of Interior of the Republic of Serbia. The changes would be primarily related to the harmonization of the curriculum with the new Police Act, which stipulates that all police officers with special authorizations must have completed at least a basic level of police training. Additional changes refer to the increased share of praxis compared to the classical forms of teaching, as well as the intensification of cooperation with other potential employers of Forensic engineering graduates.

**Keywords**: forensic science, education, curriculum modifications.

## INTRODUCTION

At the beginning of the 20th century, Archibald Reiss, seeking the establishment of a Forensics Institute within the University of 1909, addressed the Vice-Chancellor of the University of Lausanne, Switzerland with the following words: "Forensic methods attract a growing interest from professional circles. Many young people focus on this career from the start of their study. It becomes absolutely necessary for them to obtain a specialized grade at the end of their specialized study." (Rodolphe Archibald Reiss, 1909)[1]. Today, more than a hundred years later, forensic science has found its place in solving crimes, but educating forensic scientists is still a very difficult task.

Literature contains a large number of definitions of forensics, but what is actually forensics – a discipline, science or profession? One comprehensive and consistent definition of forensics that can be applied is: Forensics is any science that is used for the purpose of justice. ("Any science used for the purposes of the law is forensic science.")[2]. Inman and Rudin, 2001,

1 Jose R. Almirall , Kenneth G. Furton (2003). Trends in forensic science education: expansion and increased accountability. *Anal Bioanal Chem*, 376, pp. 1156–1159.
2 Merriam Webster Dictionary, www.merriam-webster.com.

explained that the role of forensics is to associate relevant legal issues with science.[3] Both forensic definitions are accepted by the world's largest forensic organization, the American Academy of Forensic Sciences.[4]

Already, it is clear that forensic science engages experts in the field of fundamental and applied sciences, in order to verify the existence of a criminal offense and to make certain conclusions by using the appropriate scientific knowledge, methods, and techniques by appropriate means.[5] In most countries, the examination of physical traces (evidence) that result from the offense is entrusted to forensics. It can be said that there is a division between forensic scientists, i.e. scientists of a certain scientific discipline (fundamental or applied), who are in charge of laboratory testing of traces, and police officers (criminal technicians) who are in charge of the crime scene investigation.[6] In addition to criminal technicians and forensic scientists, literature also recognizes the term criminal investigator, who is often equalized with a forensic scientist. But are terms criminalist and forensic scientist synonyms for the same profession? Namely, the role of criminalists, according to the literature data, is the analysis, comparison, identification and interpretation of physical evidence and the presentation of results in court. According to the above definitions, the difference is difficult to see. However, AAFS accepting the statement of the former president of this association Longhettie, that there is indefinite number of disciplines that by definition may be "forensic"[7], ranked criminology in discipline within forensic sciences.

Forensic disciplines include forensic anthropology, pathology, odontology, toxicology, psychiatry, entomology, forensic engineering, etc. The role of forensic engineers is, according to AAFS, solving of criminal or civil regulatory issues through the use of scientific/engineering techniques. The forensic engineer also investigates accidents, defective industries products, environment contamination, collapse of buildings, bridges, automobile, air and rail accidents, explosions, etc.

Based on all of the above, it can be concluded that there is a clear need for constant development of study programs aimed to educate and train the students for criminalistic police and security affairs. One of the new study programs developed at the Academy of Criminalistic and Police Studies is Forensic Engineering.

Therefore, in this paper, we will present a program of basic forensic engineering studies, through goals, tasks, forms of instruction, opportunities for further training and employment.

## THE STUDY PROGRAM OF UNDERGRADUATE ACADEMIC STUDIES FORENSIC ENGINEERING AT THE ACADEMY OF CRIMINALISTIC AND POLICE STUDIES

As a result of years of active discussion about needs of the Ministry of Internal Affairs, and comparison of existing similar study programs abroad, undergraduate academic studies of

3 Inman, K., & Rudin, N. (2002). *Principles and practice of criminalistics: the profession of forensic science*. Boca Raton, Florida CRC Press, pp 15–16.
4 "American Academy of Forensic Science" World of Forensic Science. Retrieved October 12, 2016 from Encyclopedia.com: http://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/american-academy-forensic-sciences.
5 Inman, K., & Rudin, N. (2002). *Principles and practice of criminalistics: the profession of forensic science*. Boca Raton, Florida CRC Press, pp 15-16.
6 Gaensslen, R.E. (2002). Forensic Science education and Educational Requirements for Forensic Scientist, *The NEACT journal,* 21(1), pp. 19–23.
7 Anthony Longhetti, Journal of Forensic Sciences, 1983;28:3–5.

Forensic Engineering were accredited in January 2014, by the Commission for Accreditation and Quality Assurance of the Republic of Serbia.[8]

The study program of undergraduate academic studies Forensic Engineering is conducted for a period of four years (240 ECTS – European Credit Transfer System). Upon completion of the studies, student obtains a higher education and a professional name of a graduated engineer of technology.[9]

The Forensic Engineering program includes a wide range of scientific disciplines in the field of technical and technological sciences and it is designed to enable students for the application of scientific methods of materials characterization in technological processes, forensic science and criminalistics during four-year basic academic studies.

In order to achieve this goal, contemporary theoretical and practical teaching takes place in adequately equipped teaching rooms of the Academy of Criminalistic and Police Studies, the National Criminalistic and Technical Center of the Ministry of Internal Affairs of the Republic of Serbia, the Institute of Physics in Belgrade and other institutes.

The ability to access the state-of-the-art equipment for identification of persons and materials, as well as all relevant information databases, enables students to get involved in all production processes and get acquainted with the work of all types of criminalistic police, security structures, etc. The commercial sector also has a special interest in this type of knowledge and skills.

The study program of undergraduate academic studies, initiated and approved by the Ministry of Interior, enables education of personnel in the field of technical and technological engineering, which will meet the needs of the Ministry of Interior in the field of detecting, clarifying, collecting and securing evidence of criminal offenses.[10]

The structure of the study program Forensic Engineering includes compulsory and elective subjects, whose mastering provides the necessary knowledge and skills. A student acquires a diploma of undergraduate academic studies from the educational and scientific field of technical and technological sciences. In the school year, a total of 60 ECTS corresponds to 40 hours per week engagement. The total student engagement consists of active teaching (lectures, exercises, practical work, seminars), independent work, colloquium, exams and other forms of engagement.

*Table 1. Organization of compulsory and elective subjects during 1st year of studies*[11]

| 1st year | | |
|---|---|---|
| No. | Subject | ECTS |
| 1 | An Introduction to Chemistry | 8 |
| 2 | Mathematics | 9 |
| 3 | Physics | 9 |
| 4 | English Language – Basic Course | 5 |
| 5 | Biology | 9 |
| 6 | Basis of Electro Engineering | 8 |

8 http://www.kpa.edu.rs/cms/data/akademija/akreditacija/sp/oas4-forenzicko%20inzenjerstvo.pdf.
9 Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. p. 4.
10 Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. p. 5.
11 Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. pp. 10–13.

| | | |
|---|---|---|
| 7 | Introduction to Forensics | 5 |
| 8 | English Language – Special Course | 5 |
| 9 | Practical Work | 2 |

*Table 2. Organization of compulsory and elective subjects during 2nd year of studies*[12]

| 2nd year | | |
|---|---|---|
| No. | Subject | ECTS |
| 1 | Physical Chemistry | 9 |
| 2 | Biophysics | 5 |
| 3 | Organic and Inorganic Chemistry | 9 |
| 4 | Probability and Statistics | 5 |
| 5 | Chemical and Technological Engineering | 8 |
| 6 | Engineering Management | 5 |
| 7 | Medicine and Medical Engineering | 8 |
| 8 | Biometric Technologies and Identifications | 9 |
| 9 | Practical Work | 2 |

*Table 3. Organization of compulsory and elective subjects during 3rd year of studies*[13]

| 3rd year | | |
|---|---|---|
| No. | Subject | ECTS |
| 1 | Optical and Spectroscopic Devices | 7 |
| 2 | Engineering of Explosives and Explosive Devices | 7 |
| 3 | Elective Subject 1 | 7 |
| | Microscopy | |
| | Environmental Protection | |
| 4 | Elective Subject 2 | 7 |
| | Technical-Technological Characterization of Materials | |
| | Application of Mass Spectroscopy for Material Identification | |
| 5 | Genetics and Genetic Engineering | 7 |
| 6 | Occupational Safety Engineering | 7 |
| 7 | Elective Subject 3 | 7 |
| | Sociology of Labor | |
| | Technological Testing of Tools | |
| 8 | Elective Subject 4 | 7 |
| | Chemical and Biological Weapons | |

12 Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. pp. 10–13.
13 Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. pp. 10–13.

| | | | |
|---|---|---|---|
| | | Risk Theory | |
| 9 | | Practical Work | 4 |

*Table 4. Organization of compulsory and elective subjects during 4th year of studies*[14]

| 4th year | | | |
|---|---|---|---|
| No. | | Subject | ECTS |
| 1 | | Traffic Engineering | 7 |
| 2 | | Geographic Software Engineering | 7 |
| 3 | | Elective Subject 1 | 7 |
| | | Ballistic Engineering | |
| | | Contemporary Antiballistic Materials | |
| 4 | | Elective Subject 2 | 7 |
| | | Digital Forensics | 7 |
| | | Engineering of Polymeric Materials | |
| 5 | | Ecotoxicology | 7 |
| 6 | | Modern Methods in Technological Engineering | 7 |
| 7 | | Elective Subject 3 | 7 |
| | | Criminal and Criminal Procedural Law | |
| | | Human and Material Resources Management | |
| 8 | | Elective Subject 4 | 7 |
| | | Human Security | |
| | | Criminalistics | |
| 9 | | Practical Work | 4 |

Acquiring a work profile of a technology engineer enables the student to position his/her knowledge in jobs that are of interest for obtaining and perfecting products for the needs of the police by using technological processes. Also, by mastering the materials characterization methods, the student is given the opportunity to acquire the status of a police officer or forensic scientist in the Ministry of Interior. As police officer, they will their job legally and efficiently and enable the provision of valid evidence of criminal offenses, which will directly improve the efficiency of court proceedings against their perpetrators.

Competence of a graduated engineer of technology:

- research and experimental development in the technical-technological and natural sciences;
- the legally-regulated approach to the crime scene;
- assessment of information and relevant facts about the criminal offense;
- processing the crime scene, collecting and securing evidence;
- application of technology in the state sector for the production of biometric documents;

14 Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. pp. 10–13.

- identification at border crossings, access to facilities and information systems of state importance;
- assessment of damage due to the commission of the criminal offense;
- risk assessment, assessment of damage in insurance companies and banking systems, protection of digital data and systems;
- knowledge and use of forensic methods (methods of physics, chemistry, biology, medicine, etc.) in criminalistics;
- exchange of information and ideas with appropriate experts and institutions at home and abroad;
- marketing;
- managing different production processes;
- use of information technologies.[15]

This study program provides opportunities for continuing further training (master, specialist and doctoral studies at the Academy of Criminalistic and Police Studies and related faculties in the technical and technological field), as well as for monitoring scientific achievements in the field of forensics and technological sciences (laboratories of the National Criminal and Technical Center and institutes of related faculties in the country and abroad), all in the function of creating a quality scientific and educational profile.

Students who complete the Forensic Engineering program have the opportunity to work in other state bodies and organizations, as well as in non-state commercial entities, where they will apply the acquired knowledge and skills in the field of technological and forensic science, at workplaces requiring the identification of persons and different types of materials.[16]

## SUGGESTIONS FOR MODIFICATION OF THE FORENSIC ENGINEERING UNDERGRADUATE STUDY PROGRAM

Over the past years, through the discussions with students, colleagues from the Ministry of Interior, as well as other potential employers, we have gathered information, suggestions and criticism about the possibility of changes in order to improve the study program. As the re-accreditation time approached, we thought it was the right time to suggest possible modification.

According to Article 10 of the Law on Police, which was enforced on 5 February 2017, police officers in the status of authorized officials must have at least completed basic level police training.[17] We think that certificate of attendance of basic police training should be introduced as one of the obligations for obtaining a diploma. The training would be carried out by teachers from the Academy during the first two weeks of each semester. Part of the training could be conducted at the Ministry of Interior training center "Mitrovo polje", as a part of the existing field practice. Obtaining this certificate would enable graduates to become easily recruited in the Ministry of Interior.

During the previous period, it was noticed that students show habit to choose certain elective subjects, while neglecting others. We believe that the solution is the change of cur-

15 Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. p. 7.
16 Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. p. 5.
17 "Službeni glasnik RS", No. 6/2016 of 28/01/2016.

riculum of the less attractive subjects, so that students would recognize the ability to acquire knowledge that will enable them to become more competitive on the labour market. We also propose the extension of the list of elective subjects in such a way that students can be trained in a narrow professional field during the third and fourth year of study.

In order to successfully pursue studies and later perform the work of a forensic scientist, students must acquire knowledge from the Criminal and Criminal Procedural Law and Criminalistics. Our opinion is that these subjects should become mandatory and should be moved to earlier years of study.

The experience tells us that one course from Introduction to Forensics is insufficient for students to master all the knowledge and skills that they will need during their later work. Therefore, we suggest that the Forensics (as a subject under this or any other title) should be studied during all four years, and that the ratio of theoretical and practical work would be 1:3, respectively.

In conversation with students, we noticed that they lacked more practice. Cooperation agreements with potential employers could allow students to apply acquired knowledge in real terms. An additional advantage of these practices is that employers will get insight into both the knowledge and skills that students possess, as well as their character, so that, as future employees, they could choose those who would easily fit into their work environment.

As one of the forms of field practice, we suggest that students of the final year, instead of duty at the school police station, fulfill this obligation as members of crime scene investigation units.

## CONCLUSION

New technical and IT achievements enable the development of new forensic disciplines, as well as continuous improvement of methods and techniques used in existing ones. Education of forensic scientists is a process that does not end with the diploma acquisition, but it lasts throughout the entire working life. Therefore, it is necessary to set up a good foundation for basic knowledge that would enable a later upgrade. We believe that introducing basic police training, amending and supplementing the list of elective courses, extending the list of compulsory subjects and increasing the practice versus theoretical learning will help educate better student who will have greater possibility of employment and advancement.

## REFERENCES

1. "American Academy of Forensic Science" World of Forensic Science. Retrieved October 12, 2016 from Encyclopedia.com: http://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/american-academy-forensic-sciences.
2. Anthony Longhetti, Journal of Forensic Sciences, 1983;28:3–5.
3. Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. p. 4.
4. Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. p. 5.
5. Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. pp. 10–13.

6. Documentation for Accreditation of Study Program: Forensic Engineering, undergraduate studies, 2014. p. 7.
7. Gaensslen, R.E. (2002). Forensic Science education and Educational Requirements for Forensic Scientist, The NEACT journal, 21(1), pp. 19–23.
8. http://www.kpa.edu.rs/cms/data/akademija/akreditacija/sp/oas4-forenzicko%20inzenjerstvo.pdf.
9. Inman, K., & Rudin, N. (2002). Principles and practice of criminalistics: the profession of forensic science. Boca Raton, Florida CRC Press, pp 15–16.
10. Jose R. Almirall, Kenneth G. Furton (2003). Trends in forensic science education: expansion and increased accountability. Anal Bioanal Chem, 376, pp. 1156–1159.
11. Merriam Webster Dictionary, www.merriam-webster.com.
12. "Službeni glasnik RS", No. 6/2016 of 28/01/2016.

# RESEARCH ON HOW TO REMOVE BACKGROUND DISTURBANCE WITH SHORT-WAVE ULTRAVIOLET BASED ON FULL BAND CCD

**Feng Xu**,
associate professor Dr.
Department of Forensic Science & Technology, China Criminal Police University
xufeng_ccpc@hotmail.com

**Abstract:** UV camera is mainly used for shooting, display and extraction of visible contrast faint traces with traces of material and material with a background in the UV reflection absorption characteristics of different materials. It can clearly show the details of the feature traces with the traces in visible light contrast and weak background in UV light to form the brightness contrast large. Because of its appearance and enhance the fingerprint effect very prominent, it has attracted more and more attention to the Public Security Department of Criminal Technology. The shortcomings of traditional ultraviolet photographic film limit its application in actual combat, which is filming process complex, long exposure time, the results show slow and inconvenient treatment etc. With the development of science and technology, the full band CCD system is attracting more and more attention. In this paper, we research the full band CCD system and analyze the method of light distribution with short-wave ultraviolet when the latent fingerprints on color plastic packaging, color photos and density board. Through the analysis of the experimental results, we get the best shooting method and quantization condition for removing background disturbance with short-wave ultraviolet. It can provide a reference for the criminal science and technology departments to use the full band CCD for short wave ultraviolet photography.

**Keywords:** full band CCD; short-wave ultraviolet; potential fingerprint; background disturbance

## INTRODUCTION

UV camera is mainly used for shooting, display and extraction of visible contrast faint traces with traces of material and material with a background in the UV reflection absorption characteristics of different materials[1]. It can clearly show the details of the feature traces with the traces in visible light contrast and weak background in UV light to form the brightness contrast large[2]. The criminal technical departments of public security pay more and more attention to it because of the effect on appearance and enhancing the fingerprint is very obvious[3]. The application of traditional ultraviolet film photography is limited greatly due to its

1 Yongsheng Chen, Analysis of the difference of the latent fingerprints of different objects by short wave UV reflection photography, Shandong Industrial Technology.
2 Haibo Zhang, Short wave ultraviolet photographic technique show wet non osmotic potential fingerprints on the object, Forensic Science and Technology.
3 Tao Liu, Ming Yang, Daiqin Tao, Short wave UV reflection photography show difference analysis of aluminum plate sweat fingerprint effect, Forensic Science and Technology.

disadvantages such as complex shooting, long exposure time, slow performance, and inconvenient post-processing[4].

In recent years, the public security organs around the country have introduced the advanced full band CCD system with the continuous development of science and technology[5]. It effectively solves the problems of the traditional ultraviolet film photography and becomes the development direction of the UV photography[6]. But the full band CCD system is a new scientific and technological achievement, it still has many problems in practice such as fingerprint type, trace carrier and lighting angle[7]. Therefore, it is very important to provide a practical reference scheme for the full band CCD system. In this paper, we use the full band CCD system to carry out short wave ultraviolet photography, summarize the best shooting methods and the experimental conditions for the elimination of the background interference in the color plastic packaging, color photos and density board based on the analysis of experimental results. This paper can provide reference for the criminal science and Technology Department to use the full band CCD for short wave ultraviolet photography.

## EXPERIMENT

1. Experimental instrument

Full band CCD of Andor Company, Nikon NK105/2.8 UV Lens, 254nm filter, 254nm3W ultraviolet lamp.

2. Experimental methods

Color plastic bags, color photos and density board are commonly used, which are the mark object of the crime scene fingerprints. It is difficult to show the fingerprints clear with various visible light shooting method because of the complex background interference and irregular surface reflection spot. We use the sweat fingerprints, oil fingerprint and blood fingerprint on the color plastic packing bag, color photograph and density board as samples, the short wave ultraviolet of full band CCD was used to shoot photo in this paper. The sample fingerprints were printed on clean plastic bags, color photos and density board, the scale was affixed to the bottom of the fingerprint.

We open Andor CCD computer control software (Andor MCD) and set the operating temperature to -5°C. When the CCD system to achieve the required temperature, we select shutter control to fully automatic, exposure time is set to 1 second, aperture is set to 5.6, 254nm filter of short wave ultraviolet is in front of the lens. We click the capture button to preview the image and capture the current image after placing the inspection material and turning on the UV lamp. In the file menu, we can select the output as the standard image, the image format as '.Jpg' and save the picture. Finally, the results of the comprehensive statistics and evaluation and record the shooting conditions.

## EXPERIMENTAL RESULTS

4 Ming Yang, Tao Liu, Cigarette packaging plastic film surface development of latent fingerprint ultraviolet reflection method, Forensic Science and Technology.
5 Lei Cheng Yuzhu Yang, ZhengXu, Ping Hu, Short wave UV reflection photography developing latent fingerprints on the object surface, Journal of Liaoning Police Academy.
6 Kang Shuai, Yuzhu Yang, Short wave UV reflection photography show garbage bag surface latent blood fingerprints, Journal of Chinese People's Public Security University(Science and Technology).
7 CHEN Shuang, TANG Zhen-an LI Tong, Design of dual Beam multi-wavelength UV-visible absorbance detectors based on CCD, Optoelectronics Letters.

**1.Extraction results of sweat fingerprint**

The sweat fingerprint results of eliminating background interference are shown in figure 1-figure 6, which are from the color plastic bag, color photo and density board. Sweat and other substances can emit long wave ultraviolet light in the ultraviolet irradiation, but the light is weak. With the increasing of irradiation time, the amount of sweat material luminescence will show a certain degree of attenuation. Full band CCD has high sensitivity, it can record in the faint light. It can clearly show and record the fingerprint in a very short period of time by reducing the exposure time.


*Fig. 1 sweat fingerprint original on color plastic*

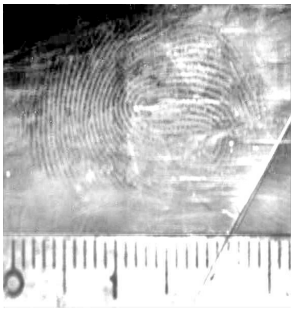


*Fig. 2 elimination result of sweat fingerprint on Color plastic*

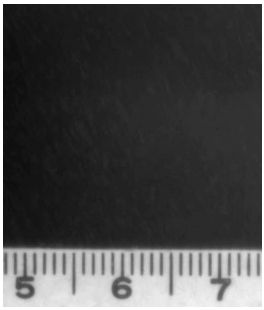


*Fig.3 sweat fingerprint Original on density board*

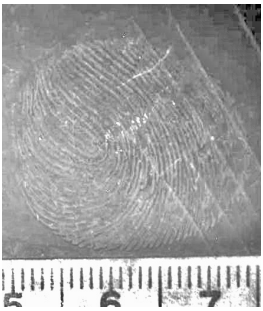


*Fig.4 elimination result of sweat fingerprint on density board*

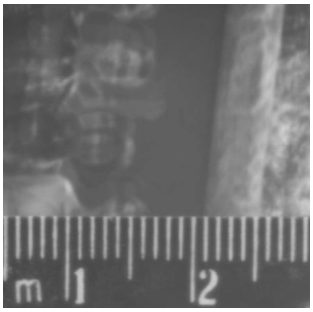


*Fig. 5 sweat fingerprint Original on color photo*

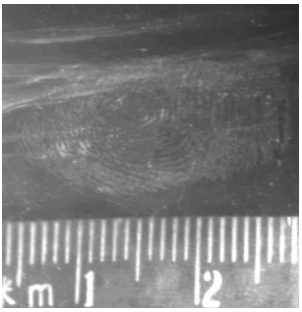


*Fig. 6 elimination result of sweat fingerprint on color photo*

The surface reflected light has a certain vertical reflected light component because of the low surface gloss through the full band CCD. Sweat fingerprint material has a maximum

absorption peak at 276nm shortwave ultraviolet light. The sweat fingerprint has strong absorption of 254nm ultraviolet, which eventually led to the deep tone fingerprint in light background. There is no internal reflection light in the UV reflection photography because of the strong absorption of 254nm short wave ultraviolet light by color plastic, color photograph and density board. The complex color background is eliminated due to the intensity of the reflected light and the hue region transformation non-existent.

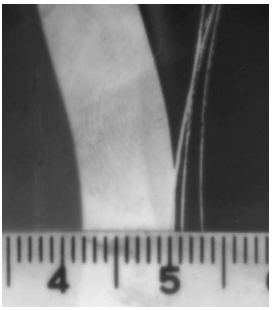


*Fig. 7 blood fingerprint original on color plastic*

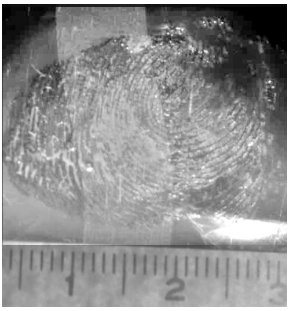


*Fig. 8 elimination result of blood fingerprint on Color plastic*

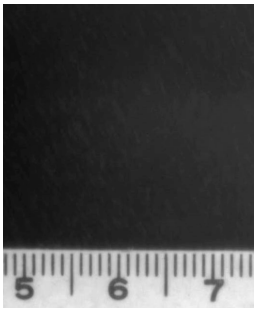


*Fig.9 blood fingerprint original on density board*

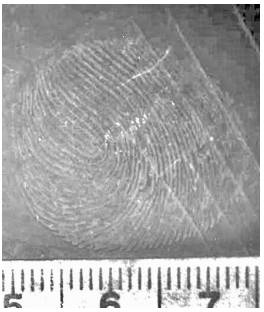


*Fig.10 elimination result of blood fingerprint on density board*

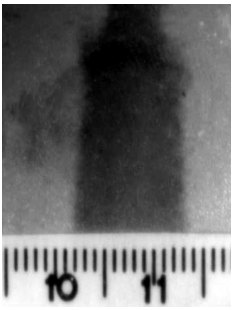


*Fig. 11 blood fingerprint original on color photo*

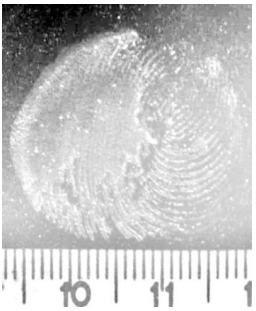


*Fig. 12 elimination result of blood fingerprint on color photo*

**2. Extraction results of blood fingerprints**

The blood fingerprint results of eliminating background interference are shown in figure 7-figure 12, which are from the color plastic bag, color photo and density board. The contrast of blood fingerprint and the background is very weak due to the interference of complex

background. We can shoot in 254nm UV lighting using full band shortwave CCD system, dark background of color plastic bags, color photos and density board is a strong absorption in the short wave ultraviolet. Blood fingerprint contains serum, plasma, hemoglobin and other substances, which can reflect the UV, it can eliminate the background interference and have high identification value because of the large brightness difference between the background and the fingerprint. It can make the feature details of blurry blood fingerprint under visible light became clear, because the full band CCD has the high resolution and sensitivity and can effectively adjust the brightness of the region.

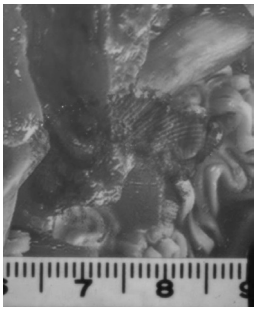


*Fig. 13 oil fingerprint original on color plastic*

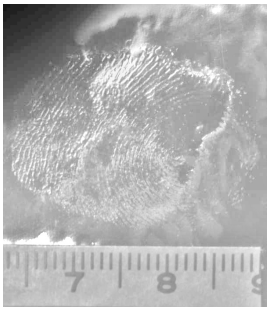


*Fig. 14 elimination result of oil fingerprint on Color plastic*

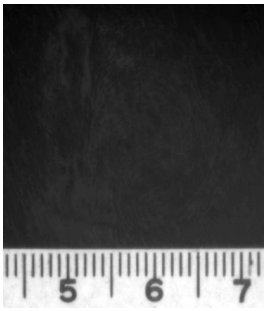


*Fig. 15 oil fingerprint original on density board*

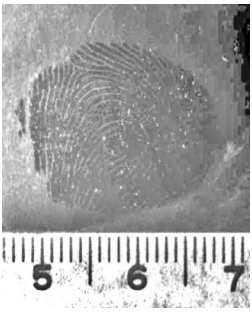


*Fig. 16 elimination result of oil fingerprint on density board*

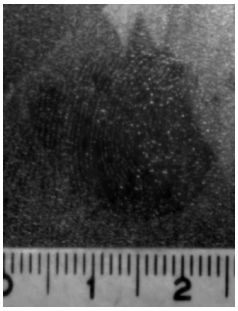


*Fig. 17 oil fingerprint original on color photo*

*Fig. 18 elimination result of oil fingerprint on color photo*

### 3. Shadow detection and elimination

The oil fingerprint results of eliminating background interference are shown in figure 13-figure 18, which are from the color plastic bag, color photo and density board. It can strengthen the contrast of fingerprint and background and eliminate background pattern with the full band CCD. When using the ordinary camera, the grease reflecting light of oil fingerprint is strong. It makes the fingerprint too bright and the whole fingerprint region fuzzy. The full band CCD can adjust the high brightness region and the interference of fingerprints and background. It can make the screen tonal balance, moderate brightness, details of the features to be clearly distinguished.

## CONCLUSION

The experiment concluded as follows:

(1) The various types of fingerprints on the color plastic bag, color photo and density board can be clearly shown. Absorption property of fingerprint material for the reflection on UV determines good and bad effects. The vertical reflected light component of fingerprint in short wave ultraviolet is much larger than the vertical reflected light component of object surface. The contrast of fingerprint and background is large, so it can eliminate the background and have a good image quality. Eliminate background interference situation, mode and angle of light distribution is shown in Table 1.

(2) This method has very good shooting effect of eliminating background interference, which uses the full band CCD to shoot all kinds of fingerprints on color plastic packaging, color photo and density board. It is an optical method and belongs to nondestructive testing. It is a feasible method for the extraction of the nondestructive inspection because it can be reused for many times without causing damage to the material.

*Table.1 shooting effect of fingerprint for eliminating background interference*

| shooting object | eliminating background effect | light direction | light angle | shooting distance |
|---|---|---|---|---|
| sweat fingerprint | +++ | single direction light | 45° | 20cm |
| blood fingerprint | ++ | single direction light | 45° | 15cm |
| oil fingerprint | ++ | single direction light | 45° | 20cm |

In summary, this paper summarizes the extraction methods of all kinds of fingerprints on color plastic packaging, color photo and density board to eliminate background interference. It can quickly use the full band CCD to shoot the fingerprint on such objects.

## REFERENCES

1. Yongsheng Chen, Analysis of the difference of the latent fingerprints of different objects by short wave UV reflection photography, Shandong Industrial Technology, 2016(05), 189-193.

2. Haibo Zhang, Short wave ultraviolet photographic technique show wet non osmotic potential fingerprints on the object, Forensic Science and Technology, 2007(06), 23-26.

3. Tao Liu, Ming Yang, Daiqin Tao, Short wave UV reflection photography show difference analysis of aluminum plate sweat fingerprint effect, Forensic Science and Technology, 2014(3), 20-24.

4. Ming Yang, Tao Liu, Cigarette packaging plastic film surface development of latent fingerprint ultraviolet reflection method, Forensic Science and Technology, 2015(5), 21-25.

5. Lei Cheng Yuzhu Yang, ZhengXu, Ping Hu, Short wave UV reflection photography developing latent fingerprints on the object surface, Journal of Liaoning Police Academy, 2015(02), 121-124.

6. Kang Shuai, Yuzhu Yang, Short wave UV reflection photography show garbage bag surface latent blood fingerprints, Journal of Chinese People's Public Security University(Science and Technology), 2010(01), 33-36.

7. CHEN Shuang, TANG Zhen-an LI Tong, Design of dual Beam multi-wavelength UV-visible absorbance detectors based on CCD, Optoelectronics Letters, 2006, (5), 683-687.

Topic IX

# EFFECTS OF PHYSICAL ACTIVITY ON ANTHROPOLOGICAL STATUS IN SECURITY AGENCY PERSONNEL

# PERCENT OF BODY FAT STANDARDS FOR SERBIAN MALE POLICE OFFICERS[1]

**Milivoj Dopsaj, PhD**
*Faculty of Sport and Physical Education*, *University of Belgrade*
milivoj.dopsaj@gmail.com
**Marko Vuković**
*Faculty of Sport and Physical Education*, *University of Belgrade*

**Abstract**

**Introduction:** Police job is well known as a very dynamic, stressful, shift work scheduled, but in a same time for some departments it is full-time sedentary. However there may be professional situations that require physical endurance, strength and excellent physical fitness level, because of situations such as foot chases and arresting suspects. It is well known that excessive body fat could be indicator of basic health status, and can impede an officer's physical abilities to deal with professional efficiency. The aim of the research was to create percent of body fat standards applicable to the Serbian male police officers.

**Methods:** Body composition measuring was done by bioelectrical impedance method (BIA), using a professional instrument – In Body720 Tetrapolar 8-Point Tactile Electrode System (Biospace, Co., Ltd). All measurements were performed in the period September 2011 – September 2015. The sample of the respondents consisted of 884 male policemen from nine different departments (Age = 33.4±7.7 yrs., BH = 182.0±6.6 cm, BM = 90.1±13.3 kg, and BMI = 27.15±3.45 $kg \bullet m^{-2}$).

**Statistics:** Basic descriptive statistical parameters were calculated for all results (Mean, SD, cV%, Std. Error). After that, using analysis of variance – ANOVA the difference between examined variable in the function of groups was applied. The difference between individual variables was determined by Bonferroni test. The level of difference of measurements between individual variables was determined on the probability level of 95%, that is, p value of 0.05. Software SPSS Statistics 17.0 was used for all statistical analyses.

**Results:** The results showed the following descriptive statistics of the percent of body fat: PBF = 19.55±6.58%, cv%=33.69, Min and Max = 2.96 to 44.83%. The general classification standards are: excellent body fat ≤ 9.68%, very good body fat = 9.68 to 16.25%, average body fat = 16.26 to 22.84%, very bad body fat = 22.85 to 29.42%, non-acceptable body fat ≥ 29.43%.

**Conclusion:** The results of prevalence distribution showed that generally 17.74% of the sample had excellent level of PBF, 52.43% had acceptable percent of body fat level, 15.37% subjects were pre-obese, while 14.46% of the sample were in obese category, which means that 29.85% of examined police officer sample have too much excess fat in the body, which certainly does not represent a professional standard for police officer body status.

**Keywords:** body structure, police, standards, body fat percent.

1 This research is part of the project Effects of applied Physical activity on locomotor, metabolic, psycho-social and educational status of the population of the Republic of Serbia, under number III47015, which is financed by Ministry of Education and Science of Republic of Serbia – Cycle of Projects 2011–2016.

# INTRODUCTION

Professional expectations in an interior affairs' job is that police officers experience unexpected physical challenges that require strength, endurance, basic and specific dexterity and skills, as well as good physical conditioning. Examples are subduing or foot chasing a suspect, climbing fences or stairs, or conducting critical life-saving activities as well as using a legal force defenses skills and weapons[2]. On the other hand, there is the situation where majority of work time involves sitting in patrol cars, writing reports, or interviewing persons[3]. Generally, police job is well known as a very dynamic, stressful, shift work scheduled, but in a same time for some departments full-time sedentary. All those usual professional situations could cause higher risk of stress for an officer, which could strongly lead to increased incidence of non-communicable diseases, especially to increased incidence of obesity[4,5].

It is well known that excessive body fat i.e. body fat percentage (BF%) is related to physical condition in previous studies and may be a better indicator than body mass index (BMI) of health status and police officer's physical abilities[6]. BMI is often used as criterion for body status and physical fitness level during police work entry assessments[7]. At the other side, it is well known that excessive body fat can be indicator of basic health status, and can impede an officer's physical abilities to deal with professional efficiency[8]. However, there are more and more scientific evidence that some individuals have high BMI scores due to heavy muscle content and others have BMI scores within the normal range and yet have a high BF%. Also, BF% has been reported to increase with years of police service[9].

Stressful work, based on unpredictable and stressful bursts of intense and strenuous physical activity in combination with prolonged sitting hours spent at work puts high demand on the entire physiological, physical and cardiovascular system of police professionals. This is the main health reason why it has been found that police officers have poorer health prognosis and more metabolic disorders then the general population[9,10]. According to the results recently published, a higher percentage of police officers in USA were obese (40.5% vs. 32.1%), had the metabolic syndrome (26.7% vs. 18.7%), and had higher mean serum total cholesterol levels (200.8 mg/dL vs. 193.2 mg/dL) than the compared employed populations. In addition to having higher levels of traditional CVD risk factors, USA police officers had higher levels of non-traditional CVD risk factors[8].

2 Gerber, M., Kellmann, M., Hartmann, T., & Pühse, U. (2010). Do exercise and fitness buffer against stress among Swiss police and emergency response service officers?. *Psychology of Sport and Exercise*, *11*(4), 286–294.

3 Violanti, J.M., Ma, C.C., Fekedulegn, D., Andrew, M.E., Gu, J.K., Hartley, T.A., Charles, L.E., Burchfiel, C.M. (2017). Associations between body fat percentage and fitness among police officers: A Statewide study. *Safety and Health at Work,* 8(1), 36–41.

4 Leischik, R., Foshag, P., Strauß, M., Littwitz, H., Garg, P., Dworrak, B., & Horlitz, M. (2015). Aerobic capacity, physical activity and metabolic risk factors in firefighters compared with police officers and sedentary clerks. *PloS one*, *10*(7), e0133113.

5 Violanti, J.M., Ma, C.C., Fekedulegn, D., Andrew, M.E., Gu, J.K., Hartley, T.A., Charles, L.E., Burchfiel, C.M. (2017). Associations between body fat percentage and fitness among police officers: A Statewide study. *Safety and Health at Work,* 8(1), 36–41.

6 Lagestad, P., & Van Den Tillaar, R. (2014). Longitudinal changes in the physical activity patterns of police officers. *International Journal of Police Science & Management*, *16*(1), 76–86.

7 Dopsaj, M., Vuković, M. (2015). Prevalence of the body mass index (BMI) among the members of the Ministry of Interior of the Republic of Serbia – pilot study. *Bezbednost*, *57*(3), 82–48.

8 Hartley, T. A., Burchfiel, C. M., Fekedulegn, D., Andrew, M. E., & Violanti, J. M. (2011). Health disparities in police officers: comparisons to the US general population. *International Journal of Emergency Mental Health*, *13*(4), 211–220.

9 Boyce, R.W., Jones, G.R., Lloyd, C.L., Boone, E.L. (2008). A longitudinal observation of police: body composition changes over 12 years with gender and race comparisons. *Journal of Exercise Physiology, 11*(6), 1–13.

Unfortunately, there are no valid published scientific studies that examine obesity among police officers working in Serbia. Because of that, the aim of the research was to create percent of body fat standards applicable to the Serbian male police officers.

# METHODS

## PARTICIPANTS

The sample of the subjects consisted of 884 male policemen randomly selected from nine different departments: border and traffic police, special anti-terrorist police units, SWAT police, gendarmerie, firefighters, criminal police investigators, communal police and the Academy for Criminalistics and Police Studies students (Age = 33.4±7.7 yrs., BH = 182.0±6.6 cm, BM = 90.1±13.3 kg, and BMI = 27.15±3.45 $kg \bullet m^{-2}$).

All examinees were informed about procedure and measuring conditions and voluntarily participated in this research. Complete process of measuring this sample was carried out during the period 2013–2015 in Methodological scientific research laboratory at the Faculty of Sport and Physical Education, University of Belgrade. The research was carried out in accordance with the conditions of the Declaration of Helsinki: Recommendations Guiding Physicians in Biomedical Research Involving Human Subjects[10], and with the approval and consent of the Ethics Committee of the Faculty of Sport and Physical Education, University of Belgrade.

## TESTING PROCEDURE

Testing procedure of measuring body constitution was carried out by usage of bioelectrical impedance analysis (BIA), precisely Inbody 720 Tetapolar 8 points by tactical electrodes system (Biospace Co, Ltd). Inbody 720 device (720 Inbody Biospace 2008) used the latest technology of measuring body structure by method DSMBIA (Direct Segmental Multifrequency Bioelectrical Impedance Analysis). This kind of equipment is intensively used in different occupational, sports health clinics and other health care improvement institutions.[11]

All participants were measured in accordance with manufacturer's suggestions. Week before the testing, participants were briefed about the rules and route of the test and they got following instructions:

- Measuring was taken in the morning between 8:00 and 10:00am,
- Participants were asked to abstain from large meal after 9pm,
- Participants were asked to abstain from eating and drinking prior to testing on the measuring day,
- Participants were asked to abstain from consuming any alcohol drinks for 48 hours before measuring,
- Participants were asked to urinate and defecate at least 30 minutes prior to measuring,

10 World Medical Association. (1992). World Medical Association Declaration of Helsinki: recommendations guiding physicians in biomedical research involving human subjects [Internet]. Somerset West, RSA: 48th World Medical Association General Assembly; 1996 Oct. [cited 2010 Jun 8]. *Nord Med*, *107*, 24–25.

11 Kukic, F., and Dopsaj, M. (2016). Structural analysis of body composition status in Abu Dhabi police personnel. NBP. Journal of Criminalistics and Law, 21(3), 19–38.

- Participants were in the standing position at least 10 minutes prior to measuring due to normal fluid distribution in the body,

- Measuring was taken in the standing position, in underwear, without any metal objects on, and with arms and hands placed 15 cm laterally aside from the body.

## STATISTICS

Basic descriptive and dispersion statistical parameters were calculated for all results (Mean, SD, cV%, Std. Error, Min and Max). After that, a standard metrological procedure for normative calculation was applied. Normality of distribution was calculated by using non-parametric Kolmogorov-Smirnov Z test. All statistical calculations were determined on the probability level of 95% and at p value of 0.05. Software SPSS Statistics 17.0 was used for all statistical analyses.

Seven class level scale, based on sports science metrology statistical principles[12] was used to evaluate the results by dividing them in 7 following classes (clusters): Superior body fat level, Excellent body fat level, Very good body fat level, Above average (very good) body fat level, Average body fat level, Under average (bad) body fat level, Very bad body fat level, and Non acceptable body fat level.

## RESULTS

The descriptive statistics data are shown in Table 1. The results showed the following descriptive statistics of the percent of body fat: PBF = 19.55±6.58%, cV% = 33.71, with relative value of standard measurement error at 1.13%, and with Min and Max from 2.96 to 44.83%. The general classification (Table 3) which could be used for initial Serbian national standards is : Superior body fat level ≤ 6.38%, Excellent body fat level = 6.39 to 12.96%, Above average (very good) body fat level = 12.97 to 16.25%, Average body fat level = 16.26 to 22.84%, Under average (bad) body fat level = 22.85 to 26.13%; Very bad body fat level = 26.14 to 32.71%, and Non acceptable body fat level ≥ 32.72%.

| | Mean | SD | cV% | Std. Err. (Aps.) | Std. Err. (Rel.) | Min | Max | Skew. | Kurt. |
|---|---|---|---|---|---|---|---|---|---|
| Age (yrs.) | 33.39 | 7.63 | 22.85 | 0.26 | 0.78 | 18.00 | 61.00 | 0.28 | -0.13 |
| BH (cm) | 182.00 | 6.64 | 3.65 | 0.22 | 0.12 | 162.70 | 206.80 | 0.22 | 0.35 |
| BM (kg) | 90.05 | 13.29 | 14.76 | 0.45 | 0.50 | 57.00 | 155.60 | 0.90 | 2.06 |
| BMI ($kg \bullet m^{-2}$) | 27.15 | 3.45 | 12.71 | 0.12 | 0.44 | 18.19 | 47.76 | 0.99 | 3.07 |
| PBF (%) | 19.55 | 6.59 | 33.71 | 0.22 | 1.13 | 2.96 | 44.83 | 0.22 | 0.08 |

*Table 2. Descriptive statistics of explored subgroups of sample (N = 884)*

12 Hartley, T. A., Burchfiel, C. M., Fekedulegn, D., Andrew, M. E., & Violanti, J. M. (2011). Health disparities in police officers: comparisons to the US general population. International Journal of Emergency Mental Health, 13(4), 211–220.

| | | N | Mean | SD | cV% | 95% Confidence Interval for Mean | | Min. | Max. |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Lower Bound | Upper Bound | | |
| KPA students | | 56 | 12.80 | 4.35 | 34.01 | 11.63 | 13.96 | 5.61 | 25.65 |
| Communal Police | | 250 | 18.62 | 6.09 | 32.74 | 17.86 | 19.38 | 4.32 | 35.30 |
| MUP | | 52 | 20.42 | 5.46 | 26.74 | 18.90 | 21.94 | 8.62 | 34.93 |
| SWAT | | 154 | 16.32 | 5.07 | 31.10 | 15.51 | 17.12 | 4.85 | 32.89 |
| 92 Police | | 32 | 22.05 | 6.34 | 28.76 | 19.77 | 24.34 | 8.12 | 33.49 |
| UZO Police | | 16 | 19.07 | 4.02 | 21.05 | 16.93 | 21.21 | 13.38 | 28.33 |
| Fire Dept Police | | 98 | 21.00 | 6.96 | 33.15 | 19.61 | 22.40 | 2.96 | 38.97 |
| Gendarmerie Police | | 99 | 22.85 | 6.99 | 30.61 | 21.45 | 24.24 | 6.48 | 44.83 |
| Brigade Police | | 127 | 23.64 | 5.29 | 22.35 | 22.72 | 24.57 | 10.06 | 40.20 |

*Table 3. General classification as an initial national percent of body fat standards for Serbian police*

| **Rank** | **Description** | **From (%)** | **To (%)** |
|---|---|---|---|
| 7 | Superior body fat level | J | |
| 6 | Excellent body fat level | 12.96 | 6.39 |
| 5 | Above average (very good) body fat level | 16.25 | 12.97 |
| 4 | Average body fat level | 22.84 | 16.26 |
| 3 | Under average (bad) body fat level | 26.13 | 22.85 |
| 2 | Very bad body fat level | 32.71 | 26.14 |
| 1 | Non acceptable body fat level | | 32.72 |

The results from the Figure 1 show us that KPA Students and SWAT members have significantly lower average level of PBF, while only two groups have under average lower PBF level (Communal police and UZO Police) than overall examined sample. The results of prevalence distribution showed that generally 17.74% of the sample had excellent level of PBF, 52.43% had acceptable percent of body fat level (PBF 3, 4, and 5 cluster), 15.37% of the subjects were pre-obese, while 14.46% of the sample were in obese category (Figure 2).

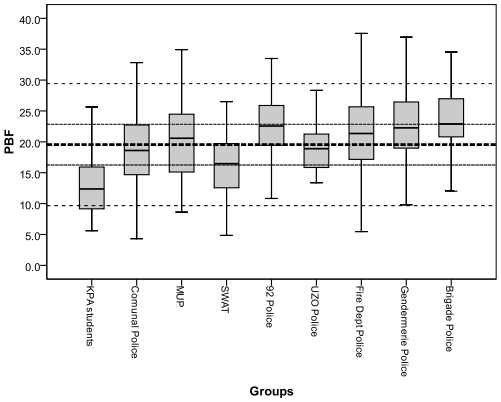



*Figure 1. Descriptive statistical results (Mean, 1 SD, a Min–Max range) for all subgroups with overall Mean, 1 SD and 2 SD reference value lines*

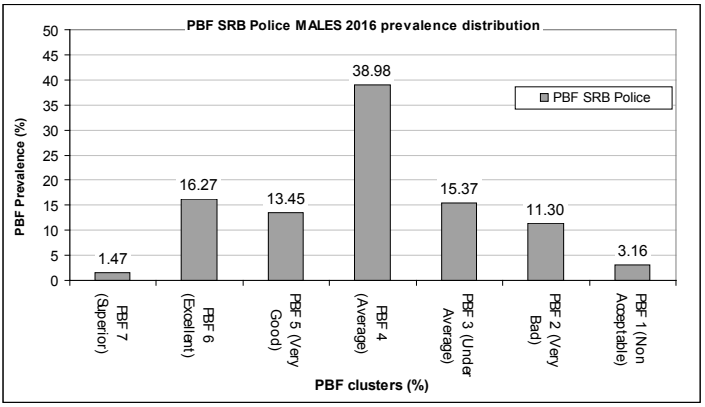



*Figure 2. Percentile distribution results (Mean, 1 SD, a Min–Max range) of PBF prevalence for Serbian police officers*

## DISCUSION

In the present study, the status of the body fat i.e. percent of body fat (PBF) for Serbian police officers was examined, with the aim of developing initial PBF standards.

Our results showed that average PBF level was 19.55±6.58%, with coefficient of variation at cV% = 33.71, and with a range between results at Min and Max from 2.96 to 44.83%. According to the subsample (Table 2) the lowest level was established at KPA students – 12.80±4.35%, with range of Min and Max values between 5.61 to 25.65%, while SWAT members at average level had a 16.32±5.07%, with the range between 4.84 to 32.89% of body fat.

Also, the results showed that the highest level of body fat was established at the Gendarmerie and the Brigade, at the level of 22.85±6.99% and 23.64±5.29%, in the absolute range from 6.48 to even 44.83% (Table 2).

In the previously published paper[13] it was established that average percent of body fat at Abu Dhabi police personnel was at level of 24.35±7.57%, which means they had by 4.8% higher percentage of body fat than the examined sample of policemen from Serbia, i.e. from this research.

Also, by processing the data from the ten most relevant researches published in the scientific literature that examined the body status of policemen from six different countries of the world (Slovenia, Brazil, USA, UAE, Germany, and Serbia), the authors of the given study concluded that on the general level the policemen in the average had belonged to the category of persons that, from the aspect of nutrition, are on the border of the first and the second level of pre-obesity, with average BMI value of 27.95±4.54 kg•m$^{-2}$, but also with the average value of body fat on the border of the clinical obesity PBF = 24.92±6.42%[14].

It could be concluded that those results showed us that the high prevalence of obesity among the police around the world could be a modern age professional phenomenon. Similar results for the level of obesity prevalence could probably be due to, at first, nature of shift scheduled police work, consequence of the bad eating habits, extremely low level of physical activity outside of work as well as other personal, cultural and social factors. Also, it seems that the prevalence of obesity among police employees is very high in different countries from different continents regardless of the economic development of the country. Many studies have shown that the prevalence of PBF is gradually rising by age of officers, and by each year spent in service[14,15].

According to the new ACSM classification the average PBF results as sample of this study should be classified in function of age as results placed between 50 to 55 percentiles i.e. as a fair result[16]. This fact should be accepted as a generally positive, but in the same time, the results of prevalence distribution showed that 15.37% subjects were pre-obese, while 14.46% of the sample were in obese category, which means that 29.85% of examined police officers sample have too much excess fat in the body, which certainly does not represent a professional standard for police officer body status. It could influence professional competency in a negative way, and it is strongly related to non-communicable diseases which could endanger the general health status[17,18].

## CONCLUSION

Generally, it could be concluded that the examined sample of 884 male police officers randomly selected from nine different departments (Age = 33.4±7.7 yrs., BH = 182.0±6.6 cm, BM = 90.1±13.3 kg, and BMI = 27.15±3.45 kg•m-2), has got normal average level of percent of body fat (PBF = 19.55±6.58%, cV% = 33.71, and with Min and Max from 2.96 to 44.83%).

13 Kukic, F., and Dopsaj, M. (2016). Structural analysis of body composition status in Abu Dhabi police personnel. NBP. Journal of Criminalistics and Law, 21(3), 19–38.
14 Boyce, R.W., Jones, G.R., Lloyd, C.L., Boone, E.L. (2008). A longitudinal observation of police: body composition changes over 12 years with gender and race comparisons. Journal of Exercise Physiology, 11(6), 1–13.
15 Dopsaj, M., Vuković, M. (2015). Prevalence of the body mass index (BMI) among the members of the Ministry of Interior of the Republic of Serbia – pilot study. Bezbednost, 57(3), 82–48.
16 American College of Sports Medicine (2016). ACSM's Guidelines for Exercise Testing and Prescription (Tenth Edition), USA: Wolters Kluwer.
17 Despres, J., Lamarche, B. (1993). Effects of diet and physical activity on adiposity and body fat distribution: implications for the prevention of cardiovascular disease. Nutrition Research Reviews, 6, 137–159.
18 Dugdill, L., Crone, D., & Murphy, R. (2009). Physical activity and health promotion: Evidence- based approaches to practice. Chichester, UK: Wiley-Blackwell.

Results should allow us to calculate normative system i.e. general PBF classification which could be used as initial Serbian national standard, as well as: Superior body fat level ≤ 6.38%, Excellent body fat level = 6.39 to 12.96%, Above average (very good) body fat level = 12.97 to 16.25%, Average body fat level = 16.26 to 22.84%, Under average (bad) body fat level = 22.85 to 26.13%; Very bad body fat level = 26.14 to 32.71%, and Non acceptable body fat level ≥ 32.72%.

The results of prevalence distribution showed that generally 17.74% of the sample had excellent level of PBF, 52.43% had acceptable percent of body fat level, 15.37% subjects were pre-obese, while 14.46% of the sample were in obese category.

According to the new ACSM classification the average PBF results of the sample of this study in function of age is classified as result placed from 50 to 55 percentiles i.e. as a fair result. This fact should be accepted as a generally positive, but in the same time, the results of prevalence distribution showed that 15.37% subjects were pre-obese, while 14.46% of the sample was in obese category, which means that 29.85% of examined police officer sample have too much excess fat in the body, which certainly does not represent a professional standard for police officer body status.

## REFERENCES

1. American College of Sports Medicine (2016). ACSM's Guidelines for Exercise Testing and Prescription (Tenth Edition), USA: Wolters Kluwer.
2. Boyce, R.W., Jones, G.R., Lloyd, C.L., Boone, E.L. (2008). A longitudinal observation of police: body composition changes over 12 years with gender and race comparisons. *Journal of Exercise Physiology, 11*(6), 1–13.
3. Despres, J., Lamarche, B. (1993). Effects of diet and physical activity on adiposity and body fat distribution: implications for the prevention of cardiovascular disease. *Nutrition Research Reviews*, 6, 137–159.
4. Dopsaj, M., Vuković, M. (2015). Prevalence of the body mass index (BMI) among the members of the Ministry of Interior of the Republic of Serbia – pilot study. *Bezbednost*, *57*(3), 82–48.
5. Dugdill, L., Crone, D., & Murphy, R. (2009). *Physical activity and health promotion: Evidence-based approaches to practice.* Chichester, UK: Wiley-Blackwell.
6. Gerber, M., Kellmann, M., Hartmann, T., & Pьhse, U. (2010). Do exercise and fitness buffer against stress among Swiss police and emergency response service officers?. *Psychology of Sport and Exercise*, *11*(4), 286–294.
7. Hartley, T. A., Burchfiel, C. M., Fekedulegn, D., Andrew, M. E., & Violanti, J. M. (2011). Health disparities in police officers: comparisons to the US general population. *International Journal of Emergency Mental Health*, *13*(4), 211–220.
8. Kukic, F., and Dopsaj, M. (2016). Structural analysis of body composition status in Abu Dhabi police personnel. *NBP. Journal of Criminalistics and Law, 21(3),* 19–38.
9. Lagestad, P., & Van Den Tillaar, R. (2014). Longitudinal changes in the physical activity patterns of police officers. *International Journal of Police Science & Management*, *16*(1), 76–86.
10. Leischik, R., Foshag, P., StrauЯ, M., Littwitz, H., Garg, P., Dworrak, B., & Horlitz, M. (2015). Aerobic capacity, physical activity and metabolic risk factors in firefighters compared with police officers and sedentary clerks. *PloS one*, *10*(7), e0133113.

11. Violanti, J.M., Ma, C.C., Fekedulegn, D., Andrew, M.E., Gu, J.K., Hartley, T.A., Charles, L.E., Burchfiel, C.M. (2017). Associations between body fat percentage and fitness among police officers: A Statewide study. *Safety and Health at Work,* 8(1), 36–41.
12. World Medical Association. (1992). World Medical Association Declaration of Helsinki: recommendations guiding physicians in biomedical research involving human subjects [Internet]. Somerset West, RSA: 48th World Medical Association General Assembly; 1996 Oct [cited 2010 Jun 8]. *Nord Med*, *107*, 24–25.
13. Zaciorski, V. M. (1982). Sportivnaja metrologija. *Moskva: Fizkultura i sport.*

# SPECIAL PHYSICAL EDUCATION AS A PART OF SPECIALIZED POLICE TRAININGS AT THE MINISTRY OF INTERIOR OF THE REPUBLIC OF SERBIA

**Bojan Mitrović, PhD**[1]
Department for Police Education and Training, Belgrade
Ministry of Interior of the Republic of Serbia
**Goran Vučković, PhD**[2]
Academy of Criminalistic and Police Studies, Belgrade

**Abstract:** Special physical education (SPE) represents an integral part of the professional training and development in the Ministry of Interior of the Republic of Serbia (MoI RS). Professional development is carried out in the organization of the MoI RS through the Professional Development Programme of Police Officers (continuous and additional training, expert gatherings, study visits, etc.), while professional training is conducted through the basis police traning, specialized police training and basic level police training (from employment). Specialized police training is aimed at training police officers to carry out more complex police work and tasks and it is implemented through courses in accordance with the established educational requirements within a certain line of work or a group of work areas in the MoI RS. SPE is a part of the scientific area of Physical education, i.e. Physical culture. The subsystem of SPE are basic motor skills (BMS), which represent the area which defines the basic physical abilities of people. BMS represents the basis for all other specific physical abilities from the aspect of more successful training and better qualifications of police officers in relation to the area of SPE. In the MoI RS, the SPE is implemented in segments with police officers through a certain number of specialized police trainings and courses according to signed programmes, which are presented in the Catalogue of Specialized Training Programmes of the Department for Police Education and Training. Some elements of SPE are contained in the following specialized police trainings: Course for Police Tasks Instructors, Training for Riot Patrols, Training for Non-Swimmers, Training for Water Rescuers (basic and advanced level), Course for Motor Boat Navigators and Operators, Specialized Training in Skiing (Skiing course, basic and higher level). It can be concluded that SPE has a very important role in professional development of police officers through specialized trainings and courses.

**Keywords:** SPE, BMS, police training, police work.

## INTRODUCTION

With the aim of successful performance of the tasks within the competence area of the Ministry of Interior of the Republic of Serbia (MoI RS), as well as for the purpose of conducting the police powers to execute work, the candidates for employment in the police service

1 Chief police inspector Bojan Mitrović, PhD, Head of Section for Specialized Training, Centre for Specialized Training and Professional Development in Belgrade, bojan.mitrovic@mup.gov.rs
2 Professor Goran Vučković, PhD, goran.vuckovic@kpa.edu.rs

are required to have certain psycho-physical properties and characteristics in order to be employed.[3] Candidates for employment in the MoI RS should firstly pass the process of basic competences and then the continuous process of development, with the purpose that tasks and duties ordered are being executed with the highest quality.

For the needs of police, the vocational training and improvement involves the acquisition, maintenance and improvement of knowledge, skills, attitudes and behaviours, in order to increase efficiency and effectiveness in performing the police duties. In the MoI RS, the training is organized by the Department for Police Education and Training (Human Resources Sector), while planning and implementation is done through professional trainings and development, in accordance with the educational need of organizational units of MoI RS (Article 131 of the Law on Police).[4]

Professional development of police officers of MoI RS is the integral part of their continuous development that affects the improvement of the quality of work. It has been executed through constant development and renewal of acquired police knowledges, skills and attitudes, or through the adoption of new legal arrangements, arising from the police practice and science with the purpose of lawful, efficient and safe performance of police duties.[5] Professional development is carried out as a part of MoI RS organization through the Professional Development Programme of Police Officers (2016), i.e. through continuous and additional training, expert gatherings (conferences, round tables, discussions, workshops) and study visits, as well as through developments outside of MoI RS, in cooperation or organized by other government agencies and organizations, or domestic and foreign entities (at the university level, in other ministries, non-governmental organizations, with foreign partners – e.g. OSCE, ICITAP, DCAF, Hanns Seidel Foundation, TAIEX, etc.) and the international cooperation. On the other hand, in accordance with the Article 2 of the Rulebook on professional training and development,[6] the professional development implies a process of continuous improvement of the existing knowledge and skills, or changes in attitudes and behaviour in order to have the most adequate and the most efficient method of performing tasks and activities within the scope of the MoI RS.

The pre-service training is essential for employees in order to pass professional trainings and acquire basic police skills and knowledge to be qualified to work in the MoI RS. Professional training, according to the Law on Police (2016), is realized through basic police training, basic police training from employment and specialized police trainings. The professional training in the MoI RS refers to the process of acquiring knowledge, gaining skills, building attitudes and behaviours necessary for safe and efficient execution of tasks and assignments.[7] Professional training is realized through courses, which are an intensive form of transmission of knowledge and acquiring of skills through processing one or more subject areas - modules in a relatively short time interval. The course contains a large number of lectures and exercises, and its duration and specificity were determined in the program of vocational training in accordance with the objectives and outcomes of the course.[8] The aim of the basic police training is to prepare participants for the lawful and efficient performance of duties and tasks of the uniformed police officer at the work place of a policeman. The aim of specialized police training is to train police officers for performing complex police tasks and activities, and it has

3 P. Dujković; S. Subotički; M. Klisarić, USE OF POLICE POWERS - Introduction into the police tactics (practicum), Belgrade, 2009, p. 8.
4 Official Gazette of the Republic of Serbia, No. 6/2016.
5 Professional Development Programme of Police Officers of the MoI RS, Belgrade, 2016.
6 Official Gazette of the Republic of Serbia, No. 80/2010.
7 *Ibidem*, Art. 2.
8 *Ibidem*, Art. 42.

been realized through courses, in accordance with established educational needs of specific lines of work or certain jobs in the MoI RS.[9]

In addition to mandatory knowledge and skills in the field of law and criminalistics sciences, the police officers are also obliged to acquire knowledge and skills in the field of military and police science, as well as certain areas of physical education. In the system of police training, the Physical culture as a science has an important place. According to Zivanović "physical culture is a human activity, which provides a tranformation of the personality from the real into possible as part of the general culture, through the knowledge of physical exercise and skills for physical exercises within their areas (physical education, sports and recreation)".[10] Physical culture contains aspects of both natural and social sciences, and it can be concluded that it is interdisciplinary, because it deals with a man as a unity of body and spirit.

Special Physical Education (SPE) is part of the scientific field of Physical Education in the system of Physical culture.[11] SPE has undergone tranformation in schools and higher education institutions, which educate staff for the needs of MOI RS, and those are the Police Secondary School (today the Basic Police Training Centre - BPTC in Sremska Kamenica), Police College and the Police Academy (today the basic vocational and academic studies at the Academy of Criminalistic and Police Studies - ACPS in Belgrade -Zemun).[12] It represents a highly specialized field that studies the principles of motor space, in other words those movements that are necessary in terms of the professional needs of the police.[13] The current security situation requires the police officers to have an adequate level of professional competences and mastery of all the knowledge and skills necessary for successfull performance of tasks, where the SPE plays an important role with the theoretical and practical knowledge and skills. Besides monitoring the physical characteristics and physical abilities of police officers, SPE deals with their general, directed and specific professional-working preparedness.[14]

According to Obradovic,[15] the personnel for admission to the MoI RS is educated in the two institutions, the ACPS in Zemun[16] and the BPTC in Sremska Kamenica.[17] At the ACPS, SPE is taught as specialized professional teaching subject, at the Department of Police Sciences, and one of the most important tasks of the SPE is the development of basic motor status, i.e. the basic motor skills (BMS).[18] Unlike the ACPS, in the BPTC, as the organizational unit of the Department of Police Education and Training (Human Resources Sector), at the basic police training, SPE is studied through an area of Defensive skills. Today, the SPE is taught at the basic vocational and academic studies at the ACPS.[19] Teaching of SPE at the ACPS, as opposed to the previous period (at the Police College and Police Academy) is represented

9 *Ibidem*, Art. 4. and 8.
10 N. Živanović, Attachment of epistemology of physical culture (2nd suppl. and revised edition), Niš, 2000, pp. 15-19.
11 M. Blagojević; G. Vučković; M. Dopsaj, *Specialized Physical Education I – basic level (reprint)*, Belgrade, 2012, p. 9.
12 G. Vučković; M. Dopsaj, Criminalistic and Police Studies students' attitudes regarding training in Special Physical Education, *Physical Culture*, No. 2/2011, Belgrade, pp. 33-41.
13 M. Blagojević; G. Vučković; M. Dopsaj, *Opus citatum*, p. 9.
14 *Ibidem*, p. 9.
15 S. Obradović, Planning, recruitment and selection of personnel in the Ministry of Internal Affairs of the Republic of Serbia, *Science-Security-Police*, 1/2011 (16), pp. 135-156.
16 Academy of Criminalistic and Police Studies (ACPS) was formed by the merger of two higher educational institutions Police Academy and Police College, both institutions were educated staff for the Ministry of Interior.
17 In 2007 are completed the transformation of the Police Secondary School in Sremska Kamenica in the Basic Police Training Center (BPTC).
18 R. Janković, Changes at repetitive strength of different muscle groups at academy of criminalistic and police studies students during first three years of studies, *Annual of the Faculty of Sport and Physical Education*, 2009, vol.16, pp. 111-124.
19 G. Vučković; M. Dopsaj, *Opus citatum*, pp. 33-41.

with inadequate teaching hours per week, if we take into account the modern tendencies that lately the graduates of academic and vocational studies of the ACPS are being employed at the workplace of the police officers (secondary education). There is a question of their adequate training and competence to apply police powers, or in this case an adequate qualification to use means of coercion.[20] The reduced number of classes of SPE initiated the lower values of the level of muscle strength and force, which adversely affects the application of the police powers, and more specifically the use of means of coercion i.e. physical strength.[21] For the purpose of necessity to upgrade the already acquired knowledge and skills, in the MoI RS the SPE and the elements of SPE are implemented as a segment with police officers through a certain number of specialized trainings and courses according to the programs which are prepared, signed and adopted in advance, as shown in the Catalog.[22]

The problem of this work is SPE and its representation in the specialized training of police officers in the MoI RS, for the purpose of safe and efficient performing of their jobs. The aim of this paper is to determine the substance of the elements of SPE in specialized police training being undertaken with police officers of the MoI RS.

## SPECIALIZED POLICE TRAINING IN MOI RS

The purpose of the specialized police training[23] is to enable police officers to effectively perform their regular and specific police duties, and to acquire new knowledge and skills during the courses according to pre-established educational needs of certain lines of work.[24] In 2007, the Center for Specialized Police Training and Professional Development (CSPTPD) was established. Before that, in 2003 as an organizational unit of the MoI RS responsible for integrated, planned and systematic organization and implementation of professional training and development of members of the Public Security Department of the MoI RS a Training Center was established, which preceded the CSPTPD. In 2004, the Training Center became the organizational unit of the then newly-formed Directorate for Police Education, Professional Development and Science, and then, on April 11, 2007, it was renamed to the Center for Specialized Police Training and Professional Development.[25] Previously, the specialized police trainings and courses were organized and implemented by the Police College of MoI RS.

Today, the CSPTPD is an organizational unit of the Department of Police Education and Training (Human Resources Sector of MoI RS), which is developing a strategy of specialized training and professional development of the police, as well as plans, organizes, monitors, coordinates and evaluates the work of its organizational, develops the labour standards which are essential for the establishment of maximum efficiency in carrying out their official duties. The CSPTPD in cooperation with other organizational units of the MoI RS, comprises training programs, organizes, implements and evaluates the specialized trainings and professional

20 B. J. Mitrović; R. Janković; M. Dopsaj; G.Vučković; S. Milojević; S. Pantelić; M. Nurkić; How an eight-month period without Specialized physical education classes affects the morphological characteristics and motor abilities of students of the Academy of Criminalistic and Police Studies, *Facta Universitatis - series: Physical Education and Sport*, 2/2016, pp. 167-178.
21 B. Mitrović; Efects of Specialized physical education on muscle strength and body composition, *PhD thesis*, Faculty of Sport and Physical Education, University of Niš, 2016.
22 Catalog of specialized police training programs of the MoI RS, 2014.
23 Law on Police, *Official Gazette of the RS*, No. 6/2016, Art. 131. and 133.
24 Rulebook on professional training and development, Official Gazette of the Republic of Serbia, No. 80/2010, Art. 4. and 8.
25 http://prezentacije.mup.gov.rs/upravazaobrazovanje/

development of police officers.[26] The Section of specialized police training is positioned within the CSPTPD, as the holder of activities related to planning, organizing and implementing the specialized police training and courses in the MoI RS. Within the CSPTPD, there are also the teaching centers "Avala" and "Makis" in Belgrade, "Mitrovo Polje" on Goc Mountain and "Kula" in Kula, where, in addition to the headquarters of the CSPTPD in the building of SIV 2 in New Belgrade and the ACPS in Zemun, the specialized trainings and courses are implemented in accordance with prepared and signed implementation plans.[27]

Specialized police trainings and courses are implemented separately for each line of work (Criminal Police, General Uniform Police, Traffic Police, Border Police, Special Units, Security Operations, Fire-Rescue Units, etc.). Also, there are specialized training and courses existing and implemented that are directly related to the problem of multiple lines of work in the MoI RS (course for controversial protection, course for motor boats navigators and operators, training in operating the off-road passenger vehicles, training for instructors of police skills – course for police work instructors, course for instructors in handling of firearms and shooting, and a course for instructors in tactics use of police powers, training for non-swimmers, training for water rescuers, specialized training in skiing, training for police negotiators, course for participation in peacekeeping missions of the United Nations, course for fighting against human trafficking, trainers development course, the course for the development of the training program, course for primary psychological prevention - peer support, course for designers and conductors of the classes for e-learning on Moodle platform, training for activities in detection and deactivation of illegal laboratories for production of psychoactive substances and precursors, etc.).[28]

## SPE AS A SEGMENT OF SPECIALIZED POLICE TRAINING IN MOI RS

Educational model of SPE involves the study of specific motor structures in accordance with the following stages or the entiteties: general, directed and situational-specific training, with an emphasis on the use means of coercion. General training phase predicts the basic movements, attitudes, tossing, punches, blocks, cleanings, levers, grips and moves. The phase of focused training provides variations and combinations of positions, movements, tossing, punches, blocks, cleaning, levers, grips and moves. The phase of situational training envisages solving the situational problems such as defense and counterattacks of unarmed and armed opponents, interception, providing passive and active resistance and bonding and bringing.[29] However, when the SPE is viewed from the aspect of police profession, we believe there is insufficient representation and situational training aimed primarily at the use of force, because this is a very important tool for the profession of a police officer.[30]

An important segment of SPE are the basic motor skills (BMS), which represent the area through which the basic physical abilities of human beings are defined. BMS are the basis for all other specific physical abilities in terms of successful training and qualification of police

26 Catalog of specialized police training programs, *Opus citatum.*
27 Law on Police, *Official Gazette of the RS*, No. 6/2016, Art. 133. paragraph 3.
28 Catalog of specialized police training programs, *Opus citatum.*
29 R. Mudrić, *Specialized physical education: handbook*, Belgrade, 2005, pp. 4. i 5.
30 D. Arlov, *Self-Defense Tools*, Novi Sad, 2002.

officers in relation to the area of SPE.[31] According to the group of authors,[32] motoric space is responsible for the implementation of the movement of a human, and is composed of the following five elements, defined as a basic physical ability:

- **the contractile ability of the muscles** (manifested as a maximum, the expulsive, instantaneous, repetitive, force or power, as well as the durability in power or strength),

- **energy mechanisms of the body** (manifested in the anaerobic-alactant, anaerobic-lactant and aerobic energy mechanisms),

- **speed of execution of individual movement and locomotion speed** (they are expressed as the latency time of the motor reaction, the speed of individual movement and the frequency of the movement),

- **the mobility of joints** - flexibility (is in function of the healthy preventive activity and a higher level of energy and the mechanical efficiency of movement),

- **agility** (expressed as the general and specific agility)

Other motor skills that are taught or were taught within the SPE course are: conditioning, swimming and skiing.[33] SPE is an important part of the training in the MoI RS. Through the elements of SPE in a number of specialized trainings the police officers acquire the necessary knowledge and skills, in order to be able to execute jobs and tasks from their job descriptions better and more professionally oriented. In particular, when it comes to the SPE as a segment of specialized training in the MoI RS, based on the Catalog of specialized trainings program, it can be concluded that the SPE elements are contained in the following specialized trainings and courses:

**Training for instructors of police skills – Course for police tasks instructors - (Formerly Course for operational police skills instructors - OPS)**

This course is intended for police officers who perform organization and implementation of teaching in the field of police tasks (formerly Operational Police Skills - OPV). The SPE elements are contained in 60 classess, which is 85.71% of the total number of classes, with the following teaching units:

- binding, inspection and bringing tools (parts of official handcuffs, procedures, techniques, processesses, etc.) - 12 classess;

- physical strength (definition of the terms physical strength and resistance, evaluation of the level of resistance, passive and active resistance, falling techniques, lever techniques, kick techniques, defense techniques of catching and encompassing, defense against cold weapons attacks, preventing the seizure of official gun, defense against weapons threatening at a reaching distance, establishment of full control over the person with active resistance - high aggression with bringing into the position for binding and binding with official cuffs) - 40 classes;

- police baton (parts of police baton, kick zones, basic usage policies, tactical positions with a baton, movement with a baton, kick techniques, blocks with a baton, release from stick capturing) - 8 classes.

**Training for riot patrols**

This training is intended for police officers who perform and carry out their tasks within general jurisdiction of riot patrols. A special requirement for referring to the mentioned

31 R. Janković; G. Vučković; M. Blagojević; Establishing the norms within the polygon for police officers' specific skill evaluation for students of the Academy of Criminalistics and Police Studies, *Security*, 2/2014, vol. 56, pp. 65-76.
32 M. Blagojević; G. Vučković; M. Dopsaj, *Opus citatum*, pp. 104. and 106.
33 G. Vučković; M. Dopsaj, *Opus citatum*, pp. 33-41.

training is that in accordance with the last physical examination checking (BMS) following the Program of professional training of police officers, they were rated in the range from 3.00 to 5.00. The SPE elements are contained in module Police tasks - OPS through 11 classes or 13.41% of the total number of classes, with the following teaching units:

- binding tools, inspection and bringing the persons - 2 classess;
- physical strength - 7 classess;
- police baton - 2 classess.

**Training for non-swimmers**

Training for non-swimmers is intended for qualifying the police officers of the MoI RS who perform the tasks of security at the rivers and lakes in their organizational units, the border control activities at border crossings for international river transport and border security on inland waterways, as well as for other police officers from the organizational unis for which the educational needs have been identified. The elements of SPE, or its important segment BMS, are contained in all 15 classess, or 100% of the total number of classes, with the following teaching units: water adaptation and the excercise classes of simple movements in the water; diving; mastering the elements of swimming technique; and jumps into the water.

**Training for water rescuers – basic level**

The basic level of the water rescuers training is intended to standardize knowledge, skills and attitudes in the field of lifesaving, as a base for efficient and effective work of police officers of the MoI RS performing duties in the field of water safety. Before the beginning of training, there is the elimination testing of candidates - the entrance exam. The elements of SPE, or its significant segment BMS are included in 28 classes, or 45.16% of the total number of classes, with the following teaching units:

- swimming training and conditioning - 14 classes;
- techniques of transporting the drowning person - 6 classes;
- rescue techniques - 8 classes.

**Training for water rescuers – advanced level**

The advanced level for water rescuers is intended for professional capacity building of teams of police officers of the MoI RS, as well as to standardize knowledge, skills and attitudes in the field of lifesaving, as a base for efficient and effective work. Before the beginning of training, there is the elimination testing of candidates – the entrance exam, and the police officers are required to have the basic level of training completed. The elements of SPE, or BMS are included in 72 classes, or 54.54% of the total number of classes, with the following teaching units:

- swimming training and conditioning - 30 classes;
- techniques of transporting the drowning person - 12 classes;
- rescue techniques - 30 classes.

**Course for motor boats of navigators and operators**

This course is intended for police officers performing the tasks in the field of river safety, and/or border control on border crossings for the international inland transport and security of state border on water, to enable acquisition of knowledge, standardizing of skills and attitudes required for successful navigation and operation of official motor vehicles and using the additional nautical devices and equipment in various situations, as well as the efficient use of positive regulations regarding control of safety of inland areas, as a base for efficient and effective work. One of the preconditions for being referred to the course is that the police officer has successfully completed the swimming test, as an element of BMS and/or SPE.

**Specialized training of skiing – skiing course, basic level**

Skiing course – basic level is intended for police officers of the MoI RS for acquisition of knowledge, skills and attitudes required for successful performance of tasks in the field of security of people and facilities, the tasks regarding safety at ski slopes and the use of additional equipment and devices in various situations, as well as the efficient use of positive regulations regarding control of safety of snow areas and winter resorts. The elements of SPE and/or BMS are included in all 60 classes, or 100% of the total number of classes, through the following teaching units: theoretical base of skiing, pre-exercises while standing in one place and while moving, straight downhill skiing, special step, snow plough, turning during plough, basic parallel turn, parallel slalom and technique of carving turn.

**Specialized training of skiing – skiing course, higher level**

Skiing course - higher level is intended for police officers of the MoI RS for acquisition of more specific and complex knowledge, skills and attitudes required for successful performance of tasks in the field of security of people and facilities, the tasks regarding safety at ski slopes and the use of additional equipment and devices in various situations, as well as the efficient use of positive regulations regarding control of safety of snow areas and winter resorts. The elements of SPE and/or BMS are included in all or 100% of the total number of classes, through the following teaching units, parallel slalom, basic carving technique, "fast slalom", turns on the unregulated terrain, techniques of changing directions in deep snow and field jump.

## CONCLUSION

SPE plays a very important role in professional competences of police officers, the first through schooling at the BPTC and the ACPS, then the beginning of their work at the MoI RS, and finally through the professional work, in the sense of use of the means of coercion, use of force and applying certain techniques of SPE primarily through preventive reactions and correct assessment and safe predicting of certain situations. That is why the role and importance of SPE in specialized police training at the MoI RS are even more significant. It is very important for police officers to have the opportunity to be constantly trained in the line of duty, and to upgrade the already acquired knowledge and skills, in this case through the elements of SPE, so that they could at least reach the minimum level of physical fitness to perform their duty in the interest of protection of public safety, and/or because of the significance of physical activity in terms of health.[34]

SPE is an important segment of basic police training as well (the field of Defensive Skills in the BPTC and basic police training from employment), as well as professional development of the police officers of the MoI RS (a part of the Professional development Programme of Police Officers in the MoI RS – Operational Police Skills (OPS) and Physical Training), but this will be the topic for some future research. It should also be mentioned that the revision of the curriculum of the Course of the Instructors of Police tasks is in its final stage, and the course will have a new name – Course for Trainers for Use of Police Powers.

In the end, it is important to mention that there is a tendency in the MoI RS to raise the capacity of police officers as much as possible, so that through their skills and knowledge, as well as their experience, they could contribute to the increased safety of the citizens of the Re-

34 J. Bonneau; J. Brown, Physical ability, fitness and police work. *Journal of Clinical Forensic Medicine*, 2/1995, pp. 157-164.

public of Serbia, particularly in the present fight against the increasing expansion of terrorism and extremism.[35]

## REFERENCES


1. Arlov, D; *Self-Defense Tools (Alati samoodbrane),* self-published by author, Verzal, Novi Sad, 2002.
2. Blagojević, M; Vučković, G; Dopsaj, M; *Special Physical Education I – basic level, reprint* (*Specijalno fizičko obrazovanje I - osnovni nivo, reprint*), Academy of Criminalistic and Police Studies, Belgrade, 2012.
3. Bonneau, J; Brown, J; Physical ability, fitness and police work, *Journal of Clinical Forensic Medicine*, vol. 2, pp. 157-164, 1995.
4. Dujković, P; Subotički, S; Klisarić, M; Use of police powers - Introduction into the police tactics, practicum (*Primena policijskih ovlašćenja - Uvod u policijsku taktiku, praktikum*) Ministry of Interior of the Republic of Serbia, Belgrade, 2009.
5. Živanović, N; *Attachment of epistemology of physical culture - 2nd suppl. and revised edition* (*Prilog epistemologiji fizičke kulture - 2. dopunjeno i prerađeno izdanje*), Panoptikum, Niš, 2000.
6. Janković, R; Changes at repetitive strength of different muscle groups at academy of criminalistic and police studies students during first three years of studies (Promene repetitivne snage posmatranih mišićnih grupa kod studenata Kriminalističko-policijske akademije tokom prve tri godine studija), *Annual of the Faculty of Sport and Physical Education*, vol. 16, pp. 111-124, 2009.
7. Janković, R; Vučković, G; Blagojević, M; Establishing the norms within the polygon for police officers' specific skill evaluation for students of the Academy of Criminalistics and Police Studies, (Utvrđivanje normativa poligona za procenu specifične spremnosti policajaca za studente Kriminalističko-policijske akademije), *Security*, 56(2), pp. 65-76, 2014.
8. Catalog of specialized police training programs (Katalog programa specijalističkih obuka), Ministry of Interior of the Republic of Serbia, Directorate for Expert Education, Professional Development and Science and OSCE Mission to Serbia. Belgrade: Fiducia 011, Print, 2014.
9. Mitrović, B; Efects of Specialized physical education on muscle strength and body composition (Efekti Specijalnog fizičkog obrazovanja na mišićnu snagu i telesnu kompoziciju), *PhD thesis*, Faculty of Sport and Physical Education, University of Niš, 2016.
10. Mitrović, B; Đorđević, A; Dopsaj, M; Uticaj telesne mase i težinsko-visinskog na kardiorespiratornu izdržljivost pripadnika specijalnih jedinica, važnu sposobnost u borbi protiv terorizma (The effect of body weight and the weight-height ratio on cardiorespiratory endurance of special unit members, an important ability in the fight against terrorism). U: Kolarić, D. (ur.), Zbornik radova naučno-stručnog skupa sa međunarodnim učešćem „Tara 2015": *Suprotstavljanje savremenim oblicima kriminaliteta - analiza stanja, evropski standardi i mere za unapređenje,* Kriminalističko-policijska akademija Beograd, *Tom I*, str. 241-251, 2015.


35 B. Mitrović, A. Đorđević, M. Dopsaj, The effect of body weight and the weight-height ratio on cardiorespiratory endurance of special unit members, an important ability in the fight against terrorism, Procedings of „Tara 2015": ACPS, I/2015, pp. 241-251.

11. Mitrović, B. J; Janković, R; Dopsaj, M; Vučković, G; Milojević, S; Pantelić, S; Nurkić, M; How an eight-month period without Specialized physical education classes affects the morphological characteristics and motor abilities of students of the Academy of Criminalistic and Police Studies, *Facta Universitatis - series: Physical Education and Sport*, 14(2), pp. 167-178, 2016.
12. Mudrić, R., *Special physical education: handbook* (*Specijalno fizičko obrazovanje: priručnik*), Police College, Belgrade, 2005.
13. Obradović, S; Planning, recruitment and selection of personnel in the Ministry of Internal Affairs of the Republic of Serbia (Planiranje, regrutovanje i selekcija kadra za prijem u Ministarstvo unutrašnjih poslova RS), *Science-Security-Police*, pp. 135-156, vol. 16 (1), 2011.
14. Professional Development Programme of Police Officers of MoI of the Republic of Serbia (Program stručnog usavršavanja policijskih službenika Ministarstva unutrašnjih poslova Republike Srbije); Belgrade, 2016.
15. Vučković, G; Dopsaj, M; Criminalistic and Police Studies students' attitudes regarding training in Special Physical Education (Stavovi studenata Kriminalističko-policijske akademije o nastavi Specijalnog fizičkog obrazovanja), *Physical Culture*, No. 2/2011, Belgrade, No. 65(2), pp. 33-41, 2011.

## REGULATIONS

*1. Law on Police (Zakon o policiji)*, "Official Gazette of the RS", No. 6/2016.
*2. Rulebook of Professional Education and Training in the Ministry of Interior (Pravilnik o stručnom osposobljavanju i usavršavanju)*, "Official Gazette of the RS", No. 80/2010

## INTERNET SOURCES

1. Center for specialized training and professional development of police officers, available at: *http://prezentacije.mup.gov.rs/upravazaobrazovanje/lat-i2007_1.html* (15.01.2016.)
2. The catalog of specialized police training programs. (2014). Ministry of Interior of the Republic of Serbia, Directorate for Expert Education, Professional Development and Science and OSCE Mission too Serbia. Belgrade: Fiducia 011 Print, available at: *http://prezentacije.mup.gov.rs/upravazaobrazovanje /Katalog%20Web.pdf* (15. 01. 2017.)

# POLICE ACADEMY STUDENTS INITIAL LEVEL OF FLEXIBILITY: A PILOT STUDY[1]

**Vladimir Timotijević**[2]
**Nenad Koropanovski**[3]
Academy of Criminalistic and Police Studies, Belgrade

**Abstract:** Flexibility influences the amplitude of body parts movement and consequently the efficiency of physical activities which are an integral part of police officers training and professional duties. The aim of this study was to determine the initial level of flexibility in students of the Academy of Criminalistic and Police Studies (ACPS), as well as the differences between genders. The sample consisted of 34 participants, 15 female (age 19,6 ± 0,8 years) and 19 male students (age 20,2 ± 1,1 years). All participants were first year students without previous specialized physical education instructions. A battery of tests for flexibility assessment included: Sideways Leg Splits (SsLS), Sideward Leg Splits right (SdLS_right), Sideward Leg Splits left (SdLS_left), Single-Legged Knee Bend right (SLKB_right), Single-Legged Knee Bend left (SLKB_left), Lengthwise Leg Splits right (LLS_right), Lengthwise Leg Splits left (LLS_left), Sit and Reach (SR), and Shoulder flexibility (SF). The existence of the general differences between groups was determined by MANOVA, for the determination of partial differences Bonferroni test was used. The results showed that on a general level there was a statistically significant difference between genders at the level of Wilks' Lambda 0.098 ($F = 24.415$, $p = 0.000$). The differences were found in tests SsLS ($F = 7.613$, $p = 0.010$), SdLS_right ($F = 38.278$, $p = 0.000$), SdLS_left ($F = 32.968$, $p = 0.000$), SLKB_left ($F = 5.545$, $p = 0.025$), LLS_right ($F = 16.100$, $p = 0.000$), LLS_left ($F = 15.507$, $p = 0.000$), SR ($F = 5.180$, $p = 0.030$) and SF ($F = 25.426$, $p = 0.000$). The obtained results indicated different initial flexibility levels between female and male students. In relation to martial arts and other athletes ACPS students have a lower level of flexibility. Future research should determine the level of flexibility during and after the completion of the educational process, as well as correlation with other physical abilities significant for successful police duties performance.

**Key words:** flexibility, gender, students, police

## INTRODUCTION

Professional engagement of police officers requires a necessary level of work qualifications and skills in all elements essential for successful operation, among which are theoretical and practical knowledge in the field of Specialized Physical Education (SPE). The diversity of activities which characterise police work emphasizes the importance of the physical fitness of police officers.[4] The method of operation and the responsibility police officers have

1 This 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 projects 2015-2019.
2 timotijevicvlada@gmail.com
3 nenad.koropanovski@kpa.edu.rs
4 Strating, M., et al. (2010). A job-related fitness test for the Dutch police. *Occupational Medicine*, 60(4): 255-260.

require optimum level of physical abilities, which is one of the factors influencing efficient performance.[5,6] Police officers should be qualified to overpower and detain a suspect, break up conflicts and control masses.[7] They also have to be able to help the injured after accidents and in emergency situations such as floods or fires.[8] To efficiently and safely fulfil the said tasks, police officers must be physically fit.[9] For successful performance of police work and fulfilling professional obligations of police officers, it is necessary to be of adequate health,[10] morphological characteristics[11,12] as well as basic and specific physical abilities.[13,14] A student of Academy of Criminalistic and Police Studies (ACPS), i.e. a future police officer, is obliged to fulfil certain selection criteria on an annual basis, which simultaneously indicate the level of their adjustment to the applied training loads during SPE.[15,16]

Flexibility is generally considered one of the most important components of physical ability. It is often used to describe the amplitude of movement of either one or more joints.[17] In training theory, "flexibility" is defined as the ability of an individual to perform movement of high amplitudes, depending on the motor activity characteristics.[18,19] If an individual is more flexible, the training is performed in a more efficient, quick and distinct manner.[20] In training practice, flexibility represents one of many important factors necessary for the successful performance of movement activities. Flexibility is important for higher amplitudes of movement performance. Having in mind that police work requires the knowledge of a great number of martial arts techniques, greater joint flexibility enables a more efficient and easier performance of the techniques. The performance of techniques at greater distances which provide greater security of police officers in critical situations is facilitated by the flexibility of muscles. Flexibility is important for performing more efficient movement as the individuals with higher levels of flexibility perform movements more efficiently, or quickly, because it enables muscular activity at a longer distance, and consequently at a higher speed. The requirements regarding muscular strength are lower, as it takes less strength to stretch the antagonist muscles which stop the movement. This is important for the fact that police officers are expected to resolve critical situations as efficiently as possible and using minimum level

5 Sorensen, L., et al. (2000). Physical activity, fitness and body composition of Finnish police officers: a 15-year follow-up study. *Occupational Medicine*, 50(1): 3-10.
6 Strating, M., et al. (2010). Opus citatum, 255-260.
7 Anderson, G., Plecas, D. (2000). Predicting shooting scores from physical performance data. *An International Journal of Police Strategies & Management,* 23(4): 525-537.
8 Anderson, G., et al. (2001). Police officers physical ability testing re-validating a selection criterion. *An International Journal of Police Strategies & Management,* 24(1): 8-31.
9 Bonneau, J., Brown, J. (1995). Physical ability, fitness and police work. *Journal of Clinical Forensic Medicine,* 2(3): 157-164.
10 Sorensen, L., et al. Opus citatum, 3-10.
11 Dopsaj, M., et al. (2005). Dijagnostika stanja Indeksa telesne mase studenata Policijske akademije. *Sportska medicina*, 5(4): 180-191.
12 Malavolti, M., et al. (2008). Effects of intense military training on body composition. *Journal of Strength and Conditioning Research*, 22(2): 503-508.
13 Copay, A., Charles, M. (1998). Police academy fitness training at the police training institute, University of Illinois. *An International Journal of Police Strategies & Management,* 21(3): 416-431.
14 Jankovic, R., et al. (2015). Validity and reliability of the test for assessment of specific physical abilities of police officers in anaerobic-lactate work regime. *Facta Universitatis, Series: Physical Education and Sport*, 13(1): 19-32.
15 Dopsaj, M., Vuckovic, G. (2006). Pokazatelji maksimalne sile pregibaca leve i desne sake u funkciji selekcionog kriterijuma za potrebe policije. *Sport Mont*, 4(10-11): 148-154.
16 Dimitrijevic, R., et al. (2014). The influence of different physical education programs on police students' physical abilities. *An International Journal of Police Strategies & Management*, 37(4): 794-808.
17 Alter, MJ. (1996). Science of Flexibility. Champaign, IL: *Human Kinetics*.
18 Zeljaskov, C. (2004). Kondicioni trening vrhunskih sportista. Sportska akademija. Beograd.
19 Fratric, F. (2006). Teorija i metodika sportskog treninga. Fakultet fizičke kulture. Novi Sad.
20 Stefanovic, D., et al. (2010). Tehnologija pripreme sportista. Fakultet sporta i fizičkog vaspitanja. Beograd.

of force. Finally, higher level of flexibility is directly related to reducing the risk of injury due to higher reserve flexibility.[21] The reduction of medical costs, sick leaves, and reduced work capacity are only some of the factors indicating that the level of flexibility should be developed and kept at a necessary level.

Flexibility is divided into functional, reserve and maximum on the one hand, as well as static and dynamic on the other. Functional flexibility is defined as flexibility with low amplitudes and is manifested in everyday activities (e.g. walking). Reserve flexibility is an addition to functional flexibility and enables movements of higher amplitudes, such as martial art techniques. Maximum flexibility is characterised by extreme joint flexion or extension, abduction, and it is most often performed during candidate testing. Static flexibility is manifested in static conditions, and dynamic in the conditions of body movement through space.[22]

All of the above mentioned indicates flexibility importance in motoric tasks which security agency personnel realize on their duty. In addition, available bibliography does not cover this topic. The issue with this research is determining the level of flexibility of first year students of ACPS using standardized flexibility assessment tests intended for upper and lower parts of the body. The aim of this research is to determine the initial level of ACPS student flexibility, as well as the differences between male and female gender of the tested individuals.

## METHODS

### Subjects

The testing was performed on 34 students of the first year of ACPS. Out of that number, 19 examinees were of male gender, and 15 of female gender. All examinees were informed about the course and the procedure of testing. None of the participants reported any injury or problem which could influence the testing results.

### Procedure

The testing included anthropometrical measurements of body height and mass, which provided the data for BMI calculation. Body height (BH) and body mass (BM) were measured to the nearest 0.5 cm and 100 g, respectively. Thereafter, the body mass index was assessed ($BMI = BM/BH^2$). Anthropometric measurements were taken by the same experimenter according to standard procedures.

Flexibility assessment was performed by using the tests already validated by previous research papers as field tests and they are practically applied in various sports,[23],[24] especially in those in which flexibility is one of dominant motor abilities such as martial arts. The testing of flexibility performance was preceded by a standard 10-min warm-up and 10-min active stretching, following a detailed explanation and qualified demonstration of each test.

*Single-Legged Knee Bend* - This test predominantly assesses the flexibility of the hip flexors muscles. The participant kneels on the right leg, with the left leg extended forward, but the lower leg is kept vertically. From this starting position, the participant slides the knee back as far as possible while supporting himself with his left hand holding the chair and the right hand being supported by the experimenter. The trunk remains in the upright position (i.e., aligned with a vertical line on the wall), no rotation of the hips is allowed, while the lower part

21 Ibidem, 74-81.
22 Ibidem, 74-81.
23 Rosch, D., et al. (2000). Assessment and evaluation of football performance. *American Journal of Sports Medicine*, 28: 29-39.
24 Bozic, P., et al. (2010). Evaluation of the field tests of flexibility of the lower extremity: reliability and the concurrent and factorial validity. *The Journal of Strength and Conditioning Research*, 24(9): 2523-31.

of the front leg remains vertical. A kinanthropometer is used for measurement of the height of the symphysis (h), whereas a ruler (fixed on the ground) is used for measurement of the horizontal distance between the back knee and the vertical projection of symphysis (a). The hip extension angle of the back leg is obtained from trigonometric calculation (a = arctan*(a/h)).

*Sideward Leg Splits* - The test predominantly assesses the flexibility of the hamstring muscles of the front leg and the adductor muscles of the back leg. The participant stands on a smooth board and supports himself with the left hand holding the chair and the right hand being supported by the experimenter. His back (i.e., right) foot is turned out and forms an angle of 90° with the forward (i.e., left) foot. Thereafter, he slowly slides both feet apart. The trunk remains upright (vertical line on the wall) and no hip rotation is allowed. A kinanthropometer is used for measurement of the distance between the symphysis and the ground (h), whereas a ruler (fixed on the ground) for measurement of the distance between the heel of the back leg and point of the vertical projection of symphysis on the ground (a) and the distance between the heel of the front leg and point of the vertical projection of symphysis on the ground (b). The angle formed by the legs is assessed by means of a trigonometric formula (a = arctan*(a/h) + arctan*(b/h)).

*Sideways Leg Splits* - This exercise mainly allows for the assessment of flexibility of the adductor muscles.[25] The participant stands on a smooth board and supports himself with the left hand holding the chair and the right hand being supported by the experimenter. The feet are placed parallel. Thereafter, he slides both of his feet slowly apart while the trunk remains in the upright position aligned with a vertical line depicted on the wall. A kinanthropometer is used for measurement of the distance between the symphysis and the ground (h), whereas a ruler (fixed on the ground) is used for measurement of the distance between the heels and the point of the vertical projection of symphysis on the ground (a, b). A trigonometric calculation (a = arctan*(a/h) + arc- tan*(b/h)) is used to calculate the angle formed by the legs.

*Lengthwise Leg Splits* - This exercise allows for the assessment of flexibility of the hamstring and quadriceps muscle.[26] The participant kneels on the right leg, with the left leg stretched out forward while supporting oneself with the left hand holding the chair and the right hand being supported by the experimenter. Thereafter, he slides the extended leg forward, while the other knee remains at the floor and the upper leg remains vertical. No hip rotation is allowed. A kinanthropometer is used for measurement of the distance between the symphysis and the ground (h), while a ruler (fixed on the ground) is used for measurement of the distance between the back knee and the point of the vertical projection of symphysis on the ground (a), and the distance between the front heel and the vertical projection of symphysis (b). A trigonometric calculation (a = arctan*(a/h) + arctan*(b/h)) is used to calculate the angle formed by 2 legs.

*Sit and Reach* - This exercise mainly allows for the assessment of flexibility of the hamstring and the spine muscles.[27] A box which has a scale marked out on the upper side ("0" marks of the ruler are 10 cm toward the hips) is placed against the wall. The participant sits on the floor with his fully extended legs and feet placed together next to the box. The participant's hands are on top of each other (tips of the middle fingers aligned) and palms down. The participant reaches slowly forward and touches the front of the box with both hands as far as possible. The examiner measures the point where the tip of the middle fingers touches the scale. Precision of the measurement is 0.5 cm.

25 Rosch, D., et al. (2000). Opus citatum: 29-39.
26 Ibidem, 29-39.
27 Jackson, AW., Langford, NJ. (1989). The criterion-related validity of the sit and reach test: Replication and extension of previous findings. *Research Quarterly for Exercise and Sport*, 60: 384-387.

*Shoulder flexibility (twist with the stick)* - Twist exercise is a test assessing the flexibility of arms and shoulder region. The participant holds a stick in his hands extended forward and his right hand holds the end of the stick, and his left hand holds the stick right next to measurement scale. From the initial position, holding the hands extended forward, the participant slowly raises the stick and parts his hands by sliding his right hand (his left hand remains fixed to the end of the stick). The task requires that the participant performs a twist above his head holding the stick with hands extended forward, thereby trying to keep as little distance between the inner sides of his hands as possible.

## RESULTS

Table 1 shows the results of median value and standard deviations of morphological characteristics of the participants, as well as the difference in results between male and female participants.

*Table 1. Demographic and anthropometric profiles of the police academy students*

| | Male (N=19) | | Female (N=15) | | |
|---|---|---|---|---|---|
| | Mean | SD | Mean | SD | p-value |
| Body Height (cm) | 182.5 | 0.05 | 169.7 | 0.03 | 0.00* |
| Body Mass (kg) | 80.6 | 8.2 | 62.0 | 6.8 | 0.00* |
| BMI (kg/m$^2$) | 24.1 | 1.7 | 21.5 | 2.2 | 0.00* |
| ** - significant difference between groups (independent t-test)* | | | | | |

Based on the data from Table 1, a statistically important difference in BH and BM is noticeable between male and female students. Also, a statistically important difference is obtained regarding BMI.

Table 2 shows the results of median values, standard deviations, as well as the difference in results in indicators between male and female participants.

*Table 2. Flexibility measures of police academy students*

| | Male (N=19) | | Female (N=15) | | |
|---|---|---|---|---|---|
| | Mean | SD | Mean | SD | p-value |
| SsLS (°) | 126.7 | 16.2 | 143.2 | 18.4 | 0.01* |
| SdLS_right (°) | 127.5 | 12.1 | 156.9 | 15.6 | 0.00* |
| SdLS_left (°) | 126.4 | 15.1 | 156.4 | 15.1 | 0.00* |
| SLKB_right (°) | 47.5 | 4.5 | 51.0 | 5.5 | 0.05* |
| SLKB_left (°) | 46.7 | 7.6 | 53.6 | 9.5 | 0.02* |
| LLS_right (°) | 117.7 | 10.6 | 140.3 | 21.4 | 0.00* |
| LLS_left (°) | 117.8 | 13.1 | 140.8 | 20.8 | 0.00* |
| SR (cm) | 6.2 | 5.8 | 11.4 | 7.3 | 0.03* |
| SF (cm) | 97.6 | 13.2 | 72.6 | 15.6 | 0.00* |

SsLS- Sideways Leg Splits; SdLS- Sideward Leg Splits;
SLKB- Single-Legged Knee Bend; LLS- Lengthwise Leg Splits;
SR- Sit and Reach; SF- Shoulder flexibility.
* - significant difference between groups (independent t-test)

Table 2 shows the statistically important difference for all variables of flexibility which is noticeable between male and female students.

## DISSCUSION

The aim of this research was to determine morphological characteristics and the initial level of flexibility in ACPS students, as well as the differences between male and female students. Expectedly, male students were statistically significantly higher ($F = 71.904$; $p = 0.00$) and heavier ($F = 49.465$; $p = 0.00$) than female students. Also, statistically significant difference was found for variable BMI ($F = 14.814$; $p = 0.00$), which was higher in male students. Both male and female, belonged to standard weight class in accordance with the standards of World Health Organization, whereby male students' results were very close to the upper bound. The average morphological parameters in male students (TV = 182.5 cm, TM = 80.6 kg, BMI = 24.1 kg/m$^2$) were very similar with the data in Dimitrijevic et al. research[28] on ACPS students (Generation 1995: BH = 182.01 cm, BM = 80.95 kg, BMI = 24.38 kg/m$^2$; Generation 2005: BH = 182.25 cm, BM = 80.63 kg, BMI = 24.23 kg/m$^2$; Generation 2010: BH = 182.62 cm, BM = 78.89 kg, BMI = 23.61 kg/m$^2$). The average morphological parameters in female students (BH = 169.7 cm, BM = 62.0 kg, BMI = 21.5 kg/m$^2$) were very similar to the data in Dopsaj et al. research[29] on ACPS students (BH = 169.5 cm, BM = 62.5 kg, BMI = 21.7 kg/m$^2$).

MANOVA results showed a significant difference in statistical terms between male and female students in all flexibility related variables. Female students demonstrated a higher level of flexibility in all tests when compared to male students. The tests which showed statistically significant differences were SsLS ($F = 7.613$; $p = 0.01$), SdLS (SdLS right $F = 38.278$; $p = 0.00$, SdLS_left $F = 32.968$; $p = 0.00$), SLKB (SLKB_right $F = 3.961$; $p = 0.05$, SLKB_left $F = 5.545$; $p = 0.02$), LLS (LLS_right $F= 16.100$; $p = 0.00$, LLS_left $F = 15.507$; $p = 0.00$), SR ($F = 5.180$; $p = 0.03$) and SF ($F = 25.426$; $p = 0.00$). Similar results were also obtained in previous research studies with distance runners and karatekas, where female participants achieved better results in comparison with male participants in flexibility related tests.[30],[31]

The diversity of activities which characterize police work emphasizes the importance of possessing a certain level of lower body flexibility. Due to the specific nature of police work, hip flexibility is necessary for foot and arm punches as well as throwing techniques. More precisely, direct foot punches (mae geri) are used when it is necessary to apply great force from a safe distance. Biomechanical requirements for performing such a punch include a certain level of flexibility of front and back hamstrings. Also, the same applies to circular foot punch (mawashi geri), whereas the complexity of this punch requires a higher flexibility of the inner part of upper legs. Efficient rotations in hips which add to previous movements of other body parts, apart from circular leg punch, are also characteristic of arm punches and some throwing techniques (uci mata, o soto gari), and largely depend on the flexibility of this joint.

28 Dimitrijevic, R., et al. (2014). Opus citatum: 794-808.
29 Dopsaj, M., et al. (2009). Antropomorfološki profil studentkinja KPA i različito treniranih sportistkinja – multicentroidni model. *Nauka, bezbednost, policija*, 14(1): 145-160.
30 Tamra, T., Robert, B. (2009). Sit and reach flexibility and running economy of men and women collegiate distance runners. *Journal of Strength and Conditioning Research,* 23(1): 158–162.
31 Timotijevic, V. et al. (2015). Morphological characteristics and flexibility at the junior karate competitors. *Godisnjak*, *Fakultet sporta i fizickog vaspitanja Beograd*, 224-236.

Bearing in mind that the techniques taught in SPE lessons are taken over from martial arts and are adjusted to the requirements of police work, the athletes in relevant disciplines can be considered a representative sample. In the comparison between karate players and ACSP students, karate players achieved significantly better results in all tests.[32]

Sit and reach is one of the tests which allows for the assessment of hamstrings flexibility which is of great importance for throwing and foot techniques. The advantage of this test is its simple application, and the disadvantage is the fact that the test does not precisely assess the flexibility in each participant individually (the value is expressed in centimetres and not in degrees), so that the participants with longer limbs have the advantage in achieving good results over those participants with shorter limbs. Also, the result of this test depends on the flexibility of spine and shoulder regions. When the results in sit and reach tests were compared, ACPS students achieved lower test results than distance runners (men 18.38 cm, women 35.88 cm),[33] judokas (16.2 cm),[34] karatekas (38.73 cm),[35] basketball players (27.1 cm), handball players (29.6 cm), soccer players (26.8 cm), volleyball players (33.7 cm)[36] and better results than football players (-5.6 cm).[37] These differences might be attributed to the influence of training process of the athletes of the categories mentioned above.

Due to its anatomy, shoulder is one of the most flexible joints in human body, and is therefore often prone to injuries. The surrounding muscles together with the ligaments contribute to its stabilization. Insufficient level of shoulder muscles flexibility may adversely influence the performance of certain techniques (arm punches, blocks, throwing and holds), and finally lead to injuries. By reviewing and comparison of the results in available bibliography, it was established that handball players achieved better results than ACPS students (95 cm),[38] whereas female tennis players also achieved better results than female ACPS students (65.9 cm) in the same tests.[39] These differences might be attributed to the influence of training process in which the athletes were involved.

The downside of this research is a relatively small sample, which is the reason why it is not possible to draw general conclusions. Future research should examine the connection between the level of flexibility and other general motor skills, as well as the efficiency of performing specific motor tasks. Also, the determination of minimum level of flexibility for successful performance of motor tasks would be of particular importance for the improvement of professional work and training process control. Finally, future research should give scientifically valid answers about the importance of flexibility in relevant space, as well as the type of flexibility of importance to the efficient performance of work by security services officers.

32 Ibidem, 224-236.
33 Tamra, T., Robert, B. (2009). Opus citatum: 158–162.
34 Ibidem: 17-21.
35 Nikookheslat, DS., et al. (2016). Physical and Physiological Profile of Elite Iranian Karate Athletes. *International Journal of Applied Exercise Physiology,* 5(4): 35-44.
36 Jaric, S., et al. (2001). Anthropometric, strength, power and flexibility variables in elite male athletes: basketball, handball, soccer and volleyball players. Journal of human movement studies, 40: 453-464.
37 Katralli, J., et al. (2015). A cross sectional study to assess flexibility and agility levels in Indian judo players. *International Journal of Current Research and Review*, *Chandrapur*▪ 7(3): 17-21.
38 Grujic, I., et al. (2011). Comparison and analyses of differences in flexibility among top-level male and female handball players of different ages. *Physical Education and Sport*, *Facta Universitatis*, 9(1): 1-7.
39 Filipcic, A., Filipcic, T. (2005). The relationship of tennis-specific motor abilities and the competition efficiency of young female tennis players. *Kinesiology*, 37(2): 164-172.

## CONCLUSION

The aim of this research represents the establishment of the initial level of ACPS students' flexibility. Female students expectedly achieved better results in flexibility tests than male students. The initial level of student flexibility was lower in comparison with athletes. Future research of this type should focus on older students to determine the level of flexibility through all years of studies. This would provide a bigger picture, and indicate potential deficiencies, as well as the possibilities for corrections of the curriculum of specific physical education regarding flexibility as one of the most important motor skills. Given that this was initial testing, measured values of these variables may represent the base for creating a database, which would serve as a base for monitoring and control of ACPS students' flexibility. Also, future research should include a higher number of participants in order to gain a more objective insight of tested skills, on the basis of which, when compared to other motor space, the importance of flexibility could be objectively understood.

## REFERENCES

1. Alter, MJ. (1996). Science of Flexibility. Champaign, IL: *Human Kinetics*.
2. Anderson, G., Plecas, D. (2000). Predicting shooting scores from physical performance data. *An International Journal of Police Strategies & Management,* 23(4): 525-537.
3. Anderson, G., Plecas, D., Segger, T. (2001). Police officers physical ability testing re-validating a selection criterion. *An International Journal of Police Strategies & Management,* 24(1): 8-31.
4. Bonneau, J., Brown, J. (1995). Physical ability, fitness and police work. *Journal of Clinical Forensic Medicine,* 2(3): 157-164.
5. Bozic, P., Pazin, N., Berjan, B., Planic, N., Cuk, I. (2010). Evaluation of the field tests of flexibility of the lower extremity: reliability and the concurrent and factorial validity. *The Journal of Strength and Conditioning Research*, 24(9): 2523-2531.
6. Copay, A., Charles, M. (1998). Police academy fitness training at the police training institute, University of Illinois. *An International Journal of Police Strategies & Management,* 21(3): 416-431.
7. Dimitrijevic, R., Koropanovski, N., Dopsaj, M., Vuckovic, G., Jankovic, R. (2014). The influence of different physical education programs on police students' physical abilities. *An International Journal of Police Strategies & Management*, 37(4): 794-808.
8. Dopsaj, M., Nešić, G., Koropanovski, N., Sikimić, M. (2009). Antropomorfološki profil studentkinja KPA i različito treniranih sportistkinja – multicentroidni model. *Nauka, bezbednost, policija*, 14(1): 145-160.
9. Dopsaj, M., Milosevic, M., Vuckovic, G., Blagojevic, M., Mudric R. (2005). Dijagnostika stanja Indeksa telesne mase studenata Policijske akademije. *Sportska medicina*, 5(4): 180-191.
10. Dopsaj, M., Vuckovic, G. (2006). Pokazatelji maksimalne sile pregibaca leve i desne sake u funkciji selekcionog kriterijuma za potrebe policije. *Sport Mont*, 4(10-11): 148-154.
11. Filipcic, A., Filipcic, T. (2005). The relationship of tennis-specific motor abilities and the competition efficiency of young female tennis players. *Kinesiology*, 37(2): 164-172.
12. Fratric, F. (2006). Teorija i metodika sportskog treninga. Fakultet fizičke kulture. Novi Sad.

13. Grujic, I., Ohnjec, K., Vuleta, D. (2011). Comparison and analyses of differences in flexibility among top-level male and female handball players of different ages. *Physical Education and Sport*, *Facta Universitatis*, 9(1): 1-7.
14. Jackson, A. W., Langford, N. J. (1989). The criterion-related validity of the sit and reach test: Replication and extension of previous findings. *Research Quarterly for Exercise and Sport*, 60: 384-387.
15. Jankovic, R., Dopsaj, M., Dimitrijevic, R., Savkovic, M., Vuckovic, G., Koropanovski, N. (2015). Validity and reliability of the test for assessment of specific physical abilities of police officers in anaerobic-lactate work regime. *Facta Universitatis, Series: Physical Education and Sport*, 13(1): 19-32.
16. Jaric, S., Ugarkovic, D., Kukolj, M. (2001). Anthropometric, strength, power and flexibility variables in elite male athletes: basketball, handball, soccer and volleyball players. *Journal of human movement studies*, 40: 453-464.
17. Katralli, J., Goudar, S.S., Itagi, V. (2015). A cross sectional study to assess flexibility and agility levels in Indian judo players. *International Journal of Current Research and Review*, *Chandrapur*, 7(3): 17-21.
18. Malavolti, M., Battistini, N., Dugoni, M., Bagani, B., Bagani, I., Pietrobelli, A. (2008). Effects of intense military training on body composition. *Journal of Strength and Conditioning Research*, 22(2): 503-508.
19. Nikookheslat, D.S., Faraji, H., Fatollahi, S., Alizadeh, M. (2016). Physical and Physiological Profile of Elite Iranian Karate Athletes. *International Journal of Applied Exercise Physiology,* 5(4): 35-44.
20. Rosch, D., Hodgson, R., Peterson, L., Graf-Baumann, T., Junge, A., Chomiak, J., Dvorak, J. (2000). Assessment and evaluation of football performance. *American Journal of Sports Medicine*, 28: 29-39.
21. Sorensen, L., Smolander, J., Louhevaara, L., Korhonen, O., Oja, P. (2000). Physical activity, fitness and body composition of Finnish police officers: a 15-year follow-up study. *Occupational Medicine*, 50(1): 3-10.
22. Stefanovic, D., Jakovljevic, S., Jankovic, N. (2010). Tehnologija pripreme sportista. Fakultet sporta i fizičkog vaspitanja. Beograd.
23. Strating, M., Bakker, R., Dijkstra, G., Lemmink, K., Groothoff, J. (2010). A job-related fitness test for the Dutch police. *Occupational Medicine*, 60(4): 255-260.
24. Tamra, T., Robert, B. (2009). Sit and reach flexibility and running economy of men and women collegiate distance runners. *Journal of Strength and Conditioning Research,* 23(1): 158–162.
25. Timotijevic, V., Aleksic, B., Jovanovic, S., Suzovic, D. (2015). Morphological characteristics and flexibility at the junior karate competitors. *Godisnjak*, *Fakultet sporta i fizickog vaspitanja Beograd*, 224-236.
26. Zeljaskov, C. (2004). Kondicioni trening vrhunskih sportista. Sportska akademija. Beograd.

# PERCEPTIVE ABILITIES IN DEFENSIVE TASKS AGAINST DIFFERENT ATACKS

**Milos Mudric**[1]
Faculty of Sports and Physical Education, University of Belgrade, Serbia
**Srecko Jovanovic**
Faculty of Sports and Physical Education, University of Belgrade, Serbia
**Aleksandar Nedeljkovic**
Faculty of Sports and Physical Education, University of Belgrade, Serbia
**Ivan Cuk**
College of Sports and Health, Belgrade, Serbia
**Slobodan Jaric**
Department of Kinesiology and Applied Physiology, University of Delaware, US
Biomechanics and Movement Science Graduate Program,
University of Delaware, US

**Abstract:** Perceptive abilities play an important role in solving complex tasks in everyday life as well as in particular specific situations related to the security issues. The aim of this study was to determine perceptive abilities of karate athletes of different knowledge level, since the training of security services is based on the elements of karate techniques. Perceptive abilities were assessed through the recorded reaction time. The sample consisted of 20 karate athletes (age 23.3 ± 3.2) and 10 beginners (age 22.2 ± 3.4) who performed defence of the reverse punch (gyaku zuki) and defence of roundhouse kick (mawashi geri). To assess the differences between the groups and offensive techniques we applied two-way mixed-model ANOVA, and the level of statistical significance was set at $p = 0.05$. Two-way mixed-model ANOVA revealed significant main effect of group [$F_{(1,29)} = 18.0$, $\eta^2 = 0.39$, $p < 0.01$] and the Group x Technique interaction [$F_{(1,29)} = 7.64$, $\eta^2 = 0.21$, $p < 0.01$], but not the main effect of the offensive techniques [$F_{(1,29)} = 0.587$, $\eta^2 = 0.02$, $p = 0.45$]. Specifically, the karate athletes reacted quicker than the beginners in both Gyaku zuki and Mawashi geri ($p < 0.01$), but the difference was more prominent in Gyaku zuki. The obtained results suggest that the applied approach could be developed into a routine test of perceptual abilities in different specific situations both in sports and other human movement related areas.

**Key words:** reaction time, blocks, kicks, punches, karate

## INTRODUCTION

A number of everyday motor activities are characterized by environmental unpredictability, such as postural responses to unexpected external perturbations. The perceptive abilities have an important role in making adequate responses in the realization of the various daily activities, professional activities, and particularly in sports. In combat sports, activities are expressed in stressful conditions. The athletes are required to quickly and accurately processed relevant information and shorten the time for decision making. Karate is a good example

1 E-mail: milosmudric@gmail.com

of competitive sport with the constant changes in offensive and defensive activities of competitors). The outcome of the fight depends on the activities of competitors in the battle for distance and the preparation actions. Each competitor is trying to "abduct" space form the opponent, to "catch" an opportune moment of his unwillingness and to suddenly perform a quick and pointed action. On the other hand, in case of the opponent attack, the competitor must anticipate the moment of initiating offensive actions and to intercept it, or avoid it or defend from it). In regard to this, perceptive abilities have an important role in solving complex competing tasks. Perceptive abilities in this study were evaluated through the reaction time. Reaction time is the time that elapses from the moment of stimuli from the environment to perform intentional reaction. Obtaining a intentional reaction, unlike the reflexes, is achieved through the processing stimulation at the cortical level, and depends on: the time reception of sensory stimulation.[2] The reaction time is often a key element of the competitive success. In this sense, this research refers to the speed of simple and choice reaction time karate athletes of different levels of knowledge. Based on the research problem, the aim of this study was to compare reaction time karate athletes of different levels of knowledge measured by using modern video technology. The measuring of reaction time was based on two real components (stimulus and response). The stimuli consisted of video recorded karate punches and kicks, while the responses represented an adequate defense in the form of blocks which are used in combat situations. Participants were elite karate athletes and beginners, because we assumed that there are differences in the speed of choice reaction time between those two groups of subjects due to the specific effects of training and experience. Expected findings could improve the methodology of karate training, and other educational groups where the techniques of karate are used as a tool of specially-physical education (police, army, etc.).

# METHODS

### Participants

The sample consisted of two groups of subjects. The first subject group consisted of male elite karate athletes who were members of national karate team of Serbia (N=20; age 23.3 ± 3.2; data shown as mean ± SD), while the second subject group consisted of age and gender matched beginners (N=10; age 22.6 ± 1.3 years) who were students of the Faculty of Sport and Physical Education. They all practiced basic karate techniques through their academic curriculum.

### Experimental procedures

The applied experimental procedures were experimentally evaluated within our previous study.[3] Perceptive abilities were assessed through the recorded reaction time. Initially, at the same time, we recorded the offensive actions (i.e., 'stimulus') and the corresponding kinematic data that are enabled set the moment of stimulus. After that, we recorded the defensive actions associated with video first offensive action (stimulus) who gave us the main set of kinematic data that were used to determine the moment of the beginning of an answer. The time interval between the onset of the stimulus (stimulus) and the response time was considered as a reaction time. The elite karate competitor performed separate two different offensive action ((Mae-mawashi geri (i.e., front roundhouse kick with front leg) and Gyaku zuki (i.e., the reverse punch)). These techniques were chosen because they are commonly used in kara-

2 Drenovac, M. (2010). Kronometrija dinamike mentalnog procesiranja (*Chronometry of dynamics of mental processing*). Osijek, HR: Filozofski fakultet.

3 Mudric, M., Cuk, I., Nedeljkovic, A., Jovanovic, S., Jaric, S. (2015) Evaluation of Video-based method for the measurement of reaction time in specific sportsituation. *International Journal of Performance Analysis in Sport*, 15: 1077-1089.

te fight. The video camera was placed in a position that simulates both the viewing distance and eye level of a hypothetical opponent in areal combat situation. The video recording was synchronized with the 3-dimensional (3D) infrared recordings of 12 reflective markers positioned on the centers of the wrist, elbow, shoulder, hip, knee, and ankle joints. Subsequently we performed the 3D kinematic movement analysis in order to determine the stimulus onset of four recorded offensive actions. Specifically, when any of the markers reached 5% of its 3D peak velocity was assumed to be the instant of the stimulus onset.

The previously recorded offensive action stimuli of karate model were displayed in real dimensions on a large 2x3 m screen. The subjects were standing 2 m apart, having a reflective marker placed on the processusstyloideus of their front hand. The subsequent kinematic analysis was conducted in order to determine the onset of the defensive response (i.e., 5% of the peak velocity of wrist marker). Note that the 3D recording of defensive action responses was coupled with the video projection of the offensive action stimuli by means of a common external trigger. The difference between onsets of an offensive action stimulus and defensive action response was calculated as RT.

RTs were calculated under one experimental condition. Within this condition, two possible offensive actions stimuli were projected in random sequence unknown for subjects (i.e., the Choice RT). Specifically, the subjects were expecting Mae-ashimawashi geri or Gjaku zuki to be projected and, therefore, instructed to react by proper defensive response (i.e., Te Nagashi uke or Gedan barai, respectively).

**Statistical analysis**

To assess the choice RT differences between the groups (i.e., Karate athletes and Beginners) and offensive stimuli (i.e., Gyaku zuki and Mae-ashi mawashi geri) we applied two-way mixed-model ANOVA on median value of the 3 tested trials. In case of the significant interactions, Bonferroni post-hoc test was applied.

Eta squared ($\eta^2$) was calculated for the two-way mixed-model ANOVA where the values of the effect sizes 0.01, 0.06 and above 0.14 were considered small, medium, and large, respectively.[4] The level of statistical significance was set to $p < 0.05$. All statistical tests were performed using SPSS 20 (IBM, Armonk, NY).

## RESULTS WITH DISCUSSION

Figure 1. depicts averaged values across the subjects RTs obtained from 2 groups under 2 offensive stimuli. Two-way mixed-model ANOVA revealed significant main effects for both group [$F_{(1,29)}= 18.0$, $\eta^2 = 0.39$, $p < 0.01$] and interaction [$F_{(1,29)}= 7.64$, $\eta^2 = 0.21$, $p < 0.01$], but not offensive stimuli [$F_{(1,29)}=0.587$, $\eta^2 = 0.02$, $p = 0.45$]. Specifically, Karate athletes reacted quicker than Beginners in both Gyaku zuki and Mae ashi mawashi geri offensive stimuli ($p < 0{,}01$). However, significant interaction indicates that Beginners, reaction time was slower when reacting on Gyaku zuki, than on Mae-ashi mawashi geri ($p = 0{,}04$), whereas Karate athletes demonstrated no differences in reaction between abovementioned offensive stimuli ($p = 0{,}95$).

4 Cohen, J. (1992). Statistical power analysis, *Current directions in psychological science*, 1, 98-101.

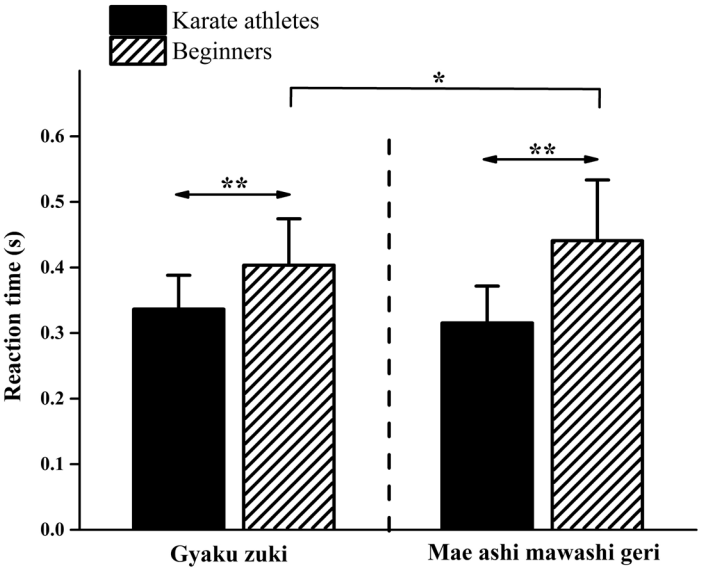



*Figure 1.Averaged across subjects data calculated from median value of 3 consecutive trials obtained from different offensive stimuli (Mae ashi mawashi geri and Gyakuzuki), groups (Karate Athletes and Beginners), and condition (Choice RT), shown together with the corresponding 95% confidence intervals error bars.*

Based on the analysis of the reation time in the applied tests, obtained data indicate a longer time in response to the techniques used in this study. The values of extended time especially are expressed in the group of beginners, but little less, in group of karate athletes. These results greatly contribute to the explanation of the results obtained in a number of earlier published researches where it is obtained that the hand techniques Gyaku zuki and the foot technique Mawashi geri belong to the scoring technique with the highest rate of application in the karate fight.[567] In particular, the resulting reaction time indicates that the kinematic schemes of these techniques are more difficult to anticipate and require more time to prepare programming responses. Special interest related to determining the differences in reaction times of karate athletes and subjects who have passed only initial training in karate and have not a competitive experience.

This study showed that in applied tests that simulate real offensive actions were obtained significant difference in reaction times between athletes of different levels of knowledge. Specifically, it was proved that karate athletes react significantly faster according to a group of beginners under complex conditions. Obtained results can be due to the influence of various forms of sparring which that applies as a method of training at karate athletes. This method of training develop the ability to timely response to the punch known in advance, based on identification and anticipation preparatory movement and position of individual body segments,

5 Gužvica, M. (2000). Tehničko-taktičke karakteristike težinskih kategorija u jugoslovenskom karateu (*Magistarski rad*), Fakultet Fizičke Kulture Univerziteta u Beogradu, Beograd.
6 Koropanovski, N., Jovanović, S. i Dopsaj, M. (2007). Kvantitativni pokazatelji zastupljenosti poentirajućih tehnika kod vrhunskih karatista. „Analytics and diagnostics of physical activity", Beograd, str. 109-116.
7 Mudrić, R.,Jovanović, S., Gužvica, M. (2001). Rezultati istraživanja tehničko taktičkih karakteristika jugoslovenskih takmičara u sportskim borbama, Nauka i karate sport, Zrenjanin, str. 55-64.

prior to a certain punch or kick. Related differences were obtained in earlier studies in which they applied the real elements.[89]

The results also show that the karate athletes have significantly shorter reaction time according to a group of beginners which explicitly shows that the applied method in karate training have a significant impact on the development of perceptual abilities in tasks situational character. This is confirmed by this study. Karate athletes in all of the tests are statistically different from the group of beginners. It should be noted that the beginners have a shorter reaction time on the offensive action when it was shown a hand technique Gjaku zuki rather than offensive action when it was shown foot techmique Mae-ashimawashi geri. Karate athletes are equally reacted quickly and on one and the other type of offensive action.

## CONCLUSIONS

Studies of the reaction time in the combat sports, especially in karate, tend for continuous improvement of conditions for testing perceptual skills which significantly affect the performance of the competition.

Potentially the main significance of this research reflected in obtaining new knowledge about the perceptual abilities of karate athletes using new video method and progress in developing situational tests for assessing these skills.

The findings from this study could contribute to improving the methodology of karate training, total training technology in this sport, particularly in improving perceptual skills relating to the responsiveness relates to the speed of response to changing competitive situations.

Also, these findings could improve the methodology of training and other educational groups where the techniques of karate used as a tool specially-physical education (police, army, etc.).

From a theoretical perspective, future studies should include a more complex set of conditions that should provide more detailed modelling of stimulus-response in different populations through the evaluation standard parameters of Hiks law.

## REFERENCES

1. Cohen, J. (1992). Statistical power analysis, *Current directions in psychological science*, 1, 98-101.
2. Gužvica, M. (2000). Tehničko-taktičke karakteristike težinskih kategorija u jugoslovenskom karateu (*Magistarski rad*), Fakultet Fizičke Kulture Univerziteta u Beogradu, Beograd.
3. Koropanovski, N., Jovanović, S. i Dopsaj, M. (2007). Kvantitativni pokazatelji zastupljenosti poentirajućih tehnika kod vrhunskih karatista. „Analytics and diagnostics of physical activity", Beograd, str. 109-116.
4. Mori S., Ohtani Y., Imanaka K. (2002) Reaction times and anticipatory skills of karate athletes. *Human Movement Science,* 21(2): 213–230.

8 Mori S., Ohtani Y., Imanaka K. (2002) Reaction times and anticipatory skills of karate athletes. *Human Movement Science,* 21(2): 213–230.
9 Williams, A.M., & Elliott, D. (1999). Anxiety and visual search strategy in karate. *Journal of Sport and Exercise Psychology, 21*, 362–375.

5. Mudric, M., Cuk, I., Nedeljkovic, A., Jovanovic, S., Jaric, S. (2015) Evaluation of Video-based method for the measurement of reaction time in specific sportsituation. *International Journal of Performance Analysis in Sport*, 15: 1077-1089.

6. Mudrić, R.,Jovanović, S., Gužvica, M. (2001). Rezultati istraživanja tehničko taktičkih karakteristika jugoslovenskih takmičara u sportskim borbama, Nauka i karate sport, Zrenjanin, str. 55-64.

7. Drenovac, M. (2010). Kronometrija dinamike mentalnog procesiranja (*Chronometry of dynamics of mental processing*). Osijek, HR: Filozofski fakultet.

8. Williams, A.M., & Elliott, D. (1999). Anxiety and visual search strategy in karate. *Journal of Sport and Exercise Psychology, 21*, 362–375.

# DIFFERENCES IN KEY PERFORMANCE INDICATORS BETWEEN POLICE COLLEGE CADETS IN DIFFERENT SEMESTERS OF THEIR EDUCATION

**Aleksandar Cvorovic**
**Ahmad Al Maamari**
Abu Dhabi Police College, Abu Dhabi, United Arab Emirates

**Abstract:**Physical preparedness is a significant component of any member of the police forces. In the system of education of future officers in the test sample it occupies a very prominent place. Schooling lasts nine semesters, and this research has been done with the aim of determining possible differences in body composition and physical performance. The research included 605 male participants (*19.98 years ±1.21 years;BW=68.14 kg, ±8.99 kg; BH=173.61 cm, ±5.36 cm*) divided into four groups based on who is currently attending which semester, in this case, the participants are the second (*n=168; 18.63 years; BW=65.22 kg; BH=173.86 cm*), fourth (*n=142; 19.43 year; BW=67.16 kg; BH=173.01 cm*), sixth (*n=152; 20.54 years, BW=69.88;BH=173.84 cm*),and eighth (*n=143; BW=70.68 kg; BH=173.67 cm*) semester of their education. The null hypothesis is that there is no significant difference among the cadets even though they belong to the different semesters of study. Further analysis confirm that there are differences in body composition as well as the physical performance of the participants. Per that, a null hypothesis is rejected. Measured Anthropometric variables, including height, weight and waist circumference, and key performance indicators in the standard procedure for testing during the final exam at the end of each semester are push-ups, sit-ups and running 2.4 kilometres. It is found that there is an improvement in almost all segments at significance level *p=0.05*. Apart from basic descriptive statistics differences between the groups treated with one-way ANOVA, and unlike in the group for Post Hoc analysis Tukey test was applied.

***Keywords:****police, performance, differences, body composition, testing*

**Corresponding author:** Aleksandar Cvorovic, email: cvorovic77@yahoo.com

## INTRODUCTION

Modern police officer job is a highly stressful occupation[1] with special requirements in terms of physical preparedness and body composition. Scientific interest in this topic started a long time ago and the beginning of the information is most collected among the members of the military,[2] but also in police especially in North American region.[3] In terms of a larger number of police research appears in the second half of the 20th century and this trend con-

1 Yao, Z., Yuan, Y., Buchanan, T. W., Zhang, K., Zhang, L., & Wu, J. (2016). Greater Heart Rate Responses to Acute Stress Are Associated with Better Post-Error Adjustment in Special Police Cadets. Plos One, 1-10.
2 Friedl, K. E. (2012). Body Composition and Military Performance - Many things to Many People. *Journal of Strength Training and Conditioning Research*, S87-S100.
3 Bonneau, J., & Brown, J. (1995). Physical Ability, Fitness and Police Work. *Journal of Clinical Forensic Medicine*, 157-164.

tinues.[4,5,6] Today, scientist from different fields are involved in the process, but there are still challenges that need to give an adequate answer. The biggest challenges occur after the end of training or schooling because the range of duties in the police is very wide and there are occupations where the level of physical activity is high, to those where they almost did not exist. Thus, there is a decline in physical ability and an increase in body weight in the form of body fat.[7] As mentioned before policeman's job is extremely stressful, with negative effects on health and there is a larger number of research on that subject.[8,9]

The main objective of this research is to present the data on the impact of continuous physical activity on the cadets who attend the various years of study. The influence of time is taken as a starting point for testing variability in terms of body composition, and in terms of physical ability. Key Performance Indicators (KPI) within the AD Police College are aerobic capacity, muscular endurance and body composition.

## METHODS

Research included 605 Police College students, where the participants were divided per criteria of the current semester attended as a part of their education, which lasts 9 semesters, or four and a half years. The collected data are the results of final examinations within Physical Education classes at the end of the second, fourth, sixth and eighth semesters respectively. It is a generation whichis currently attending College. The variables that are collected refer to the anthropometric and physical abilities. Anthropometric variables are Body Weight (BW), Body Height (BH) and waist circumference (Waist), which is used for the purposes of calculating Waist-to-Haight Ratio (WHtR). Physical abilities are aerobic endurance(capacity), which is measured by the test of Running 2.4 km (RU) and muscular endurance which is measured with two tests, maximum number of completed Push-Ups (PU) and Sit-Ups (SU) for 1 minute. Measurements were performed by trained instructors at the applicable standards within the Abu Dhabi Police to which they belong. At the start of testing the first measurements are related to Body Height, Body Weight and then Waist, accuracy of measurements is 1 cm for BH and Waist, and 0.1 kg for BW. The next step is testing the strength endurance and the first test is Push-Ups, then a Sit-Ups, and the last test is aerobic endurance (RU), with accuracy of measurements of 1 s.

Data processing was carried out with IBM SPSS 20.0 software. Apart from basic descriptive data variability between the groups treated with One-Way ANOVA at significance level $\leq 0.05$ and homogeneity between groups was checked with post-hoc analysis with the help of Tukey test, at the same significance level.

4 Stamford, B., Weltman, A., Moffat, R., &Fulco, C. (1978). Status of Police Officers with Regard to Selected Cardio-Respiratory and Body Compositional Fitness Variables. *Medicine and Science in Sports*, 294-7

5 Spliter, D., Jones, G., Hawkins, J., &Dudka, L. (1987). Body Composition and Physiological Characteristics of Law Enforcement Officers. *British Journal of Sports Medicine*, 154-7.

6 Sörensen, L., Smolander, J., Louhevaara, V., Korhonen, O., &Oja, P. (2000). Physical Activity, Fitness and Body Composition of Finish Police Officers: a 15-year Follow up Study. In *Occupational Medicine* (pp. 50(1): 3-10). London: Oxford, England.

7 Sörensen at al. Opus citatum. (pp. 50(1): 3-10).

8 Pollock, M., LR, G., & Meyer, B. (1978). Analysis of Physical Fitness and Coronary Heart Disease Risk of Dallas Area Police. *Journal of Occupational Medicine: Official Publication of the Industrial Medical Association*, 393-8.

9 Sargent, C., Gebruers, C., & O'Mahony, J. (2017). A Review of the Physiological and Psychological Health and Wellbeing of Naval Service Personnel and the Modalities Used for Monitoring. *Military Medical Research*, 4:1.

# RESULTS

As part of this work in this chapter are presentedthe results of research after processing of raw data and after statistical analysis. The presented data relate mainly to the proven variability, or they are relevant to the topic of work.

*Table 1: Descriptive Statistics for all participants and for all variables*

| Variable | N | Range | Minimum | Maximum | Mean | Std. Deviation |
|---|---|---|---|---|---|---|
| Age | 605 | 4 | 18 | 22 | 19.98 | 1.210 |
| BW | 605 | 57.0000 | 48.0000 | 105.0000 | 68.138843 | 8.9918798 |
| BH | 605 | 39 | 161 | 200 | 173.61 | 5.364 |
| Waist | 605 | 33 | 63 | 96 | 76.77 | 6.244 |
| WHtR | 605 | 19.8463 | 35.3261 | 55.1724 | 44.231524 | 3.5202738 |
| PU | 605 | 41 | 29 | 70 | 40.76 | 7.051 |
| SU | 605 | 38 | 32 | 70 | 45.95 | 6.756 |
| RU | 605 | 472 | 496 | 968 | 594.20 | 38.882 |

*Table 2: One-Way ANOVA for age and anthropometric variables*

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Age | Between Groups | 737.080 | 3 | 245.693 | 1000.146 | .000 |
| | Within Groups | 147.640 | 601 | .246 | | |
| | Total | 884.721 | 604 | | | |
| BW | Between Groups | 2952.788 | 3 | 984.263 | 12.892 | .000 |
| | Within Groups | 45882.970 | 601 | 76.344 | | |
| | Total | 48835.757 | 604 | | | |
| BH | Between Groups | 69.455 | 3 | 23.152 | .804 | .492 |
| | Within Groups | 17306.264 | 601 | 28.796 | | |
| | Total | 17375.719 | 604 | | | |
| Waist | Between Groups | 2465.662 | 3 | 821.887 | 23.427 | .000 |
| | Within Groups | 21085.009 | 601 | 35.083 | | |
| | Total | 23550.671 | 604 | | | |
| WHtR | Between Groups | 816.767 | 3 | 272.256 | 24.538 | .000 |
| | Within Groups | 6668.199 | 601 | 11.095 | | |
| | Total | 7484.966 | 604 | | | |

***Table 4:*** *Tukey Test for Weight to Haight Ratio (WHtR)*

| Semester | N | Subset for alpha = 0.05 | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| 2 | 168 | 42.55 | | |
| 4 | 142 | | 43.99 | |
| 6 | 152 | | | 45.18 |

| | | | | |
|---|---|---|---|---|
| 8 | 143 | | | 45.41 |
| Sig. | | 1.000 | 1.000 | .929 |

*Table 3: Tukey Test for Body Weight (BW)*

| Semester | N | Subset for alpha = 0.05 | |
|---|---|---|---|
| | | 1 | 2 |
| 2 | 168 | 65.22 | |
| 4 | 142 | 67.16 | |
| 6 | 152 | | 69.87 |
| 8 | 143 | | 70.68 |
| Sig. | | .216 | .854 |

*Table 5: Descriptive statistics for physical abilities in different semester, Push-Ups (PU), Sit-Ups (SU) and Running (RU)*

| Semester | | N | Mean | Std. Deviation | Std. Error | Minimum | Maximum |
|---|---|---|---|---|---|---|---|
| PU | 2 | 168 | 35.60 | 6.060 | .468 | 29 | 70 |
| | 4 | 142 | 41.55 | 7.099 | .596 | 34 | 69 |
| | 6 | 152 | 42.07 | 5.659 | .459 | 37 | 65 |
| | 8 | 143 | 44.63 | 5.931 | .496 | 37 | 67 |
| | Total | 605 | 40.76 | 7.051 | .287 | 29 | 70 |
| SU | 2 | 168 | 41.18 | 5.921 | .457 | 32 | 64 |
| | 4 | 142 | 47.74 | 7.040 | .591 | 36 | 69 |
| | 6 | 152 | 46.70 | 5.460 | .443 | 39 | 62 |
| | 8 | 143 | 48.97 | 5.669 | .474 | 39 | 70 |
| | Total | 605 | 45.95 | 6.756 | .275 | 32 | 70 |
| RU | 2 | 168 | 596.15 | 33.776 | 2.606 | 506 | 650 |
| | 4 | 142 | 588.67 | 32.923 | 2.763 | 510 | 645 |
| | 6 | 152 | 602.24 | 55.607 | 4.510 | 508 | 968 |
| | 8 | 143 | 588.85 | 24.315 | 2.033 | 496 | 633 |
| | Total | 605 | 594.20 | 38.882 | 1.581 | 496 | 968 |

*Table 6: One-Way ANOVA for physical abilities Push-Ups (PU), Sit-Ups (SU) and Running (RU)*

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| PU | Between Groups | 6962.287 | 3 | 2320.762 | 60.461 | .000 |
| | Within Groups | 23068.995 | 601 | 38.384 | | |
| | Total | 30031.283 | 604 | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SU | Between Groups | 5665.803 | 3 | 1888.601 | 51.813 | .000 |
| | Within Groups | 21906.505 | 601 | 36.450 | | |
| | Total | 27572.307 | 604 | | | |
| RU | Between Groups | 18914.866 | 3 | 6304.955 | 4.238 | .006 |
| | Within Groups | 894219.332 | 601 | 1487.886 | | |
| | Total | 913134.198 | 604 | | | |

*Table 7: Tukey test for Push-Ups (PU)*

| Semester | N | Subset for alpha = 0.05 | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| 2 | 168 | 35.60 | | |
| 4 | 142 | | 41.55 | |
| 6 | 152 | | 42.07 | |
| 8 | 143 | | | 44.63 |
| Sig. | | 1.000 | .884 | 1.000 |

*Table 8: Tukey test for Sit-Ups (SU)*

| Semester | N | Subset for alpha = 0.05 | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| 2 | 168 | 41.18 | | |
| 6 | 152 | | 46.70 | |
| 4 | 142 | | 47.74 | 47.74 |
| 8 | 143 | | | 48.97 |
| Sig. | | 1.000 | .445 | .293 |

*Table 9: Tukey test for Running (RU)*

| Semester | N | Subset for alpha = 0.05 | |
|---|---|---|---|
| | | 1 | 2 |
| 4 | 142 | 588.67 | |
| 8 | 143 | 588.85 | |
| 2 | 168 | 596.15 | 596.15 |
| 6 | 152 | | 602.24 |
| Sig. | | .334 | .518 |

## DISCUSION

It is common practice for testing within the police or armyto use thetests which are the subject of this research. The reasons for this are relatively easy implementation of the testing

on a large sample of respondents. Experts also point to a need for changes in current practice, and they should give judgment and find adequate and justifiable solutions. Most of the scientific community has agreed that the existing tests should be retained or modified, and add the tests for the measurement of specific skills directly related to operations of modern police officers or soldiers.[10, 11,12,13]

In terms of body composition within the existing sample there is no risk in terms of obesity, to the contrary with recent research in the United Arab Emirates and the Gulf region,[14] because obesity among students takes the level of the epidemic especially among boys,[15] similar trend is noted between the members of Abu Dhabi Police.[16] For these reasons, Waist to Haight Ratio is in use for obesity control because it is a better indicator of possible risk of obesity, diabetes and chronic kidney disease.[17,18] Values above 50 in WHtR indicated possible risk for illness or obesity. The reasons for good body composition in relation to the rest of the population in the country lie in the fact that when cadets enrol the college they need to pass preselection in terms of physical abilities and body composition, as well as the continuous physical activity during the entire schooling.[19] Common examples are that after completion of the training and education we have reduction infitness level and an increase in body weight, without doubt, the solution is to create the conditions for continuous training over the career of police officers.[20]

As for the physical performance, the average cadet at the College is capablewithin a one-minute period to do approximately 41 push-ups, 46 sit-ups, and run the distance of 2.4 km for 9 minutes and 54 seconds (Table 1), however, among the groups in relation to the semester there appear certain differences.The results in the number of push-ups and sit-ups have continued rising trend as training progresses. Homogeneity in the results of the number of push-ups occurs in the students of 4$^{th}$and 6$^{th}$term (Table 7),while in the case of sit-ups homogeneity occurs between 6$^{th}$and 4$^{th}$, and between 4$^{th}$and 8$^{th}$term (Table 8). In case of running homogeneity in the results exists between 2$^{nd}$, 4$^{th}$and 8$^{th}$term, but also between 2$^{nd}$ and 6$^{th}$

10 Rhodes, E., &Farenholtz, D. (1992). Police Officer's Physical Abilities Test Compared to Measures of Physical Fitness. Canadian Journal of Sport Sciences=Journal Canadien Des Sciences du Sport, 228:33.
11 Anderson, S. G., Plecas, D., &Segger, T. (2001). Police Officer Physical Ability Testing, Re-Validating a Selection Criterion. *Policing: An International Journal of Police Strategies & Management*, 8-31.
12 Nindl, B., Alvar, B., R Dudley, J., Favre, M., Martin, G., Sharp, M., Kreamer, W. (2015). Executive Summary from the National Strength and Conditioning Association's Second Blue Ribbon Panel on Military Physical Readiness: Military Physical Performance Testing. *Journal of Strength Training and Conditioning Research*, S216-20.
13 Orr, R. M., Ford, K., &Stierli, M. (2016). Implementation of an Ability-Based Training Program in Police Force Recruits. *Journal of Strngth and Conditioning Researches*, 2781-2787.
14 Vats, M., Mahboub, B., Al Hariri, H., Al Zaabi, A., & Vats, D. (2016). Obesity and Sleep-Related Breathing Disorders in Middle East and UAE. *Canadian Respiratory Journal*, 2016: 9673054.
15 Al Blooshi, A., Shaban, S., Al Tunaiji, M., Fares, N., Al Shehhi, L., Al Shehhi, H., Souid, A. (2016). Increasing Obesity Rates in School Children in United Arab Emirates. *Obesity Science and Practice*, 196-22.
16 Kukic, F., &Dopsaj, M. (2016). Structural Analysis of body Composition Status in Abu Dhabi Police Personnel. *NBP. Journal of Criminalistic and Law*, Article in Press.
17 Buchan, D. S., & Baker, J. S. (2016). Utility of Body Mass Index, Waist-to-Height-Ratio and Cardiorespiratory Fitness Thresholds for Identifying Cardiometabolic Risk in 10.4—17.6-Year-Old Children. *Obesity Research & Clinical Practice*, Article in Press.
18 Blaslov, K., Bulum, T., &Duvnjak, L. (2015). Waist-to-Height Ratio is Independently Associated with Chronic Kidney Diseease in Overweight Type 2 Diabetic Patients. *Endocrine Research*, 194-8.
19 Cvorovic, A. (2016). Body Composition Status of Abu Dhabi Police College Cadets. *2nd International Conference on Sports Medicine and Fitness.* Dubai: Journal of Sports Medicine and Doping Studies. doi:10.4172/2161-0673.C1.005.
20 Rossomanno, C., Herrick, J., Kirk, S., & Kirk, E. (2012). A 6-Month Supervised Employer-Based Minimal Exercise Program for Police Officers Improves Fitness. *Journal of Strength and Conditioning Research*, 2338-44.

term (Table 9). Running scores are also better over time with some exceptions. The reason for some nonlinear fluctuation between semesters are probably the number of classes of physical education, and generation preselection quality. Specifically, in this case, with the participants of the sixth semester a direct reason is the lack of physical education classes in the weekly schedule. During this period, the students have more academic activities and training that is not directly associated with greater physical activity.

Compared with similar research results in terms of physical abilities,the students are at a good level,[21],[22] especially in terms of running.[23] The program in physical education classes is well conceived as its continuous progress occurs over time during education. Weaknesses that manifest are the most common, and it is lack of motivation and saturation with testing procedures, especially in the period from the sixth to the ninth semester.

## CONCLUSION

The research gave a certain amount of information about physical fitness and body composition in relation to the year of study. The presented data suggest that the cadets are at a good level of fitness and body composition, as well as that their progress continued in line with expectations. Differences among the groups and variables were identified and compared with the information available from similar studies. Logical continuation should be longitudinal study with monitoring of each generation individually and their mutual comparison during the whole schooling. It would certainly be desirable to expand the number of tests for abilities that are not represented, above all, the tests of anaerobic endurance, maximum strength and flexibility.

In the future, we should strive also for implementationof tests related with mobility and identifying possible risk of injuries.[24], [25], [26]

Very important fact is that every year we have more female police officers recruited and selection and the choice of tests should support gender equality, and cannot be the source of any form of discrimination.[27]

21 Crawley, A., Sherman, R., Crawley, W., &Cosio-Lima, L. (2016). Physical Fitness of Police Academy Cadets: Baseline Characteristics and Changes during a 16-Week Academy. *Journal of Strength and Conditioning Research*, 1416-1424.
22 Wu, Y.-N., Hallbourg, K. W., & Collins, S. M. (2015). Changes of General Fitness and Muscle Properties Following Police Cadet Training. *Journal of Physical Therapy Science*, 2783-2786
23 Dawes, J. J., Orr, R. M., Siekaniec, C. L., Vanderwoude, A. A., & Pope, R. (2016). Associations between Anthropometric Characteristics and Physical Performance in Male Law Enforcement Officers: A Retrospective Cohort Study. *Annals of Occupational and Environmental Medicine*, 28:26.
24 Orr, R. M., Pope, R., Stierli, M., & Hinton, B. (2016). A Functional Movement Screen Profile of an Australian State Police Force: A Retrospective Cohort Study. *BMC Musculoskeletal Disorders*, 17:296.
25 Orr, R., Pope, R., Peterson, S., Hinton, B., &Stierli, M. (2016). Leg Power as an Indicator of Risk of Injury or Illness in Police Recruits. *International Journal of Environmental Research and Public Health*, 13, 237.
26 Larsen, B., Aisbett, B., & Silk, A. (2016). The Injury Profile of an Australian Specialist Policing Unit. *International Journal of Environmental Research and Public Health*, 1-9.
27 Shepard, B., & Bonneau, J. (2002). Assuring Gender Equity in Rcruitment Standars For Police Officers. *Canadian Journal of Applied Physiology=Revue Canadienne de Physiologie Appliquee*, 263-95.

## REFERENCES


1. Al Blooshi, A., Shaban, S., Al Tunaiji, M., Fares, N., Al Shehhi, L., Al Shehhi, H., . . . Souid, A. (2016). Increasing Obesity Rates in School Children in United Arab Emirates. *Obesity Science and Practice*, 196-202.
2. Anderson, S. G., Plecas, D., & Segger, T. (2001). Police Officer Physical Ability Testing, Re-Validating a Selection Criterion. *Policing: An International Journal of Police Strategies & Management*, 8-31.
3. Blaslov, K., Bulum, T., & Duvnjak, L. (2015). Waist-to-Height Ratio is Independently Associated with Chronic Kidney Diseease in Overweight Type 2 Diabetic Patients. *Endocrine Research*, 194-8.
4. Bonneau, J., & Brown, J. (1995). Physical Ability, Fitness and Police Work. *Journal of Clinical Forensic Medicine*, 157-164.
5. Buchan, D. S., & Baker, J. S. (2016). Utility of Body Mass Index,Waist-to-Height-Ratio and Cardiorespiratory Fitness Thresholds for Identifying Cardiometabolic Risk in 10.4—17.6-Year-Old Children. *Obesity Research & Clinical Practice*, Article in Press.
6. Crawley, A., Sherman, R., Crawley, W., & Cosio-Lima, L. (2016). Physical Fitness of Police Academy Cadets: Baseline Characteristics and Changes During a 16-Week Academy. *Journal of Strength and Conditioning Research*, 1416-1424.
7. Cvorovic, A. (2016). Body Composition Status of Abu Dhabi Police College Cadets. *2nd International Conference on Sports Medicine and Fitness.* Dubai: Journal of of Sports Medicine and Doping Studies. doi:10.4172/2161-0673.C1.005
8. Dawes, J. J., Orr, R. M., Siekaniec, C. L., Vanderwoude, A. A., & Pope, R. (2016). Associations Between Anthropometric Characteristics and Physical Performance in Male Law Enforcement Officers: a Retrospctive Cohort Study. *Annals of Occupational and Environmental Medicine* , 28:26.
9. Friedl, K. E. (2012). Body Composition and Military Performance - Many things to Many People. *Journal of Strength Training and Conditioning Research*, S87-S100.
10. Kukic, F., & Dopsaj, M. (2016). Structural Analysis of body Composition Status in Abu Dhabi Police Personel. *NBP. Journal of Criminalistic and Law*, Article in Press.
11. Larsen, B., Aisbett, B., & Silk, A. (2016). The Injury Profile of an Australian Specialist Policing Unit. *International Journal of Environmental Research and Public Health*, 1-9.
12. Nindl, B., Alvar, B., R Dudley, J., Favre, M., Martin, G., Sharp, M., . . . Kreamer, W. (2015). Executive Summary From the National Strength and Conditioning Association's Second Blue Ribbon Panel on Military Phisical Readiness: Military Physical Performance Testing. *Journal of Strength Training and Conditioning Research*, S216-20.
13. Orr, R. M., Ford, K., & Stierli, M. (2016). Implementation of an Ability-Based Training Program in Police Force Recruits. *Journal of Strngth and Conditioning Researches*, 2781-2787.
14. Orr, R. M., Pope, R., Stierli, M., & Hinton, B. (2016). A Functional Movement Screen Profile of an Australian State Police Force: a Retrospective Cohort Study. *BMC Musculosceletal Dissorders*, 17:296.
15. Orr, R., Pope, R., Peterson, S., Hinton, B., & Stierli, M. (2016). Leg Power As an Indicator of Risk of Injury or Illness in Police Recruits. *International Journal of Environmental Research and Public Health*, 13, 237.

16. Pollock, M., LR, G., & Meyer, B. (1978). Analysis of Physical Fitness and Coronary Heart Disease Risk of Dallas Area Police. *Journal of Occupational Medicine: Official Publication of The Industrial Medical Association*, 393-8.
17. Rhodes, E., & Farenholtz, D. (1992). Police Officer's Phisical Abilities Test Compared to Measures of Physical Fitness. *Canadian Journal of Sport Sciences=Journal Canadien Des Sciences du Sport*, 228:33.
18. Rossomanno, C., Herrick, J., Kirk, S., & Kirk, E. (2012). A 6-Month Supervised Employer-Based Minimal Exercise Program for Police Officers Improves Fitness. *Journal of Strength and Conditioning Research*, 2338-44.
19. Sargent, C., Gebruers, C., & O'Mahony, J. (2017). A Review of The Physiological and Psychological Health and Wellbeing of Naval Service Personnel and The Modalities Used for Monitoring. *Military Medical Research*, 4:1.
20. Shepard, B., & Bonneau, J. (2002). Assuring Gender Equity in Rcruitment Standars For Police Officers. *Canadian Journal of Applied Physiology=Revue Canadienne de Physiologie Appliquee*, 263-95.
21. Sörensen, L., Smolander, J., Louhevaara, V., Korhonen, O., & Oja, P. (2000). Physical Activity, Fitness and Body Composition of Finish Police Officers: a 15-year Follow Up Study. In *Occupational Medicine* (pp. 50(1): 3-10). London: Oxford, England.
22. Spliter, D., Jones, G., Hawkins, J., & Dudka, L. (1987). Body Composition and Physiological Characteristics of Law Enforcement Officers. *British Journal of Sports Medicine*, 154-7.
23. Stamford, B., Weltman, A., Moffat, R., & Fulco, C. (1978). Status of Police Offcers With Regard to Selected Cardio-Respiratory and Body Compositional Fitness Variables. *Medicine and Science in Sports*, 294-7.
24. Vats, M., Mahboub, B., Al Hariri, H., Al Zaabi, A., & Vats, D. (2016). Obesity and Sleep-Related Breathing Disorders in Middle East and UAE. *Canadian Respiratory Journal*, 2016: 9673054.
25. Wu, Y.-N., Hallbourg, K. W., & Collins, S. M. (2015). Changes of General Fitness and Muscle Properties Following Police Cadet Training. *Journal of Physical Therapy Science*, 2783-2786.
26. Yao, Z., Yuan, Y., Buchanan, T. W., Zhang, K., Zhang, L., & Wu, J. (2016). Greater Heart Rate Responses to Acute Stress Are Associated with Better Post-Error Adjustment in Special Police Cadets. *Plos One*, 1-10.

# EVALUATION OF THE AEROBIC FITNESS IN ABU DHABI POLICEMEN

**Filip Kukic**,

Strategic management and performance improvement department, Sports activities section, Abu Dhabi Police

**Mohammed Abdul Aziz Shamel Al Maamari**,[1]

Strategic management and performance improvement department, Sport activities section, Abu Dhabi Police

**Abstract:** Introduction: Aerobic fitness is one of the most important factors for good health and efficient work performance in police work. Accordingly, monitoring and maintenance of the aerobic capabilities on a regular basis are required. The aim of the study is the evaluation of the aerobic fitness in Abu Dhabi law enforcement officers for purposes of developing scaling system which would be used in regular physical fitness follow up.

**Methods:** 3.2 km running test was conducted outside, starting at about07:00am. Results of 780 male police officers of different rank were selected for this study. Age ranged from 19-45 years with average of 31.82±5.08years. The sample was divided into 5 age categories: ≤ 25 years, 26-30 years, 31-35 years, 36-40 years, and 41-45 years.

Statistics:Simple descriptive statistics have been used to calculate measures of central tendency and dispersity – Mean, Standard Deviation, Maximum, Minimum, Coefficient of variation. Using mean and standard deviation results were classified in 7 classes.

**Results:**

Mean±SD were as follows: All participants – 22:08±04:45 min, ≤ 25 years – 21:41±04:42 min, 26-30 years – 22:09±04:52 min, 31-35 years – 21:58min±04:32, 36-40 years – 22:14±04:46, 41-45 years – 23:23±05:32 min.

Absolute prevalence of participants by classes: superior – 0.4%, very good – 16.9%, above average – 19.7%, average – 35%, below average – 11.2%, bad – 15.3%, and very bad – 2.5%.

Age-dependent prevalence of participants by classes:

≤25 years– superior 0%, excellent 21.0%, very good 28.5%, average 22.6%, weak 17.7%, bad 11.3%, very bad 1.6%;26-30 years – superior 0%, excellent 14.1%, very good 23.3%, average 33.6%, weak 10.6%, bad 18.4%, very bad 0%;31-35 years – superior 0.4%, excellent18.3%, very good 16.7%, average 35.8%, weak10.5%, bad15.2%, very bad 3.1%;36-40 years – superior 0.8%, excellent 18.3%, very good 16.7%, average38.9%, weak 10.5%, bad 15.2%, very bad 4.8%;41-45 years – superior 1.9%, excellent 13.2%, very good 18.9%, average 39.6%, weak 13.5%, bad 10.3%, very bad 5.7%.

**Keywords:** test, police, aerobic, fitness, running, scales

**Corresponding author:** Filip Kukic, email: filip.kukic@gmail.com, mobile: (+971) 056 480 5956

1 Captain, Strategic management and performance improvement department, Sport activities section, Abu Dhabi Police

# INTRODUCTION

Abu Dhabi Police include a wide range of the various responsibilities among which are traffic department, IT department, security support, force 7 unit, force 9 unit, salary section, etc. Some of those departments and sections consist mostly of sedentary duties and responsibilities while others are "on foot", very active and physically demanding. However, the psychological stress level is increased in both cases, and cumulatively it could lead to changes in general health[2,3,4]. Thus, due to general health maintenance and readiness for the job role, a certain level of the physical fitness should be obtained. It would be hard to say which physical ability is more important, cardio endurance, muscle endurance or maximal strength or power but it is evident that all of them are important and should be maintained on a daily basis[5,6,7].

In recent review Hauschild et al. (2016) reported that there are two following tasks of physical abilities when it comes to testing: "content based" performance tests related to job requirements, and general physical components such as aerobic endurance and muscular strength[8]. In line with previously mentioned, Gerber et al. (2010) conducted the study based on the notation that the police work can be twofold stressful: organizational-based and police inherent stress[9]. Organizational stress could be defined as perceived bothersome and administration work, while police inherent stressors would be traumatic and harmful events such as danger, violence, human suffering, securing public gatherings, and maintaining social security on a daily basis[10,11,12]. In both cases, the physical fitness level is of big importance for the general health and mandatory for the job-specific purposes

Prolonged sitting hours spent at work are shown to be highly associated with the increased health risk whereas physical activity is considered as a very good buffer for most of the risk factors[13,14]. Additionally, it has been found that police employees have poorer health prognosis

2 Kukic and Dopsaj (2016). Structural analysis of body composition status in Abu Dhabi police personnel.NBP, Journal of Criminalistics and Law, 21(3), 19-37
3 Dopsaj, M., Vuković, M. (2015). Prevalence of the body mass index (BMI) among themembers of the Ministry of Interior of the Republic ofSerbia - pilot study. Bezbednost, 57(3), 82-48.
4 Lagestad, P., & Van Den Tillaar, R. (2014). Longitudinal changes in the physical activity patterns of police officers. International Journal of Police Science & Management, 16(1), 76-86.
5 Anderson, G. S., Plecas, D., & Segger, T. (2001). Police officer physical ability testing–Re-validating a selection criterion. Policing: An International Journal of Police Strategies & Management, 24(1), 8-31.
6 Lagestad, P., & Van Den Tillaar, R. Opus citatum, pages 76-86.
7 Hauschild, V. D., DeGroot, D. W., Hall, S. M., Grier, T. L., Deaver, K. D., Hauret, K. G., & Jones, B. H. (2016). Fitness tests and occupational tasks of military interest: a systematic review of correlations. Occupational and Environmental Medicine, 0, 1-10.
8 Ibidem, pages 1-10
9 Violanti, J. M., & Aron, F. (1995). Police stressors: Variations in perception among police personnel. Journal of Criminal Justice, 23(3), 287-294.
10 Gerber, M., Kellmann, M., Hartmann, T., &Pühse, U. (2010). Do exercise and fitness buffer against stress among Swiss police and emergency response service officers?. Psychology of Sport and Exercise, 11(4), 286-294.
11 Violanti, J. M., & Aron, F. Opus citatum, pages 287-294.
12 Vučković, G., Subošić, D., &Kekić, D. (2011). Physical abilities of police officers as prerequisite for suppressing violence at sporting events in republic of serbia1. "Archibald Reiss days", 629.
13 Van Uffelen, J. G., Wong, J., Chau, J. Y., van der Ploeg, H. P., Riphagen, I., Gilson, N. D., ... & Gardiner, P. A. (2010). Occupational sitting and health risks: a systematic review. American Journal of Preventive Medicine, 39(4), 379-388.
14 Gerber, M., Kellmann, M., Hartmann, T., &Pühse, U. (2010).Opus citatum, pages 286-294.

and more metabolic disorders then the general population[15,16]. Hartley et al. (2011) showed in their study that police work requires certain "curriculum vitae" for recruitment as police work is both, mentally and physically very demanding. Leischik et al. (2015) have shown that German firefighters have higher VO2max than federal police officers and sedentary office workers and that they are less likely to have metabolic syndrome and waist circumference[17]. Thus, the aerobic fitness level in police environment should be seriously and thoroughly considered and systematically followed up.

Logistically, it is very important to be clear which test is going to be used and for what purposes. Otherwise, numerous issues might occur from various aspects. First in a line could be a prediction of the performance where the task-specific tests will allow better prediction of the performance[18]. However, lack of the test sensitivity in gender and age differences might bring even legal issues[19]. In a re-validation study, Anderson et al. (2001) explained that Canadian Police officer physical abilities test (POPAT) test had to be re-validated because the test might face legal issues due to possible discrimination of the female recruits and officers because pass rate for females was 25% while 65% failed to meet standards. Driven by the examples from the history[20,21] researchers wanted to make sure that the test which will be used in physical abilities assessment will consist internal and external validity.

Abu Dhabi Police recently started to use military procedures for testing physical abilities in employees and accordingly, the scaling system is adjusted to the military population of Abu Dhabi. To be able to evaluate policemen and to develop precise scaling system, the evaluation of each test has to be done. Otherwise, grading employees according to the unadjusted scales might lead to misinterpretation of the results. In the long term, the problem could occur if the level of fitness is one of the factors for the promotion or bonus at work. To wrap it all up, the aim of this study is to evaluate the current state of the aerobic fitness in Abu Dhabi Police officers with the purpose of developing the control over the physical fitness surveillance system.

# METHODS

## PARTICIPANTS

The testing procedure was introduced in Police and announced officially so it became mandatory for all employees to come for the test. From all participants who finished 3200m running test during September 2016780 male police officers of different ranks were randomly included in the evaluation process. Age ranged from 19 to 45 years with an average of 31.82±5.08 years.

15 Hartley, T. A., Burchfiel, C. M., Fekedulegn, D., Andrew, M. E., &Violanti, J. M. (2011). Health disparities in police officers: comparisons to the US general population. International journal of emergency mental health, 13(4), 211.
16 Violanti, J. M., Hartley, T. A., Gu, J. K., Fekedulegn, D., Andrew, M. E., &Burchfiel, C. M. (2013). Life expectancy in police officers: a comparison with the US general population. International Journal of Emergency Mental Health, 15(4), 217.
17 Leischik, R., Foshag, P., Strauß, M., Littwitz, H., Garg, P., Dworrak, B., &Horlitz, M. (2015). Aerobic capacity, physical activity, and metabolic risk factors in firefighters compared with police officers and sedentary clerks. PloS one, 10(7).
18 Hauschild, V. D., DeGroot, D. W., Hall, S. M., Grier, T. L., Deaver, K. D., Hauret, K. G., & Jones, B. H. (2016). Opus citatum, pages 1-10.
19 Anderson, G. S., Plecas, D., &Segger, T. (2001). Opus citatum, pages 8-31.
20 Evans, D. H. (1980). Height, Weight, and Physical Agility Requirements-Title 7 and Public Safety Employment. Journal of Police Science and Administration, 8(4), 414-436.
21 Greenberg, G. J., & Berger, R. A. (1983). A model to assess one's ability to apprehend and restrain a resisting suspect in police work. Journal of Occupational and Environmental Medicine, 25(11), 809-813.

## TESTING PROCEDURE

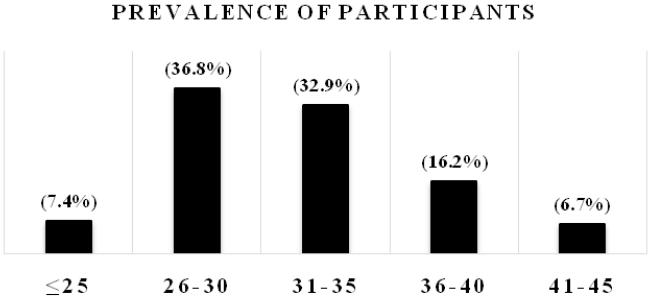
Registration for the testing started at 06:00 am and lasted until 06:45 am. From 06:45-06:50 am participants were briefed about the rules and route of the test. After that, 10 minutes warmup routine fallowed. The test of 3200m running was conducted starting at 07:00 am. The participants were instructed to run the test in the shortest time possible, and they were briefed about the time needed to pass the test. They had to run two different laps around the objects inside the Police College. Coaches were positioned at certain points so the participants could nottake shortcuts and reduce the distance. During the registration for the test, everybody got the sleeveless green t-shirt with a number on it. Those numbers were connected to the employee's ID number so the testing team could easily make an order at the end of the running. At the finish point, two coaches were waiting for the participants: one was measuring the time, and the otherone was writing down the green t-shirt numbers. That way the order of the running time and participant numbers was the same. For the time measurement Casio stopwatch (Casio HS-70W) was used with the possibility of measuring 200 split times. After all employees had passed the finish line, the timings on the stopwatch were recalled from first to last and connected with the numbers on the green t-shirt.

## STATISTICS

Both thedescriptive and prevalence statics were conducted in Microsoft Excel (Microsoft software package, Office 365, subscription 2017). Coding numbers (I-V) for age groups and *count if* function were used to calculate the prevalence of the employees in each group. Seven class level scale, based on sports science metrology statistical principles[22] was used to evaluate the results by dividing them in 7 following classes: Superior, Excellent, Very good, Good, Weak, Bad, Very bad. After the time needed for each aerobic fitness level was defined, the prevalence of the participants from each age group in each aerobic fitness level was calculated.

## RESULTS

All participants were divided into 5 age groups: 1) younger than or equal to 25 years (≤ 25), 2) from 26-30 years, 3) from 31-35 years, 4) from 36-40 years, and 5) from 41-45 years. Employees older than 45 years were not obligated to do the test. Prevalence of participants by age groups is shown in Graph 1, and it can be seen that most of the employees were between 26 and 35 years old.




*Graph 1_Prevalence of the participants in each age group*

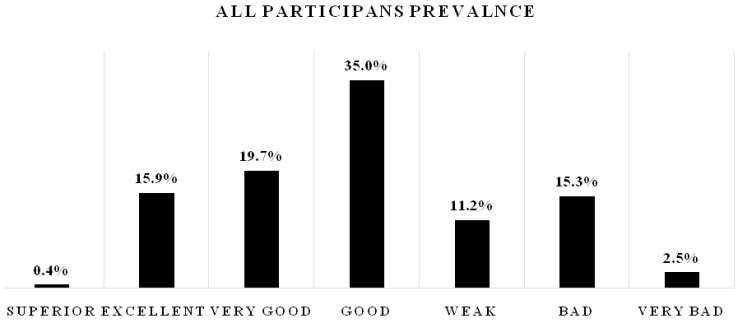
The evaluation of the aerobic fitness level followed the same principle, so participants were evaluated according to the age group which they belonged and according to the achieved result in running. Table 1 shows 7 different levels and the time needed for each of them.

22 Zaciorski, V. M. (1982). Sportivnajametrologija. Moskva: Fizkul'tura i sport

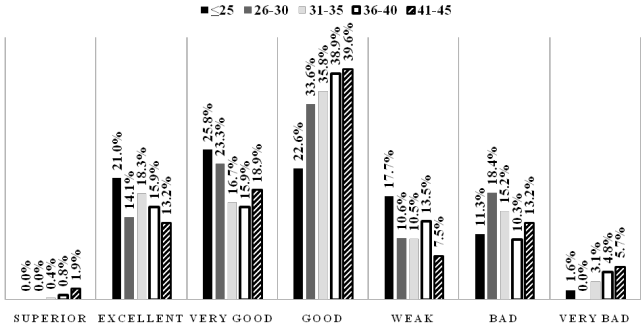
*Table 1_Seven class scale results for every aerobic fitness level in all participants and for each age group*

| 3200M RUNNING (MINUTES) | | | | | | |
|---|---|---|---|---|---|---|
| LEVEL | Sample avg. | ≤25 | 26-30 | 31-35 | **36-40** | **41-45** |
| ***Superior*** | ≤12.38 | ≤12.56 | ≤12.13 | ≤12.54 | ≤12.42 | ≤12.42 |
| ***Excellent*** | 12.37-17.23 | 12.57-17.56 | 12.14-17.08 | 12.55-17.26 | 12.43-17.28 | 12.43-17.57 |
| ***Very good*** | 17.24-19.45 | 17.57-20.26 | 17.09-19.35 | 17.27-19.41 | 17.29-19.51 | 17.58-20.35 |
| ***Good*** | 19.46-24.30 | 20.27-25.26 | 19.36-24.29 | 19.42-24.13 | 19.52-24.37 | 20.36-25.50 |
| ***Weak*** | 24.31-26.53 | 25.27-27.56 | 24.50-26.56 | 24.14-26.29 | 24.38-27.01 | 25.51-28.28 |
| ***Bad*** | 26.54-31.38 | 27.57-32.55 | 26.57-31.50 | 26.30-30.59 | 27.02-31.46 | 28.29-33.42 |
| ***Very bad*** | ≥31.39 | ≥32.56 | ≥31.51 | ≥31.00 | ≥31.47 | ≥33.43 |

Prevalence of the participants for every aerobic fitness level was calculated for the whole sample, Graph 2, and for each age group, Graph 3.




*Graph 2_Absolute prevalence of the participants in each aerobic fitness level*



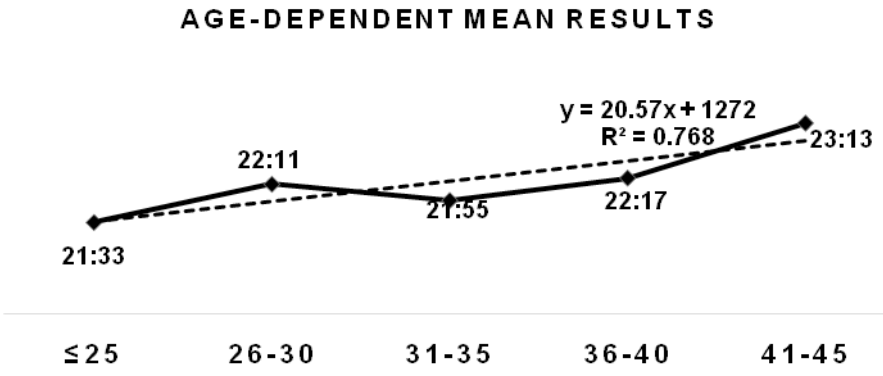

*Graph 3_Age-dependant prevalence of the participants in each aerobic fitness level*

## DISCUSSION

In the present study, we evaluated the status of the aerobic fitness in Abu Dhabi police, with the aim to develop the police employee's norming standards for the regular annual follow-up. These standards could be used for multiple purposes: health monitoring, estimating physical readiness to meet the job requirements, rank promotions, bonuses, awards, etc.

Our results showed that 7.4% of the sample was employees younger than ≤25 years, 36.8% were 26-30 years old, 32.9% were 31-35 years old, 16.2% were 36-40 years old, and 6.7% were 41-45 years old. Practically, 77.1% of the tested sample were employees younger than 36 years of age. Comparing to Canada (54% under 40), USA (average 39.6) and Serbia (average 36.5) tested sample of employees is considerably younger[23,24].

Age-dependent results were divided into 7 classes to show the discrepancy between people and their prevalence in various classes. Classes are defined as a speed of running represented in the time needed to finish the test (see Table 1). According to these results, Graph 2 shows the prevalence of tested employees in each of the 7 classes. Comparing to the average results of the whole sample, age-dependent results for ≤25, 36-40, and 41-45 years are lower for every level while results for 26-30 and 31-35 years are better than the sample average also for every level. These differences are better illustrated on Graph 1 and 2 where we can see that absolute prevalence of the participants in classes is different from that in age-dependent prevalence. Lower results in ≤25 years group might be due to the number of the participants in that group, only 58 or 7.43%. However, the effect of the age on the running time undoubtedly exists. The age is biological, permanent influencing factor which cannot be altered. People are getting older and their physical performance is changing accordingly. The law of regression on Graph 4 shows how significantly the average running time has been decreasing by the age. Calculated constancy of the performance decrease by 20.578s with the age brings the possibility of the age-related discrimination which could be reasonable evidence from the legal point of view[25]. Thus, the evaluation of the results should always be adjusted to the age, and related to that, standards and scales should be defined according to the age.




*Graph 4_Shifting of the results towards slower running time due to the age.*

Second important notation that came from the presented evaluation is influence of the time spent working in the Police workforce on the running results. It can be seen from Graph

23 http://www.statcan.gc.ca/pub/85-002-x/2015001/article/14146/c-g/c-g04-eng.gif
24 https://datausa.io/profile/soc/333050/#demographics
25 Anderson, G. S., Plecas, D., &Segger, T. (2001). *Opus citatum*, pages 8-31

3 that prevalence of the participants from ≤25 group in Excellent, Very good, and Good stays relatively unchanged (21%, 25.8% and 22.6% while in following age groups percentage of Excellent and Very good decreases on account of Good (see Graph 3). A similar trend can be seen between Weak and Bad for the age groups 26-30, 31-35, and 41-45 years of age, the number of Bad results grows at the expense of Weak. It could be due to the level of the physical activity in leisure time as well as long sitting hours at work and increased stress level in policing jobs[26,27,28,29].

The age and the years of service are among the most influential factors which should be considered in the further setting of the testing standards. Working in the Police environment requires for every decision to be explained from the logical point of view as well as from the legal point of view. Thus, the age should be taken into account very seriously because of its possible discriminative role during evaluation of the human's performance.

## CONCLUSION

The presented study should allow us to develop scaling system, norms and standards for mandatory annual aerobic fitness assessment for menof different age in Abu Dhabi Police. Results were found to be age-dependent and it should be considered in further development of the evaluation system. The years of service are found to be in close relationship with the decline of the aerobic fitness and the causes for the decline could be the level of the physical activity in leisure time, food transition and culture, long sitting hours at work, and increased stress level in policing jobs. Further research should include control of the level of physical activity in leisure time and at work, and dietary habits in order to define exact causes for the trend showed.

## PRACTICAL APPLICATIONS

Multiple practical implications might be considered as a result of the presented evaluation:

- development of the age-dependent evaluation system of the physical fitness in Abu Dhabi Police employees,
- development of the scoring system,
- development of the PASS/FAIL standards,
- development of the rewarding system according to the employee's physical performance,
- development of the standards for certain position-related requirements

26 Boyce RW, Jones GR, Lloyd CL, Boone EL (2008). A longitudinal observation of police: body composition changes over 12 years with gender and race comparisons. *Journal of Exercise Physiology,11*(6), 1-13.

27 Despres, J., Lamarche, B (1993). Effects of diet and physical activity on adiposity and body fat distribution: implications for the prevention of cardiovascular disease. *Nutrition Research Reviews*, 6, 137-159.

28 Gerber, M., Kellmann, M., Hartmann, T., &Pühse, U. (2010). *Opus citatum,* pages286-294

29 Ng, S. W., Zaghloul, S., Ali, H., Harrison, G., Yeatts, K., El Sadig, M., &Popkin, B. M. (2011). Nutrition transition in the United Arab Emirates. *European journal of clinical nutrition*, *65*(12), 1328-1337.

## REFERENCES:


1. Anderson, G. S., Plecas, D., & Segger, T. (2001). Police officer physical ability testing–Re-validating a selection criterion. *Policing: An International Journal of Police Strategies & Management*, *24*(1), 8-31.
2. Boyce RW, Jones GR, Lloyd CL, Boone EL (2008). A longitudinal observation of police: body composition changes over 12 years with gender and race comparisons. *Journal of Exercise Physiology,11*(6), 1-13.
3. Despres, J., Lamarche, B (1993). Effects of diet and physical activity on adiposity and body fat distribution: implications for the prevention of cardiovascular disease. *Nutrition Research Reviews*, 6, 137-159.
4. Dopsaj, M., Vuković, M. (2015). Prevalence of the body mass index (BMI) among the members of the Ministry of Interior of the Republic of Serbia - pilot study. *Bezbednost*, *57*(3), 82-48.
5. Dugdill, L., Crone, D., & Murphy, R. (2009). *Physical activity and health promotion: Evidence- based approaches to practice.* Chichester, UK: Wiley-Blackwell.
6. Evans, D. H. (1980). Height, Weight, and Physical Agility Requirements-Title 7 and Public Safety Employment. *Journal of Police Science and Administration*, *8*(4), 414-436.
7. Gerber, M., Kellmann, M., Hartmann, T., & Pühse, U. (2010). Do exercise and fitness buffer against stress among Swiss police and emergency response service officers? *Psychology of Sport and Exercise*, *11*(4), 286-294.
8. Greenberg, G. J., & Berger, R. A. (1983). A model to assess one's ability to apprehend and restrain a resisting suspect in police work. *Journal of Occupational and Environmental Medicine*, *25*(11), 809-813.
9. Hartley, T. A., Burchfiel, C. M., Fekedulegn, D., Andrew, M. E., & Violanti, J. M. (2011). Health disparities in police officers: comparisons to the US general population. *International Journal of Emergency Mental Health*, *13*(4), 211.
10. Hauschild, V. D., DeGroot, D. W., Hall, S. M., Grier, T. L., Deaver, K. D., Hauret, K. G., & Jones, B. H. (2016). Fitness tests and occupational tasks of military interest: a systematic review of correlations. *Occupational and Environmental Medicine*, 0, 1-10
11. Kukic and Dopsaj (2016). Structural analysis of body composition status in Abu Dhabi police personnel. *NBP. Journal of Criminalistics and Law, (3),*
12. Lagestad, P., & Van Den Tillaar, R. (2014). Longitudinal changes in the physical activity patterns of police officers. *International Journal of Police Science & Management*, *16*(1), 76-86.
13. Leischik, R., Foshag, P., Strauß, M., Littwitz, H., Garg, P., Dworrak, B., & Horlitz, M. (2015). Aerobic capacity, physical activity and metabolic risk factors in firefighters compared with police officers and sedentary clerks. *PloS one*, *10*(7), e0133113.
14. Ng, S. W., Zaghloul, S., Ali, H., Harrison, G., Yeatts, K., El Sadig, M., & Popkin, B. M. (2011). Nutrition transition in the United Arab Emirates. *European journal of clinical nutrition*, *65*(12), 1328-1337.
15. Van Uffelen, J. G., Wong, J., Chau, J. Y., van der Ploeg, H. P., Riphagen, I., Gilson, N. D., ... & Gardiner, P. A. (2010). Occupational sitting and health risks: a systematic review. *American Journal of Preventive Medicine*, *39*(4), 379-388.
16. Violanti, J. M., & Aron, F. (1993). Sources of police stressors, job attitudes, and psychological distress. *Psychological Reports*, *72*(3), 899-904.

17. Violanti, J. M., & Aron, F. (1995). Police stressors: Variations in perception among police personnel. *Journal of Criminal Justice*, *23*(3), 287-294.
18. Violanti, J. M., Hartley, T. A., Gu, J. K., Fekedulegn, D., Andrew, M. E., & Burchfiel, C. M. (2013). Life expectancy in police officers: a comparison with the US general population. *International Journal of Emergency Mental Health*, *15*(4), 217.
19. Vučković, G., Subošić, D., & Kekić, D. (2011). Physical abilities of police officers as prerequisite for suppressing violence at sporting events in republic of serbia1. *"Archibald Reiss days"*, 629.

## INTERNET SOURCES

20. http://www.statcan.gc.ca/pub/85-002-x/2015001/article/14146/c-g/c-g04-eng.gif
21. https://datausa.io/profile/soc/333050/#demographics

# CORRELATION BETWEEN BODY COMPOSITION AND PHYSICAL FITNESS OF THE POLICE OFFICERS[1]

**Radivoje Janković**[2]
Academy of Criminalistic and Police Studies, Belgrade, Serbia

**Abstract:** The police occupation is demanding, frequently dangerous, and involves periods of high physical exertion. In order to ensure that the police officers are physically capable of performing their work, criteria for morphological characteristic and physical abilities have been established. The aim of this study is to establish whether morphological characteristics affect the physical fitness of the police officers and in what manner. In the research 74 men of the average age of 28.1±6.1 took part, 19 of whom were the members of Special Anti-Terrorist Unit, 27 were general duties police officers and 28 the Academy of Criminalistic and Police Studies students. Morphological characteristic (MC) such as body height (BH), body weight (BW), body mass index (BMI), body fat mass (BFM), skeletal muscle mass (SMM), percentage of body fat (PBF) and percentage of skeletal muscle (PSM) were determined by multichannel bioelectrical impedance InBody 720. Basic physical abilities (BFA) were determined by a battery of tests which included: maximum hand grip ($F_{max}$HG), standing long jump (LJ), number of sit ups (ABD), Illinois agility test ($IA_{test}$), thirty meters sprint running (30m), 300 yards shuttle run ($ShR_{300}$) and Cooper running test (CT). The results were analysed by descriptive statistics and connection between MC and BFA was confirmed by Pearson correlation analysis. The results showed that there are highly statistically significant correlations between MC and BFA results. PMS was proved to have the largest positive impact on all the tested physical abilities, whereas the higher BW, BMI, BFM and PBF values could be observed as significantly negative to BFA. Likewise, it was demonstrated that BH and SMM have a positive influence only on $F_{max}$HG results, while correlations were not observed regarding the other tested fitness abilities. The research leads to a conclusion that higher BW to the expense of fat mass could have a considerably negative effect on physical fitness of the police officers.

**Key words**: police, morphological characteristics, physical abilities

## INTRODUCTION

Police work is among extremely stressful and high risk occupations, thus bearing a possibility of ill effects to general health and professional abilities throughout the career.[3]One of the diagnostic indicators of negative trends of the influence of the working environment to police officers' professional-working abilities is the body structure.[4] The

1 This 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 projects 2015–2019.
2 radivoje.jankovic@kpa.edu.rs
3 Sörensen, L. *et al.* (2000). Physical activity, fitness and body composition of Finnish police officers: a 15-year follow-up study. *Occupational Medicine*, 50(1), 3–10.
4 Dopsaj, M., Vuković, M. (2015).Prevalenca indeksa telesne mase kod pripadnika MUP-a Republike Srbije – pilot istraživanje.*Bezbednost*, 57(3), 28–48.

second factor related to health, but bearing the immediate impact to the police work being performed efficiently, are the physical abilities. Statistically significant correlation between the level of physical fitness and the police officers' health, as well as between physical readiness and efficiency in performing a part of the police work were determined[5].

The area defining the body shape and constitution as basic morphological characteristics defining it is called anthropometric space. Body height (BN) and body mass (BM) are elementary morphological characteristics determined in the process of selection for police work in Serbia.[6] The value obtained on the basis of these data is body-mass index (BMI), which along with BW may indicate undernourishment. Furthermore, BM and BMI are greatly adaptable characteristics, meaning they are susceptible to changes and directly related to life style and different forms of exercise.[7]High BMI value may indicate potentially deteriorated health status, decline of general and specific endurance and increase of cardiovascular disease risk.[8] However, BMI does not provide an insight in the state of overall fat or distribution of the fat in certain body parts and which may vary greatly within the normal body mass index values. To gain the insight to the examinees' morphological characteristics (enabled today by modern technologies), along with the above mentioned, it is necessary to observe the amount of fat and muscular tissue and their percentage in relations to the body mass.[9]

In an earlier research, a correlation between physical abilities and BMI was determined. It was observed that PCT test scores of police officers is in relation to BMI and the number of hours of physical exercise invested.[10] It was also determined that fitness program may influence on BW and BMI decrease, as well as that the ceasing to actively exercise negatively impacts the cardiovascular fitness and, with it, the afore mentioned morphological characteristics.[11] However, another research conducted by Jackson & Wilson showed that BMI were not significantly independently associated with satisfactory GeNTOC performance in the way that might be expected.[12] The research demonstrated that over 76% of candidates passed the GeNTOC successfully. However, over 42% of them were overweight, and a further 7% were obese. The low number of candidates being screened out by this tool and the high percentage of those passing despite being overweight or obese poses a concern as the usefulness of a screening tool must be questioned if it screens out around 25% of candidates, while a significant proportion of those who pass

5 Copay, A., Charles, M. (1998).Police academy fitness training at the Police Training Institute, University of Illinois.*Policing: An International Journal of Police Strategies & Management.* 21(3), 416–431; Sörensen, L. *et al.*, *op. cit.*, 3–10; Strating, M. *et al.* (2010). A job-related fitness test for the Dutch police. *Occupational Medicine*, T. 60.

6 Dopsaj, M. *et al.* (2005).Dijagnostika stanja indeksa telesne mase studenata Policijske akademije. *Sportska medicina*, 5(4), 180–191; Janković, R. *et al.* (2008).Trend promene osnovnih antropometrijskih karakteristika studenata Kriminalističko-policijske akademije u toku studija.*Nauka – bezbednost – policija*,13(2), 137–152.

7 Bonneau, J., Brown, J. (1995). Physical ability, fitness and police work. *Journal of Clinical Forensic Medicine.* 2, 157–164.

8 Sörensen, L. *et al.*, *op. cit.*, 3–10.

9 Akpinar, E. *et al.* (2007). Which is the best anthropometric technique to identify obesity: body mass index, waist circumference or waist-hip ratio? *Collegium Antropologicum*, 31(2), 387–393; Dimitrijević, R. *et al.* (2012).Strukturni pokazatelji komponenti masnog tkiva kod studentkinja Kriminalističko-policijske akademije.*Bezbednost*, 54(3), 62–85.

10 Strating, M. et al, *op. cit.*, T. 60.

11 Rossomanno, I. *et al.* (2012). 6-Month Supervised Employer-Based Minimal Exercise Program for Police Officers Improves Fitness. *Journal of Strength and Conditioning Research*. 26(9), 2338–2344.

12 Jackson, C. A., Wilson, D. (2013). The Gender-Neutral Timed Obstacle Course: a valid test of police fitness? *Occupational Medicine*. 63, 479–484.

are overweight. This leads to a conclusion that BMI can be unreliable in the categorization of obesity, especially in individuals and occupations with extreme or high levels of muscular density.

Today, modern technology enables us to measure body structure more precisely and in an effective and fast way. The aim of this research is to help define the influence of muscular mass and fat mass to physical abilities; namely, to determine a more precise correlation between body structure and basic fitness abilities of police officers.

# METHOD

### Subjects

74 men of the average age of 28.5±6.2 participated in this research, 19 of them were the members of Special Anti-Terrorist Unit (SAU), 27 were general duties police officers (GDPO) and 28 the Academy of Criminalistic and Police Studies students (STUD) that accomplished all three levels of Specialized physical education (SPE) subject. The rest of the examinees (SAU and GDPO) were authorised persons who had received educational treatment adequate for police work.

### Procedures

Morphological characteristics were measured at the Faculty of Sport and Physical Education in Belgrade, and multichannel body structure analyser InBody 720 was used. The following morphological characteristics were observed: body height (BH), body mass (BM), body mass index (BMI), body fat mass (BFM), skeletal muscle mass (SMM), percentage of body fat (PBF) and percentage of skeletal muscle (PSM). The measurement was conducted with standard procedure[13]and the testing of motor abilities was realised in basic physical abilities (BPA) laboratory at ACPS. BFA were determined by a battery of tests which included: maximum hand grip ($F_{max}$HG), standing long jump (LJ), number of sit ups (ABD), Illinois agility test ($IA_{test}$), thirty meters sprint running (30m), 300 yards shuttle run ($ShR_{300}$) and Cooper running test (CT). All the measurements were realised by applying standard metrological procedures.[14]

### Statistical analysis

In the first step of data analysis, a descriptive statistical analysis was used which determined the measurements of central tendency and dispersion of the results: the average (Mean), standard deviation (SD) minimal and maximum value (Min, Max). The homogeneousness was defined by measurements defining the skew and kurt in relations to the Gauss curve. In the further process of the analysis of the results of causality assessment between the observed trends, namely the correlation between morphological characteristics and BFA, *the Pearson correlation* was applied.[15] The level of statistical significance was defined in the 95%, namely, $p < 0.05$ correlation. For all the statistical analysis the software program IBM SPSS Statistics 22, ID: 729327 was used.

13 Umičević, D., Dopsaj, M., Dimitrijević, R. (2012).Morphological Model of Members of the Cummunal Police of Belgrade.Proceeding book of: *International scientific conference Archibald Reiss Days* (pp. 1051–1064), Belgrade, Academy of Criminalistic and Police Studies.
14 Janković, R. (2015). *Validacija poligona kao testa za procenu specifične spretnosti kod policajaca.* Fakultet sporta i fizičkog vaspitanja .Beograd.
15 Hair J. *et al.*(1998).*Multivariate Data Analysis.* USA: Prentice – Hall, Inc.

## RESULTS

Table 1 shows the basic results of the descriptive statistics, while the Table 2 displays the results of correlation analysis which determined the connection between morphological characteristics and basic motor skills of the tested population.

*Table 1 Results of the descriptive statistics*

| | Mean | SD | Min | Max | Skew | Kurt |
|---|---|---|---|---|---|---|
| BH (cm) | 181.34 | 5.39 | 166.1 | 196.5 | -0.002 | 0.986 |
| BM (kg) | 86.45 | 10.14 | 66.0 | 106.4 | -0.165 | -0.470 |
| BMI (kg/m$^2$) | 26.28 | 2.81 | 19.0 | 32.9 | 0.072 | 0.585 |
| BFM (kg) | 15.26 | 6.86 | 5.2 | 35.1 | 0.860 | 0.473 |
| PBF (%) | 17.24 | 6.36 | 7.6 | 34.4 | 0.725 | 0.099 |
| SMM (kg) | 40.63 | 4.11 | 33.6 | 52.1 | 0.486 | -0.060 |
| PBM (%) | 47.25 | 3.93 | 37.3 | 54.5 | -0.562 | -0.190 |
| $F_{max}$HG (DaN) | 53.10 | 6.32 | 37.8 | 75.3 | 0.251 | 1.334 |
| LJ (cm) | 224.43 | 19.14 | 165 | 267 | -0.951 | 1.768 |
| ABD (No) | 26.39 | 4.80 | 13 | 33 | -1.217 | 1.066 |
| $IA_{test}$ (sec) | 19.05 | 1.40 | 16.78 | 24.76 | 1.053 | 2.673 |
| 30m (sec) | 4.64 | 0.24 | 4.17 | 5.35 | 0.633 | 0.314 |
| $ShR_{300}$ (sec) | 66.47 | 5.32 | 57.8 | 86.7 | 1.477 | 2.961 |
| CT (m) | 2517.19 | 363.37 | 1800 | 3600 | 0.053 | 0.086 |

*Table 2 Results of the Pearson correlation between morphological characteristics and fitness abilities*

| | $F_{max}$HG | LJ | ABD | $IA_{test}$ | 30m | ShR300 | CT |
|---|---|---|---|---|---|---|---|
| BH | **0.346**$^{**}$ | -0.063 | -0.123 | 0.158 | 0.075 | 0.153 | -0.140 |
| | **0.003** | 0.593 | 0.296 | 0.180 | 0.525 | 0.194 | 0.235 |
| BM | 0.187 | **-0.415**$^{**}$ | **-0.267**$^{*}$ | 0.207 | **0.382**$^{**}$ | **0.405**$^{**}$ | **-0.355**$^{**}$ |
| | 0.110 | **0.000** | **0.021** | 0.076 | **0.001** | **0.000** | **0.002** |
| BMI | 0.005 | **-0.422**$^{**}$ | **-0.235**$^{*}$ | 0.155 | **0.391**$^{**}$ | **0.373**$^{**}$ | **-0.327**$^{**}$ |
| | 0.963 | **0.000** | **0.044** | 0.189 | **0.001** | **0.001** | **0.004** |
| BFM | **-0.241**$^{*}$ | **-0.661**$^{**}$ | **-0.564**$^{**}$ | **0.474**$^{**}$ | **0.601**$^{**}$ | **0.644**$^{**}$ | **-0.617**$^{**}$ |
| | **0.039** | **0.000** | **0.000** | **0.000** | **0.000** | **0.000** | **0.000** |
| PBF | **-0.318**$^{**}$ | **-0.665**$^{**}$ | **-0.575**$^{**}$ | **0.507**$^{**}$ | **0.595**$^{**}$ | **0.650**$^{**}$ | **-0.632**$^{**}$ |
| | **0.006** | **0.000** | **0.000** | **0.000** | **0.000** | **0.000** | **0.000** |
| SMM | **0.484**$^{**}$ | 0.042 | 0.165 | -0.194 | -0.036 | -0.075 | 0.118 |
| | **0.000** | 0.720 | 0.160 | 0.098 | 0.761 | 0.526 | 0.316 |
| PSM | **0.295**$^{*}$ | **0.626**$^{**}$ | **0.546**$^{**}$ | **-0.507**$^{**}$ | **-0.563**$^{**}$ | **-0.632**$^{**}$ | **0.620**$^{**}$ |
| | **0.011** | **0.000** | **0.000** | **0.000** | **0.000** | **0.000** | **0.000** |

**Correlation is significant at the 0.01 level (2-tailed)

* Correlation is significant at the 0.05 level (2-tailed)

# DISCUSSION

In general, the results have shown that there is a correlation between morphological characteristics and BFA. A high positive statistical connection of the results between all observed motor abilities and PSM was determined and the negative one with PBF. The results shown in Table 2 indicated that BM and BMI have no effect on $F_{max}$HG and$IA_{test}$. The least influence on BFA was displayed by TV and SMM which affected solely $F_{max}$HG. The highest positive correlation of the results was determined between PSM and $ShR_{300}$, LJ, CT (r = 0.632, r = 0.626, r = 0.620, p = 0.000, respectively). On the other hand, the largest negative effect of morphological characteristics to BFA was determined between PFM and LJ, $ShR_{300}$, CT (r = 0.665, r = 0.650, r = 0.632, p = 0.000, respectively), as well as between BFM and LJ, $ShR_{300}$, CT, 30m (r = 0.661, r = 0.644, r = 0.617, r = 0.601, p = 0.000, respectively).

Morphological characteristics, along with motor abilities, are a part of the selection process for police work, and the justification of including morphology lies in its correlation with physical abilities and health.[16]Except BFA, it was determined that morphological characteristics influence the speed and quality of acquiring judo techniques, as well as the specific part of police physical abilities.[17] Firearm handling is also a specific police activity. Anderson and Plecas attempted to conclude if the forearm size may influence the shooting precision.[18] Significant correlations were found only when the male and female results were analysed together. When the subjects were grouped according to the gender, neither the males' not females' results displayed any connection between shooting precision, morphological characteristics and motor abilities. Thus, the results of the research showed the difficulty of predicting the shooting efficiency from a short firearm based on the anthropometric characteristics.

Even though BMI may be unreliable in determining the obesity in persons with high muscle mass[19], our research found that that there is a correlation between high BMI and low results on police physical abilities assessment test results. An earlier research determined that the members of SAU when compared to GDPO show statistically significantly lower BFM and PBF, but higher PSM. Moreover, the study showed statistically significantly better results in fitness tests.[20] We may presume that high BMI is a consequence of high BFM, in other words, that based on the BMI the degree of the obese employed in the police may be identified.[21]Unfortunately, the earlier research pointed out that inadequate procedures and testing standards enable a certain number of overweighed and undertrained police officers to be admitted and to remain in police force, which is not only unprofessional, but also increases the risks of deterioration of health or existing health issues worsening.[22] High BW and BMI as a result of fat mass increase may jeopardize health status and basic fitness abilities. Moreover, reducing the level of basic motor skills which are required for the police work could consequently have a negative influence on the professional and work efficiency of police officers.[23] Hence, it is of extreme importance to adequately define the ways of assessing morphological characteristics

16 Arvey, R. *et al.* (1992). Development of physical ability tests for police officers. *Journal of Applied Psychology*. 77(6), 996–1009; Sörensen, L. *et al.*, *op. cit.*, 3–10.
17 Blagojević, M. (1996).*Uticaj morfoloških i motoričkih karakteristika policajaca na efikasnost džudo tehnika*. Beograd: Kaligraf.
18 Anderson, S. G., Plecas, D. (2000). Predicting shooting scores from physical performance data.*Policing: An International Journal of Police Strategies & Management*. 23(4), 525–537.
19 Bonneau, J., Brown, J., *op. cit.*, 157–164.
20 Janković, R., *op. cit.*
21 Jackson, C. A., Wilson, D., *op. cit.*, 479–484.
22 Kales, S. N. *et al.* .(1999) Correlates of body mass index in hazardous materials fire-fighters. *Journal of Occupational and Environmental Medicine*, 41(7), 589–595; Sörensen, L. *et al.*, *op. cit.*, 3–10; Clark, S. *et al.* (2002). Association of body mass index and health status in fire-fighters. *Journal of Occupational and Environmental Medicine*, 44(10), 940–946.
23 Umičević, D., Dopsaj, M., Dimitrijević, R. ,*op. cit.*, 1051–1064.

and physical abilities of the police officers, and to precisely define the criteria that would enable high proficiency and good health status of police officer.[24] On the basis of this research results we may suggest that in the course of selection and assessment of morphological characteristics of police officers PBF and PMM should be used as the data with the highest correlation with fitness abilities. Furthermore, by determining PBF and PMM it will be possible to determine with certainty if high BMI is a result of muscle mass or fat mass.

## CONCLUSION

Morphological characteristics may be an indicator of health status, life style habits and the level of physical readiness. The most observed ones are BW and BMI, whose increase may indicate a potentially bad health status and decrease in work abilities. The results of our research confirmed the correlation of morphological characteristics and BFA of police officers. However, a higher negative influence on BFA was displayed by PBF and BFM whereas PSM is shown to positively correlate with all displayed tested BFA. The results determined that BH has no effect on BFS, except on $F_{max}$HG, so we may conclude that it could be a consequence of higher SMM and BW and also of displaying a higher maximum force. Modern technology used for assessment of body composition enable easy measure of body structure, so we may suggest that in the course of selection and monitoring of morphological characteristics of police officers PBF and PSM should be taken into account along with BW and BMI. That way it would be additionally defined if high BW or BMI is a consequence of training, namely high SMM, or of high BFM which may negatively influence health status and the professional abilities of police officers.

## REFERENCES

1. Akpinar, E., Bashan, I., Bozdemir, N., Saatci, E. (2007). Which is the best anthropometric technique to identify obesity: body mass index, waist circumference or waist-hip ratio? *Collegium Antropologicum*, 31(2), 387–393.
2. Anderson, S.G., Plecas, D. (2000). Predicting shooting scores from physical performance data. *Policing: An International Journal of Police Strategies & Management*. 2000, 23(4), 525–537.
3. Arvey, R., Landon, T., Nutting, S., Maxwell, S. (1992). Development of physical ability tests for police officers. *Journal of Applied Psychology*. 77(6), 996–1009.
4. Blagojević, M. (1996). *Uticaj morfoloških i motoričkih karakteristika policajaca na efikasnost džudo tehnika*. Beograd: Kaligraf.
5. Bonneau, J., Brown, J. (1995). Physical ability, fitness and police work. *Journal of Clinical Forensic Medicine.* 2, 157–164.
6. Boyce, R., Ciulla, S., Jones, G., Boone, E., Elliott, S., Combs, C. (2008). Muscular Strength and Body Composition Comparison between the Charlotte-Mecklenburg Fire and Police Departments. *International Journal of Exercise Science*. 1(3), 125–135.

24 Arvey, R. *et al.*, *op. cit.*, 996–1009; Boyce, R. *et al.* (2008). Muscular Strength and Body Composition Comparison between the Charlotte-Mecklenburg Fire and Police Departments. *International Journal of Exercise Science*. 1(3), 125–135.

7. Clark, S., Rene, A., Theurer, W.M., Marshall, M.(2002). Association of body mass index and health status in fire-fighters. *Journal of Occupational and Environmental Medicine*, 44(10), 940–946.

8. Copay, A., Charles, M. (1998). Police academy fitness training at the Police Training Institute, University of Illinois. *Policing: An International Journal of Police Strategies & Management.* 21(3), 416–431.

9. Dimitrijević, R., Vuković, M., Ćopić, N., Dopsaj, M. (2012). Strukturni pokazatelji komponenti masnog tkiva kod studentkinja Kriminalističko-policijske akademije. *Bezbednost*, 54(3), 62–85.

10. Dopsaj, M., Milošević, M., Vučković, G., Blagojević, M., Mudrić, R. (2005).Dijagnostika stanja indeksa telesne mase studenata Policijske akademije. *Sportska medicina*, 5(4), 180–191.

11. Dopsaj, M., Vuković, M. (2015). Prevalenca indeksa telesne mase kod pripadnika MUP-a Republike Srbije – pilot istraživanje. *Bezbednost*, 57(3), 28–48.

12. Hair J., Anderson R., Tatham R., Black W. (1998). *Multivariate Data Analysis*. USA: Prentice – Hall, Inc.

13. Jackson, C.A., Wilson, D. (2013). The Gender-Neutral Timed Obstacle Course: a valid test of police fitness? *Occupational Medicine*. 63, 479–484.

14. Janković, R. (2015). *Validacija poligona kao testa za procenu specifične spretnosti kod policajaca.*Fakultet sporta i fizičkog vaspitanja. Beograd.

15. Janković, R., Koropanovski, N., Vučković, G., Dimitrijević, R., Atanasov, D., Miljuš, D., Marinković, B., Ivanović, J., Blagojević, M., Dopsaj, M. (2008).Trend promene osnovnih antropometrijskih karakteristika studenata Kriminalističko-policijske akademije u toku studija. *Nauka – bezbednost – policija,* 13(2), 137–152.

16. Rossomanno, I., C., Herrick, E, J., Kirk, M. S., Kirka, E., P. (2012). 6-Month Supervised Employer-Based Minimal Exercise Program for Police Officers Improves Fitness. *Journal of Strength and Conditioning Research*. 26(9), 2338–2344.

17. Kales, S.N., Polyhronopoulos, G.N., Aldrich, J.M., Leitao, E.O., Christiani, D.C. (1999). Correlates of body mass index in hazardous materials fire-fighters. *Journal of Occupational and Environmental Medicine*, 41(7), 589–595.

18. Sörensen, L., Smolander, J., Louhevaara, V., Korhonene, O., Oja, P. (2000). Physical activity, fitness and body composition of Finnish police officers: a 15-year follow-up study. *Occupational Medicine*, 50(1), 3–10.

19. Strating, M., Bakker, R., Dijkstra, G., Lemmink, K., Groothoff, J.W. (2010). A job-related fitness test for the Dutch police. *Occupational Medicine*. T. 60

20. Umičević, D., Dopsaj, M., Dimitrijević, R. (2012). Morphological Model of Members of the Cummunal Police of Belgrade. Proceeding book of: *International scientific conference Archibald Reiss Days* (pp. 1051–1064), Belgrade, Academy of Criminalistic and Police Studies

# CHANGES IN INDICATORS OF MUSCLE FORCE IN FEMALE STUDENTS OF THE ACADEMY OF CRIMINALISTIC AND POLICE STUDIES[1]

**Raša Dimitrijević**[2]
The Academy of Criminalistic and Police Studies, Belgrade, Serbia
Tutor in the Department for tutorials and security

**Abstract:** Certain level of muscular contractile properties expression, and therefore the maximum isometric force, is of great importance for efficient work of the police. The aim of the research was directed to determination of changes in different indicators of muscle force in female students of Academy of Criminalistic and Police Studies. The total sample consisted of 218 subjects divided in four groups: 83 students of the 1st (I YR), 53 students of the 2nd (II YR), 50 students of the 3rd (III YR) and 32 students of the 4th year (IV YR) of study. Muscle forces assessment included testing of maximal isometric force of the left (FmaxLH) and right hand finger flexors (FmaxRH), back (FmaxBE) and leg (FmaxLE) extensor muscles. The standard battery of tests was used provided by the curriculum of Specialized physical education (SPE). The existence of differences was determined by MANOVA and Bonferroni post-hoc test. MANOVA results showed statistically significant differences in all variables at the level of F = 21.279, p = 0.000 for FmaxLH, F = 18.384, p = 0.000 for FmaxRH, F = 22.376, p = 0.000 for FmaxBE and F = 24,337 and p = 0.000 for FmaxLE. Statistically significant differences between groups were found in all the monitored variables. For the variables FmaxLH and FmaxRH there is a constant increase from I to IV YR. For the variables FmaxBE and FmaxLE the lowest level of force was found in the I YR, the highest was in the students of II YR, declines in III YR and again increases in IV YR. It can be concluded that there is no general regularity in the increase of muscle force level between observed groups. These findings are largely attributable to the conception of the SPE subject, total number of teaching hours and mode of basic motor status assessment.

**Key words**: Specialized physical education, isometric force, female students, police

## INTRODUCTION

The structure of policing is varied, complex and includes adequate levels of development of the different individual skills and characteristics.[3, 4] The level of motor abilities is associated with the efficient work of the police, and also there is a statistically significant correlation be-

1 This 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 projects 2015-2019.
2 *rasa_flok@yahoo.com*
3 Anderson, G., Plecas, D., Segger, T. (2001). Police officer physical ability testing. An International Journal of Police Strategies & Management, 24(1): 8-31.
4 Strating, M., Bakker, R., Dijkstra, G., Lemmink, K., Groothoff, J.W. (2010). A job-related fitness test for the Dutch police. Occupational Medicine, 60: 255–260.

tween the level of physical fitness and health in police officers.[5, 6] The initial phase of the police officers career represents the selection process and then, the period of professional training. One of the parameters in the selection process for police work is testing of the motor abilities level which aims at the most capable candidates.[7, 8, 9] After selection, it is necessary to further control and develop motor abilities. Their inadequate level can be a limiting factor during the training and in the performance of work tasks, lead to decreased work productivity, injuries, long-term incapacity for work, cause loss of human resources and huge economic costs.[10] These characteristics in the performance of police duties are further complicated by the gender structure and the trend of increasing number of women in police organizations.[11] The stated reasons impose the need for new studies, aimed at finding adequate models to improve the working skills, regarding the specific features of the women population in the police force. In this sense, it is necessary to develop and improve the processes of selection, training, and control of existing levels of various abilities during education and professional career.[12, 13, 14]

One of the segments in the education of the Academy of Criminalistic and Police Studies (ACPS) students is the subject of Specialized physical education (SPE) aimed at achieving certain levels of general and specific motor abilities. Defining SPE course educational and training process derives from the need to transform the student's motor abilities, with the aim of their development in accordance with the requirements for the employees of the Ministry of Internal Affairs (MIA).[15, 16] The specificity of professional duties requires that police officers, compared to the average citizen population, must have a higher level of motor abilities. One of the ways to ensure the necessary motor abilities level is a criterion for the ACPS enrollment, and the realization of norms that are defined in accordance with the projected needs of effective coping with SPE subject. The enrollment criteria provide the initial applicants motor abilities level above the 33.33 percentile (‰) in relation to the average Republic of Serbia (RS) civil population. The standards for the basic-motor abilities (BMA) assessment in the SPE subjects predict that after graduation, each of the evaluated motor ability is on a minimum level of 66.66‰ of the RS average civil population distribution, as the standard of the future professional working environment.

A certain level of muscular contractile properties expression, and therefore the maximum isometric force of the back and leg extensors and hand flexors, regardless of whether in ab-

5 Sorensen, L., Smolander, J., Louhevaara, V., Korhonen, O., Oja, P. (2000). Physical activity, fitness and body composition of Finnish police officers: a 15-year follow-up study. *Occupational Medicine*, 50(1): 3-10.
6 *Ibidem, 4.*
7 Copay, A., Charles, M. (1998). Police academy fitness training at the Police Training Institute, University of Illinois. Policing: *An International Journal of Police Strategies & Management,* 21(3): 416-431.
8 *Ibidem, 3.*
9 *Ibidem, 4.*
10 Lonsway, K. (2003). Tearing down the wall: problems with consistency, validity, and adverse inpact of physical agility testing in police selection. *Police Quarterly,* 6(3): 237–277.
11 Spasić, D. (2008). Žene u sistemu policijskog obrazovanja: stanje i perspektive ženskih ljudskih prava. *Temida*, 11(3): 41-61.
12 Dopsaj, M., Vučković, G. (2006). Pokazatelji maksimalne sile pregibača leve i desne šake u funkciji selekcionog kriterijuma za potrebe policije. *Sport Mont*, 4(10-11): 148-154.
13 Dopsaj, M., Blagojević, M., Vučković, G. (2007[a]). Normativno-selekcioni kriterijum za procenu bazično motoričkog statusa kandidata za prijem na studije Kriminalističko-policijske akademije u Beogradu. *Bezbednost*, 49(4): 166-183.
14 Vučković, G., Blagojević, M., Dopsaj, M. (2011). *Specijalno fizičko obrazovanje 2*. Kriminalističko-policijska akademija, Beograd.
15 Blagojević, M. (1996). *Uticaj morfoloških i motoričkih karakteristika policajaca na efikasnost džudo tehnika.* Kaligraf, Beograd.
16 Dopsaj, M., Milošević, M., Blagojević, M., Vučković, G. (2002). Evaluacija valjanosti testova za procenu kontraktilnog potencijala mišića ruku kod policajaca. *Bezbednost*, 44(3): 434-444.

solute or relative indicators, is of great importance for successful and efficient performance of police duties.[17, 18] The manifestation of the maximum muscle force in isometric conditions is a relatively stable characteristic of an individual motor space.[19] Caudal-dorsal part of the body with their muscle groups along with the back extensors, are the most important muscles of all major muscle groups, which are from the biomechanical point of view, primarily responsible for the quality of locomotion.[20], [21] A hand represents the basic human manipulation instrument, while the force of flexor finger muscles - grip force, is identified as a limiting factor in most of the activities performed with the cranial parts of a body.[22, 23, 24] The testing of muscular hand grip force in the police population is widespread.[25, 26, 27, 28] In the realization of police professional duties, finger flexor muscles play an important role from biomechanical, motor and manipulative aspects.[29, 30, 31] A large number of techniques applied in SPE subjects are realized by hands, for example grips for clothes in preparation for throw techniques, most of the levers, as well as techniques of pressure and pinching.[32, 33] Additionally, a variety of specific police skills within the use of the means of coercion are realized entirely by hands (handcuffing, use of baton and firearm), where a well-developed contractile properties of the finger flexor muscle have an important role in the efficiency of its application.[34, 35, 36, 37, 38] Overall, an adequate level of muscle force provides the basis for the expression of various forms of

17 *Ibidem, 15.*
18 *Ibidem, 12.*
19 Zatsiorsky, V.M., Kraemer, W.J. (2006). *Science and practice of strength training (Second Ed.).* Human Kinetics, Champaign, Illinois, USA.
20 Tyldesley, B., Grieve, J. (2000). *Muscles, nerves and movement: kinesiology in daily living.* Blackwell Science Ltd, Oxford, England.
21 Janković, R., Dimitrijević, R., Koropanovski, N., Vučković, G., Dopsaj, M. (2010). Promene maksimalne izometrijske sile opružača leđa i nogu kod studenata Kriminalističko-policijske akademije u toku prve tri godine studija. U: Stanković, R. (Ur.) XIV Međunarodni naučni skup FIS komunikacije 2010. u sportu, fizičkom vaspitanju i rekreaciji (p. 129-142), Niš: Fakultet sporta i fizičkog vaspitanja.
22 *Ibidem, 20.*
23 Dopsaj, M., Koropanovski, N., Vučković, G., Blagojević, M., Marinković, B., Miljuš, D. (2007[b]). Maximal isometric hand grip force in well-trained university students in Serbia: descriptive, functional and sexual dimorphic model. *Serbian Journal of Sports Sciences*, 1(4): 138-147.
24 Ivanovic, J., Koropanovski, N., Vuckovic, G., Jankovic, R., Miljus, D., Marinkovic, B., Atanasov, D., Blagojevic, M., Dopsaj, M. (2009). Functional dimorphism and characteristics considering maximal hand grip force in top level athletes in the Republic of Serbia. *Gazzetta Medica Italiana*, 168(5): 297-310.
25 *Ibidem, 7.*
26 Anderson, G., Plecas, D. (2000). Predicting shooting scores from physical performance data. *An International Journal of Police Strategies & Management,* 23(4): 525-537.
27 *Ibidem, 3.*
28 Dopsaj, M., Vučković, G., Milojković, B., Subošić, D., Eminović, F. (2012). Hand grip scaling in defining risk factors when using authorized physical force. *Facta universitatis - series: Physical Education and Sport*, 10(3): 169-181.
29 Blagojević, M. (2003). *Uticaj nastave specijalnog fizičkog obrazovanja na promene morfoloških i motoričkih karakteristika studenata Policijske akademije*. Energograf, Beograd.
30 *Ibidem, 12.*
31 Leyk, D., Gorges, W., Ridder, D., Wunderlich, M., Ruther, T., Sievert, A., Essfeld, D. (2007). Handgrip strength of young men, women and highly trained female athletes. *European Journal of Applied Physiology*, 99: 415-421.
32 Milošević, M., Zulić, M., Božić, S. (2001). *Specijalno fizičko obrazovanje.* Grmeč, Beograd.
33 Blagojević, M., Dopsaj, M., Vučković, G. (2006). *Specijalno fizičko obrazovanje I*. Policijska akademija, Beograd.
34 *Ibidem, 7.*
35 *Ibidem, 26.*
36 *Ibidem, 3.*
37 *Ibidem, 23.*
38 *Ibidem, 14.*

muscular strength.[39, 40, 41] The aim of the research was directed to determination of changes in different indicators of muscle force in female students of ACPS during all four years of study.

# METHODS

## The sample

The total sample consisted of 218 subjects divided in four groups: 83 students of the 1st (I YR), 53 students of the 2nd (II YR), 50 students of the 3rd (III YR) and 32 students of the 4th year (IV YR) of study. Basic anthropometric measures per group were as follows: body height (BH) = 169.25 ± 4.55cm, body weight (BW) = 62.91 ± 6.77kg and body mass index (BMI) = 21.59 ± 2.06kg/m$^2$ for the I YR, BH = 168.80 ± 5.46cm, BW = 63.38 ± 7.59kg and BMI = 22.22 ± 2.25 kg/m$^2$ for the II YR, BH = 169.84 ± 5.87cm, BW = 62.53 ± 6.60kg and BMI = 21.74 ± 2.19 kg/m$^2$ for the III YR and BH = 169.47 ± 5.60cm, BW = 61.37 ± 7.34kg and BMI = 21.36 ± 2.20 kg/m$^2$ for the IV YR. During the measurements period, all respondents were healthy, with no acute and chronic diseases and without injuries of the locomotors apparatus to influence the test results. Before testing, respondents were introduced with the object and purpose of the research. The research was conducted in accordance with the terms of "Declaration of Helsinki for recommendations guiding physicians in biomedical research involving human subjects" - (http://www.cirp.org/library/ethics/helsinki/), as well as with the permission of the Ethics Committee of the Faculty of sport and physical education, University of Belgrade.

## Testing procedure

All tests were performed in the Laboratory for assessing the basic physical abilities within the subjects of SPE at the ACPS in Belgrade. The testing of physical abilities was preceded by a standard 10-min running warm-up and 10-min active stretching. Following a detailed explanation and qualified demonstration of each test, respondents performed one practice trial followed by two consecutive experimental trials and the best result was used for further analysis. The rest periods between the consecutive trials and between two consecutive tests were 2 and 15 min, respectively. The maximal isometric force was measured by the tensiometric probe, by employing the hardware and software system for testing physical abilities - PAT 01 (Physical Ability Test 01), using the standardized measurement procedures.[42, 43, 44] The maximal isometric force of the left and right hand finger flexors (FmaxLH and FmaxRH) was measured by standardized "hand grip test" (Figure 1). The respondents were standing in the upright position and holding the measuring device in the natural posture alongside the body, while the other arm was resting alongside the body or the hand of the other arm was leaning against the thigh. The testing hand holding was approximately 10 cm away from the body. The participants were not allowed to move from the initial position during the test trial,

39 Jarić, S. (1997). *Biomehanika humane lokomocije sa biomehanikom sporta*. Beograd: Dosije.
40 Bohannon, R. (2001). Dynamometer measurements of hand grip strenght predict multiple outcomes. *Perceptual and Motor Skills*, 93: 323-328.
41 *Ibidem, 19.*
42 Dopsaj, M., Milošević, M., Blagojević, M. (2000). An analysis of the reliability and factorial validity of selected muscle force mechanical characteristics during isometric multi-joint test. 17th International Symposium of Biomechanics in Sport (pp. 146-149), Hong Kong: The Chinese University
43 *Ibidem, 21.*
44 Kolarević, D., Dimitrijević, R., Vučković, G., Koropanovski, N., Dopsaj, M. (2014). Relations between psychological characteristics and physical abilities in a sample of female police candidates. *The Open Sports Sciences Journal*, 7: 22-28.

nor could they lean the hand or the device against the thigh or another solid object.[45, 46, 47] the measurement of the maximal isometric force of the back extensors (FmaxBE) was carried by the "Isometric dead lift" test (Figure 2). The respondents were standing on the platform with chest facing the bar carrier and feet placed in a parallel position in the width of the hips. The bar was fixed to the tensiometric probe and platform. The arms and legs of the respondents were maximally stretched in the joints of the elbows and knees; the body was bent with chest protruding forward. After taking the correct position, the respondents performed the maximum contraction of the back muscles in an attempt of the body extension.[48, 49, 50] The measurement of maximal isometric force of the leg extensors (FmaxLE) was performed in the way that the respondents were standing on the platform with the back facing the carrier bar. The respondents took position so the bar was located under the muscles gluteus. At the signal of the teacher who was measuring results, the respondents exerted maximal isometric contraction of the leg extensor muscles in an attempt of movement vertically up (Figure 3).[51] The values of all measured muscle forces are expressed in kN.

***Figure 1.*** *Hand grip test*

***Figure 2.*** *Isometric dead lift*

***Figure 3.*** *Leg extension*

**Statistical analysis**

All data were analyzed using the descriptive statistics to calculate the basic parameters of central tendency: arithmetic mean (MEAN), standard deviation (SD), coefficient of variation (cV%), minimum (Min) and maximum (Max) values. The existence of a general difference of variability between the groups was determined by multivariate analysis of variance (MANOVA), while for the determination of partial difference between pairs of variables the Bonferroni post-hoc test was used. Statistical significance was defined at 95% probability, i.e., at $p < 0.05$ level.[52] All statistical analyses were done by the application of software package SPSS Statistics 17.0.

45 *Ibidem, 12.*
46 Dimitrijević, R., Koropanovski, N., Dopsaj, M., Vučković, G., Janković, R. (2014). The influence of different physical education programs on police students physical abilities. *Policing: an international Journal of Police Strategies and Management*, 37(4): 794-808.
47 *Ibidem, 44.*
48 Dopsaj, M., Blagojević, M., Marinković, B., Miljuš, D., Vučković, G., Koropanovski, N., Ivanović, J., Atansov, D., Janković, R. (2010). *Modelne karakteristike antropometrijskih pokazatelja i bazično-motoričkih sposobnosti (BMS) zdravih i utreniranih mladih osoba oba pola – populacioni pokazatelji Republike Srbije.* Kriminalističko-policijska akademija, Beograd.
49 *Ibidem, 21.*
50 *Ibidem, 46.*
51 *Ibidem, 48.*
52 Hair, J., Anderson, R., Tatham, R., Black, W. (1998). *Multivariate Data Analysis (Fifth Ed.)*. Prentice – Hall, Inc., USA.

# RESULTS

The results of muscular forces descriptive indicators for all groups of the ACPS student are shown in Table 1.

*Table 1 Results of descriptive statistics*

| Variable | MEAN | SD | cV% | Min | Max |
|---|---|---|---|---|---|
| I YR | | | | | |
| FmaxLH | 27.03 | 5.65 | 20.78 | 13.80 | 46.90 |
| FmaxRH | 29.12 | 5.49 | 18.73 | 16.50 | 46.30 |
| FmaxBE | 87.63 | 15.97 | 18.11 | 26.50 | 125.10 |
| FmaxLE | 81.14 | 15.23 | 18.66 | 47.50 | 120.50 |
| II YR | | | | | |
| FmaxLH | 29.35 | 4.16 | 14.17 | 21.20 | 36.80 |
| FmaxRH | 31.37 | 4.65 | 14.81 | 21.90 | 41.40 |
| FmaxBE | 108.36 | 18.41 | 16.99 | 63.30 | 147.20 |
| FmaxLE | 101.82 | 18.96 | 18.62 | 54.50 | 145.60 |
| III YR | | | | | |
| FmaxLH | 32.23 | 4.02 | 12.48 | 26.20 | 44.90 |
| FmaxRH | 34.37 | 4.30 | 12.52 | 27.20 | 44.20 |
| FmaxBE | 97.26 | 10.20 | 10.49 | 80.90 | 120.10 |
| FmaxLE | 92.22 | 9.87 | 10.70 | 78.40 | 115.40 |
| IV YR | | | | | |
| FmaxLH | 33.71 | 3.99 | 11.84 | 26.10 | 43.50 |
| FmaxRH | 35.32 | 4.64 | 13.14 | 28.70 | 46.60 |
| FmaxBE | 102.90 | 12.64 | 12.28 | 73.60 | 137.30 |
| FmaxLE | 99.61 | 14.39 | 14.45 | 74.10 | 129.00 |

The results of the differences in the indicators of muscular forces between groups in a function of years of study are shown in Table 2. The results of the difference are shown in the general and partial level.

*Table 2 Results of MANOVA*

| General level | | | | | | |
|---|---|---|---|---|---|---|
| Effect | | Value | F | Hypothesis df | Error df | Sig. |
| Year of study | Wilks' Lambda | .270 | 12.612 | 27.000 | 602.269 | .000 |
| Partial level | | | | | | |
| Source | Dependent Variable | Type III Sum of Squares | df | Mean Square | F | Sig. |
| Year of study | FmaxLH | 1433.222 | 3 | 477.741 | 21.279 | .000 |
| | FmaxRH | 1331.934 | 3 | 443.978 | 18.384 | .000 |
| | FmaxBE | 15240.048 | 3 | 5080.016 | 22.376 | .000 |
| | FmaxLE | 16687.349 | 3 | 5562.450 | 24.337 | .000 |

Table 3 presents the results of the Bonferroni post-hoc test, showing statistically significant differences of the observed muscular forces between groups, defined at 95% probability ($p < 0.05$).

*Table 3 Results of Bonferroni post-hoc test*

| Variable | | II YR | III YR | IV YR |
|---|---|---|---|---|
| FmaxLH | I YR | .034* | .000*** | .000*** |
| | II YR | | .014* | .000*** |
| | III YR | | | 1.000 |
| FmaxRH | I YR | .059 | .000*** | .000*** |
| | II YR | | .013* | .002** |
| | III YR | | | 1.000 |
| FmaxBE | I YR | .000*** | .003** | .000*** |
| | II YR | | .001** | .640 |
| | III YR | | | .600 |
| FmaxLE | I YR | .000*** | .000*** | .000*** |
| | II YR | | .009** | 1.000 |
| | III YR | | | .192 |
| ** $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$* | | | | |

## DISCUSSION

The statistically significant differences between students of different years of study were found both on general and partial levels (Table 2). The results of Bonfferoni test showed a great number of statistically significant difference between the groups (Table 3). For the variable FmaxLH differences were not determined only between III YR and IV YR, while for the variable FmaxRH no differences were found between I YR and II YR, as well as between III YR and IV YR (Table 3). For the variables FmaxBE and FmaxLE the differences were not found between II YR and IV YR, as well as between III YR and IV YR (Table 3). From the results of descriptive statistics (Table 1), it can be observed that there is a constant increase in the level of force from first to fourth year of study for the variables FmaxLH and FmaxRH. For the variables FmaxBE and FmaxLE the level of force is the lowest among the students of the I YR, the highest in the II YR group, then decline in the III YR group and finally increases in the IV YR students. In general, the levels of force for the all observed variables are the lowest in the I YR group, and then have an increasing trend. From the descriptive and Bonfferoni test results, it can be concluded that the IV YR students had significantly higher levels of force compared to the I YR for all monitored variables. However, a more complete picture can be obtained if the results of this research are compared with the results of previous studies in similar populations. Specifically, observed for the whole sample and according to the standards of Dopsaj et al. (2010)[53], the ACPS students can be classified into the following groups: FmaxLH - below the average force level, FmaxRH - low force level, FmaxBE - average force level and FmaxLE - below the average force level. A bit different image is obtained in classification of the IV YR students according to the same standards (Table 4), where the percentile distribution of the sample according to year of study is shown:

53 *Ibidem, 48.*

*Table 4 Classification in relation to the Republic of Serbia population*

| Variable | Percentile (‰) | | | | IV YR compared to RS |
|---|---|---|---|---|---|
| | I YR | II YR | III YR | IV YR | |
| FmaxLH | 5 | 10 | 30 | 40 | The average force level |
| FmaxRH | 2 | 5 | 20 | 30 | The average force level |
| FmaxBE | 20 | 65 | 35 | 50 | The average force level |
| FmaxLE | 15 | 50 | 25 | 40 | The average force level |
| ∑ | 10.50 | 32.50 | 27.50 | 40.00 | |

Based on the results shown in Table 3, it can be concluded that the total level of force in the I YR group is below 33.33‰ compared to the RS trained young population, i.e. slightly above the 10‰. The reasons may be multiple. First, measurements of muscular force for the purpose of this research were performed during the winter semester in which the I YR students do not have SPE classes. Second, according to the research results of Koropanovski et al. (2015)[54], in the selection process for the ACPS enrollment, there was a greater pass of candidates with a lower level of motor abilities. Moreover, with the fact that selection of students for the ACPS was carried out from the general youth population, the negative trend of motor abilities initial level could be the consequence of: physical activity reduction in children and adolescents as a result of modern life[55]; teaching programs at lower levels of education with fewer classes of physical education; the fact that the system of sport and school sport in the RS, due to the overall financial situation, provides fewer opportunities to the secondary school population.

From previously stated, it can be concluded that there is no general trend in force level increasing between the observed groups. These findings could be largely attributable to the concept of the SPE subject and a total fund of teaching classes during studies. In fact, Dimitrijevic et al. (2014)[56] found that the total number of SPE subjects classes, which were reduced from the initial 1085 to current 180 has statistically significant influence on the levels of motor abilities expression. The first modified SPE curriculum with a total fund of 999 classes was realized in the period from 2000 until 2006, when female students started to enroll the Police Academy. Both the initial and the modified SPE programs were implemented during all four years of study while the current SPE program is implemented only in three out of eight semesters: in the summer semester of the first, the winter semester of the second, and finally in the summer semester of the third year of study. In relation to the research of Vuckovic (2007)[57], the force levels observed in this study are for the all variables on a lower level compared to female students who have attended classes according to the modified program. Additionally, it should be noted that students have the opportunity for the partial motor abilities level examination on the SPE colloquium, which gives them a chance to reach the prescribed norms for different motor skills several times during the year. More specifically, the students have the opportunity not to meet the standards for all tests at once, but to pass "only what is left" on the next colloquium. It is evident that the current SPE teaching program, with a small number of classes and the long-time gaps, has an undesirable effect on the motor abilities expression, i.e.

54 Koropanovski, N., Janković, R., Dimitrijević, R. (2015). Trend promena inicijalnog nivoa motoričkih sposobnosti studentkinja Policijske akademije. U: Kasum, G., Mudrić, M. (Ur.) Međunarodna naučna konferencija, Efekti primene fizičke aktivnosti na antropološki status dece, omladine i odraslih (str. 431-442), Beograd: Fakultet sporta i fizičkog vaspitanja.

55 Hass, C., Feigenbaum, M., Franklin, B. (2001). Perception of resistance training for healthy populations. *Sports Medicine*, 31(14): 953-964.

56 *Ibidem, 46.*

57 Vučković, G. (2007). Uticaj morfoloških karakteristika i motoričkih sposobnosti na tačnost gađanja pištoljem kod žena - doktorska disertacija. *Godišnjak Fakulteta sporta i fizičkog vaspitanja*, 15:44-59.

the period of classes and testing are not a requirement for the continuous physical workout, why there is no permanent adaptation and stabilization in levels of muscle forces.

To avoid this negative trend, and in order to improve the quality of the selection and training process, it is essential to increase motor abilities elimination level on the entrance exam. After the selection and during the education, it is necessary to further develop students motor abilities level. However, it can be concluded that the current fund of SPE is not sufficient for the achieving a stable state of muscle force at a minimum of 66.66‰ compared to the RS trained young population. Therefore, it is necessary to suggest an increase in SPE total fund classes, which would be implemented during all eight semesters of study. This would provide continuous, planned and systematic educational and training impact throughout the whole period of schooling. There is also a need for the implementation of teaching/training programs in swimming, snow skiing, morning exercise, etc., which were an integral parts of initial and modified SPE curriculums, as well as other exercise contents within the obligatory extracurricular activities.

## CONCLUSION

The aim of this research was focused on changes in the levels of different muscle forces in the ACPS female students during all four years of schooling. The research was conducted on a sample of 218 students divided into four groups. A large number of statistically significant differences, at the general and partial level, was found between groups for all of the observed variables. It can be concluded that the levels of maximal muscle force increase from the first to the final year of study, but their level does not meet predetermined SPE criteria in relation to the RS trained young population. The reasons are various: the present system of the ACPS entrance examination allows greater pass of the candidates with lower levels of motor abilities; SPE subjects are implemented in only three out of eight semesters during the four-year study; the current number of SPE teaching classes does not provide continuous, systematic physical activities with the desired intensity and scope of exercises; the actual method of SPE colloquiums allows students partial examinations with long intervals between testing. The above reasons stimulate motives for intentional preparing for partial exercise, and not practical exercise based on a conscious professional motive.

Based on these results, and the fact that muscular force is the basis for the expression of various indicators of muscle strength, there is a need for the new researches that will determine the status and trends of changes in other motor abilities of the ACPS students during the educational process. Thus obtained results, can be used for a more detailed analysis of the effectiveness of the current SPE programs. The final goal of further researches should be related to the improvement of educational and training processes in the field of basic motor abilities, as well as the basis for the setting of a long-term strategy for the development and improvement of teaching programs on SPE subjects.

## LITERATURE

1. Anderson, G., Plecas, D. (2000). Predicting shooting scores from physical performance data. *An International Journal of Police Strategies & Management,* 23(4): 525-537.
2. Anderson, G., Plecas, D., Segger, T. (2001). Police officer physical ability testing. *An International Journal of Police Strategies & Management,* 24(1): 8-31.

3. Blagojević, M. (1996). *Uticaj morfoloških i motoričkih karakteristika policajaca na efikasnost džudo tehnika.* Kaligraf, Beograd.

4. Blagojević, M. (2003). *Uticaj nastave specijalnog fizičkog obrazovanja na promene morfoloških i motoričkih karakteristika studenata Policijske akademije*. Energograf, Beograd.

5. Blagojević, M., Dopsaj, M., Vučković, G. (2006). *Specijalno fizičko obrazovanje I*. Policijska akademija, Beograd.

6. Bohannon, R. (2001). Dynamometer measurements of hand grip strength predict multiple outcomes. *Perceptual and Motor Skills*, 93: 323-328.

7. Copay, A., Charles, M. (1998). Police academy fitness training at the Police Training Institute, University of Illinois. Policing: *An International Journal of Police Strategies & Management,* 21(3): 416-431.

8. Dimitrijević, R., Koropanovski, N., Dopsaj, M., Vučković, G., Janković, R. (2014). The influence of different physical education programs on police students physical abilities. *Policing: An International Journal of Police Strategies and Management*, 37(4): 794-808.

9. Dopsaj, M., Milošević, M., Blagojević, M. (2000). An analysis of the reliability and factorial validity of selected muscle force mechanical characteristics during isometric multi-joint test. 17th International Symposium of Biomechanics in Sport (pp. 146-149), Hong Kong: The Chinese University.

10. Dopsaj, M., Milošević, M., Blagojević, M., Vučković, G. (2002). Evaluacija valjanosti testova za procenu kontraktilnog potencijala mišića ruku kod policajaca. *Bezbednost*, 44(3): 434-444.

11. Dopsaj, M., Vučković, G. (2006). Pokazatelji maksimalne sile pregibača leve i desne šake u funkciji selekcionog kriterijuma za potrebe policije. *Sport Mont*, 4(10-11): 148-154.

12. Dopsaj, M., Blagojević, M., Vučković, G. (2007[a]). Normativno-selekcioni kriterijum za procenu bazično motoričkog statusa kandidata za prijem na studije Kriminalističko-policijske akademije u Beogradu. *Bezbednost*, 49(4): 166-183.

13. Dopsaj, M., Koropanovski, N., Vučković, G., Blagojević, M., Marinković, B., Miljuš, D. (2007[b]). Maximal isometric hand grip force in well-trained university students in Serbia: descriptive, functional and sexual dimorphic model. *Serbian Journal of Sports Sciences*, 1(4): 138-147.

14. Dopsaj, M., Blagojević, M., Marinković, B., Miljuš, D., Vučković, G., Koropanovski, N., Ivanović, J., Atansov, D., Janković, R. (2010). *Modelne karakteristike antropometrijskih pokazatelja i bazično-motoričkih sposobnosti (BMS) zdravih i utreniranih mladih osoba oba pola – populacioni pokazatelji Republike Srbije.* Kriminalističko-policijska akademija, Beograd.

15. Dopsaj, M., Vučković, G., Milojković, B., Subošić, D., Eminović, F. (2012). Hand grip scaling in defining risk factors when using authorized physical force. *Facta universitatis - series: Physical Education and Sport*, 10(3): 169-181.

16. Hair, J., Anderson, R., Tatham, R., Black, W. (1998). *Multivariate Data Analysis (Fifth Ed.)*. Prentice – Hall, Inc., USA.

17. Hass, C., Feigenbaum, M., Franklin, B. (2001). Perception of resistance training for healthy populations. *Sports Medicine*, 31(14): 953-964.

18. Ivanovic, J., Koropanovski, N., Vuckovic, G., Jankovic, R., Miljus, D., Marinkovic, B., Atanasov, D., Blagojevic, M., Dopsaj, M. (2009). Functional dimorphism and characteristics considering maximal hand grip force in top level athletes in the Republic of Serbia. *Gazzetta Medica Italiana*, 168(5): 297-310.

19. Janković, R., Dimitrijević, R., Koropanovski, N., Vučković, G., Dopsaj, M. (2010). Promene maksimalne izometrijske sile opružača leđa i nogu kod studenata Kriminalističko-policijske

akademije u toku prve tri godine studija. U: Stanković, R. (Ur.) XIV Međunarodni naučni skup FIS komunikacije 2010 u sportu, fizičkom vaspitanju i rekreaciji (str. 129-142), Niš: Fakultet sporta i fizičkog vaspitanja.

20. Jarić, S. (1997). *Biomehanika humane lokomocije sa biomehanikom sporta*. Beograd: Dosije.
21. Kolarević, D., Dimitrijević, R., Vučković, G., Koropanovski, N., Dopsaj, M. (2014). Relations between psychological characteristics and physical abilities in a sample of female police candidates. *The Open Sports Sciences Journal*, 7: 22-28.
22. Koropanovski, N., Janković, R., Dimitrijević, R. (2015). Trend promena inicijalnog nivoa motoričkih sposobnosti studentkinja Policijske akademije. U: Kasum, G., Mudrić, M. (Ur.) Međunarodna naučna konferencija, Efekti primene fizičke aktivnosti na antropološki status dece, omladine i odraslih (str. 431-442), Beograd: Fakultet sporta i fizičkog vaspitanja.
23. Leyk, D., Gorges, W., Ridder, D., Wunderlich, M., Ruther, T., Sievert, A., Essfeld, D. (2007). Hand-grip strength of young men, women and highly trained female athletes. *European Journal of Applied Physiology*, 99: 415-421.
24. Lonsway, K. (2003). Tearing down the wall: problems with consistency, validity, and adverse impact of physical agility testing in police selection. *Police Quarterly,* 6(3): 237–277.
25. Milošević, M., Zulić, M., Božić, S. (2001). *Specijalno fizičko obrazovanje.* Grmeč, Beograd.
26. Sorensen, L., Smolander, J., Louhevaara, V., Korhonen, O., Oja, P. (2000). Physical activity, fitness and body composition of Finnish police officers: a 15-year follow-up study. *Occupational Medicine*, 50(1): 3-10.
27. Spasić, D. (2008). Žene u sistemu policijskog obrazovanja: stanje i perspektive ženskih ljudskih prava. *Temida*, 11(3): 41-61.
28. Strating, M., Bakker, R., Dijkstra, G., Lemmink, K., Groothoff, J.W. (2010). A job-related fitness test for the Dutch police. *Occupational Medicine*, 60: 255–260.
29. Tyldesley, B., Grieve, J. (2000). *Muscles, nerves and movement: kinesiology in daily living.* Blackwell Science Ltd, Oxford, England.
30. Vučković, G. (2007). Uticaj morfoloških karakteristika i motoričkih sposobnosti na tačnost gađanja pištoljem kod žena - doktorska disertacija. *Godišnjak Fakulteta sporta i fizičkog vaspitanja*, 15:44-59.
31. Vučković, G., Blagojević, M., Dopsaj, M. (2011). *Specijalno fizičko obrazovanje 2*. Kriminalističko-policijska akademija, Beograd.
32. Zatsiorsky, V.M., Kraemer, W.J. (2006). *Science and practice of strength training (Second Ed.).* Human Kinetics, Champaign, Illinois, USA.

# EFFECTS OF TWELVE-WEEK TRAINING PROGRAM ON FITNESS LEVEL AND ANTHROPOMETRIC STATUS OF POLICE COLLEGE STUDENTS

**Velimir Jeknic, Milos Stojkovic**
Abu Dhabi Police College

**Abstract:** The aim was to determine the changes in fitness level and anthropometricstatusof Police College students occurred under the influence of twelve-week training program. Training process included 64 individual trainings. Sample consisted of 158 students. The first testing was performed at the beginning and another at the end of the training process, which lasted for 12 weeks. Motor abilities, repetitive strength, endurance and anthropometric were evaluated by the selected tests. The existence of the differences between initial and final results was determined by T-test, and statistical significance was defined at the level of $p<0.01$ for the variables weight, ratio of waist and height, the maximum number of push-ups and sit-upsin 60 seconds, running 2.4 km distance.

**Key words**: Training program, testing, anthropometric, strength, endurance

**Correspondence to:** Velimir Jeknic, Abu Dhabi Police College; e – mail address: velimirjeknic@yahoo.com

## INTRODUCTION

Dynamics and diversity of tasks that characterize the challenges of police work emphasize the importance of adequate physical preparation[1]. Physical fitness is an essential component of being prepared to do infrequent but often critical tasks, including pursuing fleeing subjects, close combat, handcuffing, use of firearms, as well as crowd control[2]. An adequate level of physical ability makes it possible to carry out professional tasks at appropriate speed, dexterity, strength, coordination, precision, with appropriate intensity and endurance[3]. Inability to perform physical aspects of police work may endanger public safety[4].

Members of police force often have a task to make fast adaptation from sedentary, passive positions and take action in a hostile environment[5]. From the routines of shift-work and uneventful patrol to physical responses and actions required in critical incidents, police officers must be physically capable of performing all occupational requirements successfully, and in a way which maximizes safety and security of all those concerned[6].

1 Dimitrijević, R., Koropanovski, N., Dopsaj, M., Vučković, G., Janković, R. (2014) The influence of different physical education programs on police students' physical abilities. Policing: An International Journal of Police Strategies & Management, 37(4): 794–808

2 Crawley, A., Sherman, R., Crawley, W., Cosio-Lima, L. (2016) Physical Fitness of Police Academy Cadets: Baseline Characteristics and Changes During a 16-Week Academy. Journal of Strength and Conditioning Research, 30(5): 1416–1424

3 Janković R. (2015) Validacija poligona kao testa za procenu specificne spretnosti kod policajaca. Fakultet sporta i fizickog vaspitanja, Doktorska disertacija. 4. str.

4 Bonneau, J., Brown, J. (1995) Physical ability, fitness and police work. Journal of clinical forensic medicine. 2(3): 157-164

5 Shell D. (2002) Law enforcement entrance-level physical training: Does it need a new approach? Sheriff, 54(4): 26–60

6 Anderson, S., Plecas, D., Segger, T. (2001) Police officer physical ability testing. Re-validating a selec-

Social and psychological demands related to police work, such as the pace of daily work, occupational responsibilities, and distressing situations, as well as factors such as poor diet and physical inactivity can initiate health problems and affect quality of life among police officers[7]. The routine physical demands of this job, such as riding in a patrol car and preparing paperwork, are often inadequate for maintaining necessary physical fitness to perform these infrequent but possibly lifesaving critical functions. Low levels of physical activity have been shown to promote increase in weight, body fat, and potential health issues[8]. Body mass increase caused by obesity can compromise this physical condition. Although policemen, in their early career, are considered more physically active than general population, studies indicate that police officers are more prone to being obese or having diseases related to obesity over time as a result of physical and psychological work requirements that are sometimes in conflict with maintenance of physical fitness[9]. This is why constant monitoring of anthropological status, from entering police academy as a student and during police officer career is a must.

Since the measure of central adiposity – waist-to-height ratio has been consistently shown to be more strongly related to several diseases or poor health outcomes than BMI in both genders[10], it will be used in this research.

As one of the safest cities in the world with very low crime rate[11,12,13], Abu Dhabi Police is trying to maintain that level of peace by educating high quality cadets at the Abu Dhabi Police College. Contrary to the opinion of Bykov O. from San Jose State University[14], who thinks that physical training should be completely removed from the police academy syllabus and that candidates should be responsible for gaining proper level of physical fitness in their own time, Abu Dhabi Police provides physical education classes 5 to 10 times per week to their cadets.

Tactical athletes, such as firefighters, military and police officers require speed, strength, agility, and endurance training for physical preparation of their future job[15]. Repetitive strength measures assess the ability to generate continuous or repetitive submaximal forces[16], which are essential during repeated muscle activation while controlling those resisting arrest, grappling, and handcuffing suspect.

Strength supports the ability of police personnel to safely perform critical emergency functions while fulfilling the local government's legal responsibility to deliver adequate pro-

tion criterion. Policing: An International Journal of Police Strategies & Management. 24(1): 8-31

7 Da Silva, CF., Soleman, Hernandez SS., Valdivia, Arancibia BA., Da Silva Castro, TL., GutierresFilho, PJB., Rudney Da Silva, R. (2014) Health-related quality of life and related factors of military police officers. Health and quality of life outcomes. 12: 60

8 Boyce, R., Ciulla, S., Jones, G., Boone, E., Ellito, S., Combs, C. (2008) Muscular strength and body composition comparison between the Charlotte-Mecklenburg fire and police departments. International Journal of Exercise Science. 1(3): 125 – 135

9 Da Silva, CF., Soleman, Hernandez SS., Valdivia, Arancibia BA., Da Silva, Castro TL., Gutierres, Filho PJB., Rudney, Da Silva, R. (2014) Anthropometric indicators of obesity in policemen: A systematic review of observational studies. International Journal of Occupational Medicine and Environmental Health. 27(6): 891–901

10 Luenda, C., Fekedulegn, D., McCall, T., Burchfiel, C., Andrew, M., Violant, J. (2012) Obesity, white blood cell counts, and platelet counts among police officers. Obesity (Silver Spring). 15(11): 2846-2854

11 http://m.thenational.ae/opinion/editorial/abu-dhabi-nearly-free-of-crime

12 http://m.thenational.ae/uae/abu-dhabi-among-worlds-safest-cities---graphic

13 http://m.thenational.ae/uae/abu-dhabi-is-the-safest-city-on-the-planet-with-lowest-crime-rate-numbeocom

14 Bykov, O. (2014). Police academy training: An evaluation of the strengths and weaknesses of police academy Research Journal of Justice Studies and Forensic Science. 2(1): 142-159

15 http://www.usmc-mccs.org/articles/what-is-a-tactical-athlete/

16 Vickers, R., Barnard, A. (2010) Effects of Physical Training in Military Populations: A Meta-Analytic Summary. Naval Health Research Center. Report No. 11-17

tection to the public[17] Good muscular strength will have an impact on police ability to apprehend an agitated suspect, sprint up a set of stairs, or burst through a locked door[18].

Endurance is the key ability when it comes to chase a suspect running out of the car, through a variety of terrains. It is a challenge that requires a police officer whose respiratory system can survive this effort and then quickly recover for possible next actions.

Crawley and associates did research about changes during a 16-week academy on physical fitness of police academy cadets[19]. A number of individual parameters of physical fitness showed evidence of improvement in the first eight weeks, whereas none of the variables showed significant improvement in the second eight weeks. This suggests that modifications could be made to increase the overall effectiveness of cadet physical training specifically after the eight-week mark.

Copay and coworkers from The Police Training Institute at the University of Illinois[20] designed a fitness training program which allowed the participants to choose the intensity and mode of their exercise. Between June 1993 and March 1995, the incoming recruits' fitness level was assessed before and after the training program in order to measure the improvement induced by the training and to compare the recruits' fitness level to the general population. The male recruits significantly improved their flexibility, abdominal strength and aerobic capacity.

Burke and Dyer have studied the eight-week ranger training and its effects on strength and cardiovascular endurance assessed by a modified Harvard step test, push-ups and pull-ups. The results have shown that the training had produced significant positive changes in the test of aerobic endurance and push-ups and significant negative changes in the test of pull-ups[21].

The purpose of this research is to investigate the impact of a supervised 12-week physical fitness training program on motor abilities and anthropometry of police academy cadets.

## METHOD

### Subjects

One hundred and fifty-eight healthy students of the Police College in Abu Dhabi participated in this study. All respondents had a regular strength and endurance training at least five times per week in a period from initial to final testing.The examined students were between 19 and 21 years old. The average weight on the initial measurement was 67.15kg, with a standard deviation of ± 9.4kg. The average height was 173.8cm, with a standard deviation of ± 5.47cm.

Training approach used a weekly cycle, with daily tasks to increase endurance, hypertrophy, strength, or power for general health and physical conditioning. All fitness-training sessions, regardless of approach, began with a warmup lasting approximately 15 minutes that included activities of running, increasing intensity basic movements and dynamic stretching

17 Boyce, R., Ciulla, S., Jones, G., Boone, E., Ellito, S., Combs, C. (2008) Muscular strength and body composition comparison between the Charlotte-Mecklenburg fire and police departments. International Journal of Exercise Science. 1(3): 125 – 135

18 http://www.ctsccc.com/the-importance-of-being-physically-fit-as-a-police-officer/

19 Crawley, A., Sherman, R., Crawley, W., Cosio-Lima, L. (2016) Physical Fitness of Police Academy Cadets: Baseline Characteristics and Changes During a 16-Week Academy. Journal of Strength and Conditioning Research, 30(5): 1416–1424

20 Copay, A., Charles, M. (1998) Police academy fitness training at the Police Training Institute, University of Illinois. Policing: An International Journal of Police Strategies & Management, 21(3): 416-431

21 Burke, W., Dyer, F. (1980) Effects of ranger training on selected measures of strength and cardiovascular fitness. US army research institute for the behavioral and social sciences. Research report 1353

and concluded with a cool-down lasting approximately 5 - 10 minutes, including a general focus on static stretching. The total length of each session was approximately 60 minutes. Training program was based on progressive increase of training complexity.From one to the next week cycle, the number of push-ups, sit-ups and external load increased, while the running time for the same distances decreased. Example of one training week: day one (Sunday): strength, day two (Monday) interval training, day three (Tuesday) strength, day four (Wednesday) 4km time trial run, day five (Thursday) cross fit training. All trainings started in the morning from 6 a.m.The afternoon training sessions were comprised of core stability training or exercise which would increase the level of fitness that were considered as class's weakness as per trainer's opinion. Those cadets whose physical fitness was assessed as having potential to be approved and those cadets whose efforts were not at an adequate level, as per trainers' and other college staff opinion, trained at the weekend.

**Materials and measured parameters**

All the tests that we have chosen for the evaluation of the effects and changes caused by the application of educational and training programs for the Police College students have a psychometric properties, excellent informativeness, objectivity, reliability, validity and economy of application:

- Body composition – weight and waist to height ratio (WTHR);
- Aerobic endurance test – running 2.4km distance (RUN);
- Abdominal repetitive strength test – maximum number of sit-ups in sixty seconds (SU);
- Upper body repetitive strength test – maximum number of push-ups in sixty seconds (PU).

**Testing protocols**

Protocol on initial and final testing had the same routine. Weight and waist were measured at the beginning of procedure. This was followed by warming up and giving precise instructions to cadets, after which they did PU and SU test in sixty seconds in order to finalize the 2.4km running test. The cadets were tested in their sport uniforms, which consisted of shorts, T-shirts and sport shoes. Testing team consisted of instructors from the Abu Dhabi Police College. Only perfectly done repetitions were counted, following high standard of testing rules. Shortening the range of motion or irregular contact with the ground for rest was not allowed.

**Statistical analysis**

All data were presented as means values and standard deviations. From descriptive statistics, for each variable, measures of central tendency (arithmetic mean) and dispersion (standard deviation) were calculated. From comparative statistics, T test for paired samples were used with a statistical significance level of $p < 0.01$. Statistical analysis was performed with a help of IBM SPSS Statistics 20.

# RESULTS

*Table 1 Showing mean values, standard deviations, minimum, maximum values and significance*

| | *Initial testing* | | | *Final Testing* | | | |
|---|---|---|---|---|---|---|---|
| Variables | Mean ± Std.Dev. | Min. | Max. | Mean ± Std.Dev. | Min. | Max. | Sig. |
| **WEIGHT** | 67.14 ± 9.42 | 49.5 | 96 | 65.84 ± 8.75 | 51 | 94.5 | 0.00 |
| **WAIST** | 77.42 ± 6.70 | 62 | 96 | 75.27 ± 6.12 | 63 | 94 | 0.00 |
| **WTHR** | 44.58 ± 4.03 | 33.51 | 55.88 | 43.33 ± 3.49 | 34.59 | 54.11 | 0.00 |
| **PU** | 34.33 ± 6.19 | 10 | 60 | 36.88 ± 6.62 | 11 | 62 | 0.00 |
| **SU** | 37.77 ± 4.56 | 28 | 50 | 40.47 ± 6.16 | 20 | 64 | 0.00 |
| **RUN** | 626.75 ± 36.70 | 540 | 854 | 592.25 ± 36.03 | 498 | 696 | 0.00 |

After finalizing results with T test for paired samples, the results in Table 1 shows that there is statistically significant difference between initial and final testing in all variables.

# DISCUSION

The biggest improvement between the initial and final testing was obtained by PU; there was an increase of 7.5%. It can be concluded that this progress is best achieved in training with emphasis on upper body repetitive strength. The exercises designed to build repetitive strength of participants with body weight approach included,but were not limited to: PU, diamond PU, incline PU, 8 count PU, plyometric PU. Progress in this test is also achieved as a result of weight training (training with external load) – bench press and dumbbell chest press.During this training coaches tend to motivate cadets to meet three demands: to raise relatively large (submaximal) load, progressively shorten the break between sets and achieve a large volume (number of repetitions). Adam Scotts' study from Mountain tactical institute has confirmed that simply doing PU is a necessary training component in improving result in PU test, if for no other reason than to simply build the neurological familiarity with the exercise. Consistent with results in this study, researches done byVossen, J. and associates[22] andGouvali, M. and associates[23] emphasize the importance of PU variants, such as the use of plyometrics, tempos and even hand position variations.

22 Vossen, J., Kramer, J., Burke, D., and Vossen, D. (2000) Comparison of dynamic push-up training and plyometric push-up training on upper-body power and strength. Journal of Strength and Conditioning Research. 14(3): 248-253

23 Gouvali, M, Boudolos, K. (2005) Dynamic and electromyographical analysis in variants of push-up exercise. Journal of Strength and Conditioning Research, 19(1): 146-151

In the test for valuation of repetitive abdominal strength (SU) there was a statistically significant improvement in the period from initial to final testing– 7.1%. The resulting changes can be attributed to the positive impact of the following exercises: mountain climbers, crunches, diagonal crunches, flutter kicks, medicine ball twists etc., but mostly big number of full motion SU identically like on future test. Bexter and associates[24] compared the outcomes of two different abdominal muscular fitness training regimens on SU performance (two-minute test) during six-week training period. Twenty foursubjects were randomly assigned to either a training group using curl-up exercise, a training group using sit-up exercise, or a control group. Results showed that specificity of training provided improvement in two-minute sit-up test. No significant difference in SU performance was noted for the curl-up or control groups.

RUN test indicates a positive change between the initial and final testing in 5.5%. Statistically significant change is the result of daily running under warming up at a length of 2 km, run training on 4km distance at a given time (once per week), interval training (once per week), etc.The results ofresearchat the sample of 90 Police Academy cadets from the United States are considered as very interesting[25]. The participants completed one of two 6-month training programs. The randomized training group (RTG) completed a randomized training program that incorporated various strength and endurance exercises chosen on the day of training. The periodized group (PG) completed a periodized training program that alternated specific phases of training.Results showed that only the RTG improved in the aerobic 2.4km run. A potential reason why PG did not have improvement in 2.4km test may have been the final block period of training, which focused on strength and power just before testing. This research supports Head of AD Police College sport decision not to use block periodization in cadets training process.

WTHRimproved by 2.7% owing to the decreased fat component of cadets' body and decreased average weight.Violanti J. and colleagues examined connection between body composition and physical fitness level[26].They obtained data from fitness screening among 1,826 male and 115 female officers in a large US police agency. Similar to our research, the participants were tested on 2.4km run, push-ups, sit-ups and sit-and-reach test.As assumed, the results suggested that increased body fat percent was significantly associated with decreased prevalence of overall fitness in police officers.

## CONCLUSION

Fitness level and antropometric status are improved in the final, when compared to the initial testing, which clearly indicates the effectiveness of the applied training process. The change in results of the selected tests confirms the set hypothesis.

The limitation of this study is the relatively small variable sample. Future directive for expansion of this research is testing other physical abilities (through pulling, squatting, jumping, sprinting, hand grip power tests etc.) and morphological parameters to better characterize effects of the training program.Also, future studies should be initiated to explore annual

24 Baxter, R., Moore, J., Pendergrass, T., Crowder, T., Lynch, S. (2003) Improvement in sit-up performance associated with 2 different training regimens. The Journal of orthopaedic and sports physical therapy. 33(1): 40-47

25 Cocke, C., Dawes, J., Marc, R. (2016) The use of two conditioning programs and the fitness characteristics of Police Academy cadets. Journal of Athletic Training. 51(11): 887-896

26 Violanti, J., Ma, C., Fekedulegn, D., Andrew, M., Gu, J., Hartley, T., Charles, L., Burchfiel, C. (2017) Associations between body fat percentage and fitness among police officers. Safety and health at work. 8(1): 36 - 41

fluctuation of fitness level under specific local influences, such astemperature and humidity changes, Ramadan strict fasting etc.

## REFERENCE

1. Anderson, S., Plecas, D., Segger, T. (2001) Police officer physical ability testing. Re-validating a selection criterion. Policing: An International Journal of Police Strategies & Management. 24(1): 8-31
2. Baxter, R., Moore, J., Pendergrass, T., Crowder, T., Lynch, S. (2003) Improvement in sit-up performance associated with 2 different training regimens. The Journal of orthopaedic and sports physical therapy. 33(1):40-47
3. Bonneau, J., Brown, J. (1995) Physical ability, fitness and police work. Journal of clinical forensic medicine. 2(3):157-164
4. Boyce, R., Ciulla, S., Jones, G., Boone, E., Ellito, S., Combs, C. (2008) Muscular strength and body composition comparison between the Charlotte-Mecklenburg fire and police departments. International Journal of Exercise Science. 1(3): 125 – 135
5. Burke, W., Dyer, F. (1980) Effects of ranger training on selectedmeasures of strength and cardiovascular fitness. US armyresearch institute for the behavioral and social sciences. Research report 1353
6. Bykov, O. (2014). Police academy training: An evaluation of the strengths and weaknesses of police academies. Research Journal of Justice Studies and Forensic Science. 2(1): 142-159
7. Crawley, A., Sherman, R., Crawley, W., Cosio-Lima, L. (2016) Physical Fitness of Police Academy Cadets: Baseline Characteristics and Changes During a 16-Week Academy. Journal of Strength and Conditioning Research, 30(5): 1416–1424
8. Cocke, C., Dawes, J., Marc, R. (2016) The use of two conditioning programs and the fitness characteristics of Police Academy cadets. Journal of Athletic Training. 51(11): 887-896
9. Copay, A., Charles, M. (1998) Police academy fitness training at the Police Training Institute, University of Illinois. Policing: An International Journal of Police Strategies & Management, 21(3): 416-431
10. Da Silva, CF., Soleman, Hernandez SS., Valdivia,Arancibia BA., Da Silva Castro, TL.,GutierresFilho, PJB., Rudney Da Silva, R. (2014) Health-related quality of life and related factors of military police officers. Health and quality of life outcomes. 12: 60
11. Da Silva, CF., Soleman, Hernandez SS., Valdivia,Arancibia BA., Da Silva, Castro TL., Gutierres,Filho PJB., Rudney, Da Silva, R. (2014) Anthropometric indicators of obesity in policemen: A systematic review of observational studies. International Journal of Occupational Medicine and Environmental Health. 27(6): 891–901
12. Dimitrijević, R., Koropanovski, N., Dopsaj, M., Vučković, G., Janković, R. (2014) The influence of different physical education programs on police students' physical abilities. Policing: An International Journal of Police Strategies & Management, 37(4): 794-808
13. Gouvali, M, Boudolos, K. (2005) Dynamic and electromyographical analysis in variants of push-up exercise. Journal of Strength and Conditioning Research, 19(1): 146-151
14. Janković R. (2015) Validacijapoligonakaotestazaprocenuspecificnespretnostikodpolicajaca. Fakultetsporta i fizickogvaspitanja, Doktorskadisertacija. 4. str.

15. Luenda, C., Fekedulegn, D., McCall, T., Burchfiel, C., Andrew, M., Violant, J. (2012) Obesity, white blood cell counts, and platelet counts among police officers. Obesity (Silver Spring). 15(11):2846-2854
16. Mudric R. (2005)Specijalnofizickoobrazovanje.Prirucnik. Visa skolaunutrasnjihposlova. 180. str.
17. Shell D. (2002) Law enforcement entrance-level physical training: Does it need a new approach? Sheriff, 54(4): 26–60
18. Sporis, G., Harasin, D., Bok, D., Matika, D.,Vuleta, D. (2011) Effects of a training program for special operations battalion on soldiers fitness. The Journal of Strength and Conditioning Research, 26(10):2872-2882
19. Vickers, R., Barnard, A. (2010) Effects of Physical Training in Military Populations: A Meta-Analytic Summary. Naval Health Research Center. Report No. 11-17
20. Violanti, J., Ma, C., Fekedulegn, D., Andrew, M., Gu, J., Hartley, T., Charles, L., Burchfiel, C. (2017) Associations between body fat percentage and fitness among police officers. Safety and health at work. 8(1): 36 - 41
21. Vossen, J., Kramer, J., Burke, D., and Vossen, D. (2000) Comparison of dynamic push-up training and plyometric push-up training on upper-body power and strength. Journal of Strength and Conditioning Research. 14(3):248-253
22. http://www.ctsccc.com/the-importance-of-being-physically-fit-as-a-police-officer/
23. http://www.usmc-mccs.org/articles/what-is-a-tactical-athlete/
24. http://m.thenational.ae/opinion/editorial/abu-dhabi-nearly-free-of-crime
25. http://m.thenational.ae/uae/abu-dhabi-among-worlds-safest-cities---graphic
26. http://m.thenational.ae/uae/abu-dhabi-is-the-safest-city-on-the-planet-with-lowest-crime-rate-numbeocom