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, 3-4. mart 2015.
Belgrade, 3-4 March 2015

TEMATSKI ZBORNIK RADOVA
MEĐUNARODNOG ZNAČAJA

THEMATIC CONFERENCE PROCEEDINGS
OF INTERNATIONAL SIGNIFICANCE

TOM III
VOLUME III

KRIMINALISTIČKO-POLICIJSKA AKADEMIJA
Beograd, 2015
ACADEMY OF CRIMINALISTIC AND POLICE STUDIES
Belgrade, 2015

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

For Publisher
MLADEN BAJAGIĆ, PhD
Acting Dean of the Academy of Criminalistic and Police Studies

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

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

Thematic Proceedings Reviewers
Full Professor MILAN ŠKULIĆ, PhD
Faculty of Law, University of Belgrade, Serbia
Associate Professor GABOR KOVACS, PhD
Faculty of Law Enforcement, National University of Public Service, Hungary
Associate Professor JOZEF METENKO, LLD
Academy of Police Force in Bratislava, Slovakia
JOANA WHYTE
Center of Studies in European Union Law, Minho University Law School, Portugal
LAURA HAYRUNI
OSCE Office in Yerevan, Armenia
Assistant Professor NILGUN SEN, PhD
Forensic Science Institute, Police Academy, Turkey

Impression
200 copies

Print
Official Gazette, Belgrade

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

ISBN 978-86-7020-321-1
ISBN 978-86-7020-190-3

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

Za izdavača
prof. dr MLADEN BAJAGIĆ
v.d. dekana Kriminalističko-policijske akademije

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

Tiraž
200 primeraka

Štampa
Službeni glasnik, Beograd

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

ISBN 978-86-7020-321-1
ISBN 978-86-7020-190-3

INTERNATIONAL SCIENTIFIC CONFERENCE
ARCHIBALD REISS DAYS

PROGRAMME COMMITTEE

Mladen Bajagić, PhD, Academy of Criminalistic and Police Studies, President
Dragana Kolarić, PhD, Vice Dean of the Academy of Criminalistic and Police Studies
Sima Avramović, LLD, Dean of the Faculty of Law in Belgrade
Zoran Stojanović, LLD, Full Professor at the Faculty of Law in Belgrade
Radomir Milašinović, PhD, Dean of the Faculty of Security in Belgrade
Major-General **Mladen Vuruna**, PhD, Rector of the University of Defence in Belgrade

International members

Hélène Martini, PhD, Director of the France's National Police College
and President of the Association of European Police Colleges
Norbert Leitner, PhD, Vice President of the Association of European Police Colleges
and Director of SIAK, Vienna, Austria
Wang Shiquan, PhD, President of the National Police University of China
Vladimir Tretyakov, PhD, Chief of the Volgograd Academy of the Russian Internal Affairs Ministry
Police colonel **Sereda Valeriy Vyacheslavovich**, PhD,
Rector of the Lviv State University of Internal Affairs, Ukraine
Major-general of militia **Vladimir Bachila**, LLD,
Head of the Academy of the Interior Ministry of Belarus
Simon Carp, PhD, Rector of the Academy "Stefan cel Mare", Ministry of Interior of Moldova
Mihai Badescu, PhD, Acting Rector of the Police Academy „Alexandru Ioan Cuza", Bucharest, Romania
Piotr Bogdalski, PhD, Commandant-Rector of the Police Academy in Szczytno, Poland
Štefan Kočan, PhD, Academy of Police Force, Bratislava, Slovakia
Jozef Metenko, PhD, Academy of Police Force, Bratislava, Slovakia
Peter Ruzsonyi, PhD, Dean of the Faculty of Law Enforcement, Hungary
Gorazd Meško, PhD, Dean of the Faculty of Criminal Justice and Security, University of Maribor, Slovenia
Ivan Toth, PhD, Dean of the University of Applied Sciences Velika Gorica, Croatia
Oliver Bačanović, PhD, Dean of the Faculty of Security, Skopje, Macedonia
Nedžad Korajlić, PhD, Dean of the Faculty for Criminal Justice, Criminology
and Security Studies, University of Sarajevo, Bosnia and Herzegovina
Duško Pena, MA, Director of the Police College in Banja Luka, Republic of Srpska
Mile Šikman, PhD, MoI of the Republic of Srpska
Dragan Radonjić, LLD, Dean of the Faculty of Law, Podgorica, Montenegro
Milica Pajović, Dean of the Police Academy in Danilovgrad, Montenegro

ORGANIZING COMMITTEE

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

MEĐUNARODNI NAUČNI SKUP
DANI ARČIBALDA RAJSA

PROGRAMSKI ODBOR

prof. dr **Mladen Bajagić**, Kriminalističko-policijska akademija, **predsednik**
prof. dr **Dragana Kolarić**, Kriminalističko-policijska akademija
prof. dr **Sima Avramović**, dekan Pravnog fakulteta u Beogradu
prof. dr **Zoran Stojanović**, redovni profesor Pravnog fakulteta u Beogradu
prof. dr **Radomir Milašinović**, dekan Fakulteta bezbednosti u Beogradu
general-major prof. dr **Mladen Vuruna**, rektor Univerziteta odbrane u Beogradu

Članovi iz inostranstva

Hélène Martini, predsednica Asocijacije evropskih policijskih koledža
i direktorka Francuskog nacionalnog policijskog koledža, Francuska
dr **Norbert Leitner**, potpredsednik Asocijacije evropskih policijskih koledža
i direktor SIAK Policijske akademije iz Beča, Austrija
prof. dr **Wang Shiquan**, predsednik Kineskog kriminalističko-policijskog univerziteta
prof. dr **Vladimir Tretjakov**, načelnik Volgogradske akademije Ministarstva unutrašnjih poslova Rusije
prof. dr **Sereda Valeriy Vyacheslavovich**,
rektor Državnog univerziteta unutrašnjih poslova u Lavovu, Ukrajina
general-major milicije, doc. dr **Vladimir Bačila**, načelnik Akademije MUP Belorusije
prof. dr **Simon Karp**, rektor Akademije "Stefan cel Mare", MUP Moldavije
prof. dr **Mihai Badescu**, v.d. rektor Policijske akademije „Alexandru Ioan Cuza", Bukurešt, Rumunija
prof. dr **Piotr Bogdalski**, komandant-rektor Policijske akademije u Šitnu, Poljska
prof. dr **Štefan Kočan**, Policijska akademija, Bratislava, Slovačka
prof. dr **Jozef Metenko**, Policijska akademija, Bratislava, Slovačka
prof. dr **Peter Ruzsonyi**, dekan Fakulteta za sprovođenje zakona, Mađarska
prof. dr **Gorazd Meško**, Fakultet bezbednosnih studija, Univerzitet u Mariboru, Slovenija
Prof. mr. sc. **Ivan Toth**, dekan Veleučilišta Velika Gorica, Hrvatska
prof. dr **Oliver Bačanović**, dekan Fakulteta bezbednosti, Skoplje, Makedonija
prof. dr **Nedžad Korajlić**, dekan Fakulteta za kriminalistiku, kriminologiju
i sigurnosne studije, Univerzitet u Sarajevu, BiH
mr **Duško Pena**, direktor Visoke škole unutrašnjih poslova u Banjoj Luci, Republika Srpska
doc. dr **Mile Šikman**, MUP Republike Srpske
prof. dr **Dragan Radonjić**, dekan Pravnog fakulteta, Podgorica, Crna Gora
Milica Pajović, direktor Policijske akademije u Danilovgradu, Crna Gora

ORGANIZACIONI ODBOR

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

PREFACE

Dear readers,

In front of you is the Thematic Collection of Papers presented at the International Scientific Conference "Archibald Reiss Days", which was organized by the Academy of Criminalistic and Police Studies in Belgrade, in co-operation with the Ministry of Interior and the Ministry of Education, Science and Technological Development of the Republic of Serbia, National Police University of China, Lviv State University of Internal Affairs, Volgograd Academy of the Russian Internal Affairs Ministry, Faculty of Security in Skopje, Faculty of Criminal Justice and Security in Ljubljana, Police Academy "Alexandru Ioan Cuza" in Bucharest, Academy of Police Force in Bratislava and Police College in Banjaluka, and held at the Academy of Criminalistic and Police Studies, on 3 and 4 March 2015.

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

The Thematic Collection of Papers contains 168 papers written by eminent scholars in the field of law, security, criminalistics, police studies, forensics, informatics, as well as members of national security system participating in education of the police, army and other security services from Spain, Russia, Ukraine, Belarus, China, Poland, Armenia, Portugal, Turkey, Austria, Slovakia, Hungary, Slovenia, Macedonia, Croatia, Montenegro, Bosnia and Herzegovina, Republic of Srpska and Serbia. Each paper has been reviewed by two reviewers, international experts competent for the field to which the paper is related, and the Thematic Conference Proceedings in whole has been reviewed by five competent international reviewers.

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

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

Finally, we wish to extend our gratitude to all the authors and participants at 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 of the Republic of Serbia and the Ministry of Education, Science and Technological Development of the Republic of Serbia.

Belgrade, June 2015

Programme and Organizing Committees

TABLE OF CONTENTS

TOPIC V

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

TOPIC VIII

Innovative Techniques and Equipment in Forensic Engineering

Topic V

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

UDC: 343.352:351.74/.75
174:351.74/.75

POLICE CORRUPTION AS A SUBJECT OF SCIENTIFIC RESEARCH

Branislav Simonovic
University of Kragujevac, Faculty of Law[1]

Abstract: This paper investigates police corruption and its harmful consequences. The paper also touches upon certain comparative researches that investigated the citizens' perception on the problem of police corruption. Special attention was paid to the problems of administrative and scientific view of police corruption. Some misconceptions with regard to this are also presented, as well as problems in viewing the actual situation in the domain of police corruption. The paper points to the problem of the police corruption related to drug crime. Special attention was dedicated to scientific research of police integrity based on the so-called model of eleven scenarios. Apart from that other researches are also presented that included scientific overview of police integrity.

Keywords: police corruption; police integrity; the research model of hypothetical eleven scenarios.

INTRODUCTION

Corruption represents one of the persisting dangerous phenomena with which all societies were faced in the past, present, and which will undoubtedly face with in the future. The corruption in the police represents a manifestation of a problem which is, in itself, very serious – the problem of corruption in society. While on the one hand, the police (and prosecutors and courts) are expected to fight corruption, to reveal perpetrators and protect the society from criminal, on the other hand precisely the police have the problem with corruption, building and maintaining professional integrity (e.g. Fijnaut, Huberts, 2002). The history of the police is full of corruption scandals which in their scale and extent were used to undermine the very foundations of the countries (examples of Mexico and Columbia). Police corruption is a universal problem. It can be found in all the countries of the world regardless of the level of social development, economic power and the level of democratic institutions. Many quotes of Knapp Commission Report 1972 and Mollen Commission Report 1994 (Mollen Commission Report, 1994) can be found in the literature as well as the reports on the alarming state of the corruption in the USA. Numerous scandals about the police corruption were recorded in Great Britain, Belgium, Germany, Spain, Turkey, Australia, etc. (Newburn, 1999; Punch, 2000). A general scientific conclusion is drawn that the police are quite vulnerable to the matters of corruption (Huberts 2003). Therefore, the ever current question is raised – quas custodiet ipsos custodies- who inspects the inspectors? (Punch, 2000: 301).

The consequences of the corruption are very severe and dangerous. The scientific and professional literature points out that the phenomenon of corruption has many faces. It has many levels, different gravity from case to case, starting from accepting free lunches and moving forward to gaining millions through the collaboration in organized crime. Corruption is universal. Among many consequences of police corruption is also, the absence of legitimacy in the police (Bayley, Perito, 2011: 5; Punch, 2000: 301), lack of trust in the legal state, lack of public support of the police (Jenks, et al., 2012: 4; Weitzer, 2002; Sellbom, et al., 2007: 985; Tankebe, 2010: 297; Kutnjak-Ivković, 2009: 777). Corruption destroys fundamental values of human dignity and political equality, diminishes human rights and equality of the citizens before state authorities and the law (Kolthoff, 2010: 13-14). When special authorizations of police officers are added to this (e.g. secret surveillance), their right to exercise force and arms (Kääriäinen, 2007: 410) then the trust of citizens is essential for maintaining the legitimacy that is seriously threatened by the corruption. The problem is that small acts of corruption and abuse in the police can lead to large-scale corruption and severe violations of professional codes (Moran, 2005:74).

Numerous researches have been conducted in various countries of the world on the citizens' perception of the corruption in various institutions in the society. In all of these researches, the police take up a high place on the list. The police are appraised regardless of the region and the period of observation, as one of the most corrupted institutions in the society. For instance, a citizens' survey in Latin America rates the police as one of the most corrupted institutions in the society, which together with the perception of police brutality directly contributes to the negative evaluation of the police by the citizens (Väsquez, 2013: 403).

1 simonov99@gmail.com

In South Africa, the police are constantly rated as the second most corrupted institution in the state (Meyer et al. 2013: 141). In one of the reports made by Transparency International, it is stated that in 86 countries the police is the most corrupted institution, after political parties, public service in general, parliament and legislature (Bayley, Perito, 2011: 2).

The above statements agree with the situation in Serbia. In October 2010, the Statistical Office of the Republic of Serbia conducted a research on corruption on the territory of the Republic of Serbia. Based on the indicators of perception and corruption in certain sectors and institutions in Serbia, the police take the fourth place. (The first on the list are political parties, followed by the local self-government, state hospitals and then the police. The courts are on the fifth place, followed by customs administration, the Government of the Republic of Serbia, etc.) The same research shows that the bribe in Serbia is mostly given to the doctors (57% of the total bribe percentage), then to the police officers (26%) and the civil servants (13%). According to this research the police officers are the second professional group susceptible to bribe taking, following the doctors on the first place. According to the indicator of measuring the highest average rate of corruption, the police officers have the worst reputation (9%), then doctors (7%), administrative officers (6%), etc. (Corruption in Serbia, citizens' experience, 2010).

The scientific conclusion points out that the police officers are particularly exposed to the risk of corruption considering the nature of their profession which is characterized by the specific nature of the work, characteristic value system, solidarity among the police officers, police cynicism, silence codex, tolerating the violation of service codex, police discretion. Considering the fact that the police officers are in constant contact with the criminals, dishonest people characterized by the distorted value system, their profession is exposed more to the temptations and offers from the criminal world which constantly attempts to win them over to their side. According to Punch, the police organization deals with the people who are in problems, people who create problems, while the job of the police officers is characterized by low visibility, that is to say, insufficient transparency, which represents a problem in implementing control within police organization (Punch, 2000: 321). Taken into account that the police do not function in vacuum (Kutnjak Ivković, Kang, 2012: 84), the influences of social surrounding, and the exposure to local pressure have impact on the corruption in the police (Aremu et al., 2009:146). If one adds to this the fact that the police officers have low salaries, while at the same time they are constantly in contact with wealthy criminals, the corruption risk becomes a realistic category.

THE PROBLEM OF ADMINISTRATIVE AND SCIENTIFIC RESEARCH AND OVERVIEW OF POLICE CORRUPTION

Bearing in mind all mentioned above, it is not unusual to find police corruption as one of the subjects of administrative and scientific research in the countries of western democracy. However, the researchers who deal with this problem point out that practical research of police corruption faces a number of difficulties. "Corruption is extremely difficult to study in a direct, quantitative, and empirical manner. Because most incidents of corruption are never reported or recorded, official data on corruption are best regarded as measures of a police agency's anti-corruption activity, not the actual level of corruption" (Klockars et al., 2000: 2, cited by Meyer et al: 143-144). The police officers all over the world are reluctant to talk about the problem of corruption within their profession, especially with those people who are outside of the police milieu. Police superiors show a tendency to deny or minimize the problem of corruption in their ranks. For decades there has been a ruling stance in police institutions all over the world that the corruption in the police is not a serious problem and that it can all be reduced to individual cases, especially to few corrupted individuals, based on which a theory of "rotten apples" was created as an explanation for police corruption (Väsquez, 2013: 406, 414).

In western literature it is pointed out that the riskiest positions for corruption are those linked to fighting drug criminal (close contact with drug dealers), the work of undercover investigators, working with informers, suppressing organized crime, licence issuing service, closing contracts with companies (Mollen Commission Report, 1994: 2; Police Integrity, England, Wales and Northern Ireland, 1999: 8; Punch, 2000: 308, 319; Moran, 2005: 61; Stinson, et al., 2013; Väsquez, 2013: 406).

In our region, on the Balkan territory, the situation seems different at first sight. In one research conducted in Bosnia and Herzegovina, the matters of police traffic control are stated as the areas with the highest risk of police corruption.

The research conducted in 2012 in Serbia included the sample of 2.224 citizens. When answering the question: „What is the position of the police officer you bribed?" 30% of participants, who gave a bribe, stated that they gave it to the traffic police officers (162). The analyses of citizens' answers which point to

police corruption denote the traffic police as one of the most corrupted (Strategic intelligence estimate of the corruption, 2012: 16, 59-60).

The same research conducted a survey about the police officers and their knowledge of the colleagues that accepted a bribe. Out of 10,168 surveyed police officers, 1,358 of them stated that they have information on their corrupted colleagues. To this question they answered that they have information at disposal that show that 2,730 police officers have accepted a bribe. The majority of them were those who were performing tasks related to traffic control (Strategic intelligence estimate of the corruption, 2012:39).

The above stated results lead to a conclusion that traffic police are the area with the highest risk of corruption. There is no doubt that the traffic police are the most transparent and under close eye of the citizens who are not perpetrators of criminal actions. It is necessary to emphasize that it is usually, the so-called „small-scale corruption" with high occurrence frequency, which makes it the most visible.

Poor results regarding traffic police and „the statistics of big numbers" should not distort the picture of corruption and the police in general. In this regard, the warning from an Australian commission is very important. Their research came to a conclusion that the most of citizens' complaints are related to less serious cases of corruption. Relying on the citizens' complaints can be wrong, because the most severe of corruption cases happen in relation to drugs and out of public sight. These activities happen outside of so-called "soft" approaches, such as citizens' perception and complaints. That is why the mentioned research concludes that it is necessary to apply other measures of criminalistic control that are focused on detecting more serious and hidden forms of corruption. These actions can be revealed by applying effective proactive methods, e.g. special (hidden) police and investigative techniques that have a powerful diversive effect (Criminal Justice Commission, 2001: 10).

The experience in Serbia is another reason why this warning from the Australian commission should be taken seriously as a general warning that should be integrated in anti-corruption policy of all police institutions. Hardly a year goes by in Serbia without a big affair revealed, usually related to drugs, where the police officers, who should prevent and fight these crimes, appear as perpetrators (drug dealers) or they actively participate in protection and covering the activities of the criminal group. On the other hand, the mentioned research points to the caution and danger of making wrong conclusions, that is to say, the risk of losing the focus on anti-corruption strategies in less transparent areas where the so-called big corruption happens.

When it comes to administrative overview of the corruption in the police, the real picture of the scale and forms of this phenomenon could usually be made only after big affairs that happened in certain countries with developed democracy, after which independent and competent bodies have been formed with the support of public and media. Due to the size of the scandals internal (police) sabotage and the obstructions by the politicians could not be intensified. The scientific and professional literature most often comments the results of Knapp Commission 1992 (Knapp Commission, http://en.wikipedia.org/wiki/Knapp_Commission), Mollen Commission 1994 (Mollen Commission, http://www.nyc.gov/html/ccpc/assets/downloads/pdf/final_report.pdf). (both were formed in the USA) and Wood Commission that dealt with this problem in Australia in 1997.

The reports of all three commissions emphasize that the corruption in the police is a systematic, and not an individual phenomenon, that covering individual cases, which is a usual practice, brings problems to escalation point. In the control of police corruption there is a lack of systematic and organizational preventive measures. The most serious case of corruption is related to drugs, which is why a proactive approach is needed, as well as measures and methods of internal control that are used in suppressing organized crime. Each of the commissions has suggested the implementation of a wide system of measures that aim to implement corruption control within the police in a systematic, comprehensive and diverse manner.

POLICE INTEGRITY AS A SUBJECT OF SCIENTIFIC RESEARCH

a) Research, measurement, evaluation of police officers' integrity based on the **scenario method**

Within the research on police corruption conducted by academics, there is the majority of papers that investigate integrity of the police profession. Within this group, judging by the number of published papers and conducted research dominant are papers by Sanja Kutnjak Ivković (Croatian-born, Professor of Michigan State University). Professors Klockars and Kutnjak-Ivković drew up a questionnaire in 2003 intended for interviewing police officers (see Klockars, and Kutnjak Ivković, 2003) that is based on scenarios, that is to say, hypothetical situations. The police officers were asked to state their opinion on whether there was and in which situation a violation of police integrity and to what extent. Hypothetical situations presented to the police officers were always the same in numerous researches conducted all over the world (that is,

with slight variations and adjustments to the local milieu). The initial research included seven hypothetical scenarios, while, later on, the number was settled to eleven. The hypothetical situations were the following:

Case 1

A police officer runs his own private business in which he sells and installs security devices, such as alarms, special locks, etc. He does this work during his off-duty hours.

Case 2

A police officer routinely accepts free meals, cigarettes, and other items of small value from the merchants on his beat. He does not solicit these gifts and is careful not to abuse the generosity of those who give gifts to him.

Case 3

A police officer stops a motorist for speeding. The officer agrees to accept a personal gift of half of the amount of the fine in exchange for not issuing a citation.

Case 4

A police officer is widely liked in the community, and on holidays local merchants and restaurant and bar owners show their appreciation for his attention by giving him gifts of food and liquor.

Case 5

A police officer discovers a burglary of a jewelry shop. The display cases are smashed and it is obvious that many items have been taken. While searching the shop, he takes a watch, worth about two days' pay for that officer. He reports that the watch was stolen during the burglary.

Case 6

A police officer has a private arrangement with a local auto body shop to refer the owners of the cars damaged in the accidents to the shop. In exchange for each referral, he receives a payment of 5 percent of the repair bill from the shop owner.

Case 7

A police officer, who happens to be a very good auto mechanic, is scheduled to work during coming holidays. A supervisor offers to give him these days off, if he agrees to tune-up his supervisor's personal car. Evaluate the supervisor's behavior.

Case 8

At 2 a.m. a police officer, who is on duty, is driving his patrol car on a deserted road. He sees a vehicle that has been driven off the road and is stuck in a ditch. He approaches the vehicle and observes that the driver is not hurt but is obviously intoxicated. He also finds that the driver is a police officer. Instead of reporting this accident and offense he transports the driver to his home.

Case 9

A police officer finds a bar on his beat which is still serving drinks half an hour past its legal closing time. Instead of reporting this violation, the police officer agrees to accept a couple of free drinks from the owner.

Case 10

Two police officers on foot patrol surprise a man who is attempting to break into an automobile. The man flees. They chase him for about two blocks before apprehending him by tackling him and wrestling him to the ground. After he is under control both officers punch him a couple of times in the stomach as punishment for fleeing and resisting.

Case 11

A police officer finds a wallet in a parking lot. It contains the amount of money equivalent to a full-day's pay for that officer. He reports the wallet as lost property, but keeps the money for himself.

The interviewed police officers were supposed to answer a couple of questions related to each one of scenarios.

The first group of questions was intended to estimate the **perception of the severity of violations.** The interviewed police officers had the assignment to estimate the severity of violation on Likert scale for each situation of hypothetical scenario (starting with 1- not severe to 5- very severe). The second task was to estimate how would most of their colleagues (in some questionnaires their superiors) evaluate the severity

of the scenarios. Finally, they were asked if the behavior from the scenarios would be considered as violation in their station and they were supposed to use a five-level scale starting with 1-'definitely no' to 5-'definitely yes'.

The second group of questions would estimate the **penalty which the interviewed police officers would suggest** for every mentioned violation on the scale of 1 to 6 (starting with no penalty to getting fired). The interviewed officers were expected to say which penalty would be their choice. Then their task would be to estimate which penalty, in their opinion, would most officers from their unit choose (or their superiors).

The third group was for the estimation of the **willingness to report certain violation** (firstly, would the interviewed officer report it, and would the most officers from the unit report that, in his or her opinion). The answers were graded on the 1 to 5 scale (1- 'definitely not' to 5-'definitely yes').

Police officers in a big number of countries were interviewed using the same questionnaire, for example: Bosnia and Herzegovina (Kutnjak Ivković and Shelley, 2005); Croatia (Kutnjak Ivković, 2009); the Czech Republic (Kutnjak Ivković and Shelley, 2007); South Africa (Kutnjak Ivković and Sauerman, 2011), Armenia (Kutnjak Ivković and Khechumyan, 2013) etc. Apart from that, police officers from different countries were interviewed simultaneosly using the same questionnaire and their answers were statistically compared and analysed in order to estimate, compare and measure (as the authors pointed) police officers' integrity. A research in which 11 hypothetical situations were estimated by police officers from Croatia, Finland and the USA can be mentioned in relation to the previous one (see Kutnjak Ivković, 2005). The same method (of 11 scenarios) was applied in the papers of other authors in the research of police executives' integrity, Schafer, Martinelli, 2008 for example.

The number of the questionnaires which were filled in by the police officers in the researches mentioned above was 250 and more.

It is interesting to mention newer research conducted in one area of South Africa which is in relation to the research of police integrity based on the use of 11 given scenarios. Within this research, beside the police officers (sample of 160 of them), students of the faculty of law were also interviewed using the same model (sample of 160 of them). Three groups of questions were given: a) their estimation of the severity of violation on the 1 to 5 scale; b) what would, in their opinion, the police management do about the violation of the rules of the service from the scenarios (the answers were given on a six-level scale and went from 'nothing' to 'getting fired'); and c) if they were police executives, how would they punish the violation from the offered scenarios (with the answers given on a six-level scale from 'in no way' to 'firing'). The authors of the research started with the assumption that in the estimation of police integrity attitude of the public is equally important as attitude of police employees and, in accordance to that fact, a comparison was made between the police officers' evaluation and law students' evaluation of given eleven scenarios. (Meyer et al., 2013).

b) 'Silent codex' Research among police officers based on the **scenario method**

Professor Sanja Kutnjak Ivković published numerous papers during the last decade in which she researched the phenomenon of silence codex among police officers in relation to tolerating and not reporting police corruption cases and other irregularities in police work (Kutnjak Ivkovic, 2009; Kutnjak Ivković and Shelley 2010; Kutnjak Ivkovic´ and Sauerman 2013). Within the researches all papers were based on the same eleven hypothetical scenarios. In the papers there was a comparison of police officers' opinion and police executives' opinion about reporting and punishing the violation, as well as the estimation of how someone else (officer or executive) would behave if they encountered the violation described in the scenario. The sample of interviewed police employees was, for example, about 150 executives and about 450 officers (Kutnjak Ivković and Shelley 2010).

The research of police integrity and 'silence codex' as one of the variations of lack of integrity by application of eleven scenarios method represents the most dominant method in the world during the last decade. The authors who apply it define it as 'universal method for estimation of police integrity'. It seems to us that this is too bold (arbitrary statement). A profession's integrity, including policing, is too complex a phenomenon to be reduced 'only' to eleven hypothetical scenarios. It seems like a good solution to find some other methods of exact scientific research (or estimation) of police integrity, that is, integrity of civil servant in general.

The first scenario (private business beyond working hours) cannot be seen as universal violation of police working discipline all aroud the world and without holdback. Maybe it is the case in the USA, but in some other countries police officers are allowed to do some other private business beyond working hours in order to boost their budget and to fight corruptional temptations at the workplace more successfully. The question which arises is which jobs can be acceptable? Security of criminals certainly isn't one of them. Owning a corner shop, grocery store or driving a taxi is. The question is whether the police officer endangers integrity of police profession by owning a private store selling alarm and security systems and working in it beyond working hours? (scenario 1)

In spite of the doubts mentioned, asking different questions, determining correlations between personal estimation of the interviewed people and their predictions (how their colleagues or superiors would answer to the same questions) represent an interesting method and give the opportunity to consider the integrity subject from various angles. One of the characteristics of the mentioned researches is the use of various statistical methods.

POLICE INTEGRITY RESEARCH BASED ON COURT CASES ANALYSIS

The paper of Norwegian Professor Gottschalk, whose empirical research was based on court cases analysis and verdicts brought in Norway against police officers for different criminal deeds, represents true refreshment in the great number of papers about police integrity based on hypothetical scenarios. The research included determining the correlation among different criminal offenses, motives for them and issued penalties. The research comprised 57 court cases (Gottschalk, 2010). Gottschalk suggested this model to be a new instrument for police integrity assessment.

c) Research of drug related criminal acts on police corruption

When it comes to researches on the police corruption conducted by academics and published in relevant scientific journals, there is an interesting paper reflecting the influence of drug related crimes on police corruption. In this paper the method of gathering data was based on searching key words on Google. During the defined period of time the researchers analyzed American newspaper articles which brought about the cases where police officers were arrested due to the determined links to drugs and corruption. The paper was published in a relevant journal and it represents a comprehensive analysis of the links that exist between police corruption and police officers involved in drug related crimes (Stinson, et al., 2013).

The research of police corruption in which the only sources of information are newspaper articles gathered through Google has its weaknesses because the press cannot be considered reliable source of information. The press often presents the problem as a sensation, arbitrarily and non-critically, so the scientific research based on this kind of source cannot be considered reliable. However, the mentioned paper uses sophisticated statistical methods in data analysis. Therefore a dilemma arises as to what the use of complex statistical methods is if the source of information is unreliable.

The research of the connection between a drug related crime and police corruption based on court verdicts would probably have greater scientific significance. However, the analysis of court verdicts and cases brings other difficulties for researchers. This is especially true for slow and inefficient court systems such as ours in Serbia where there are no quality electronic data bases which would enable a simple access to the verdicts and court cases for the purposes of a scientific research.

CONCLUSION

On the Thomson's list of relevant scientific journals there were papers published in the last ten or fifteen years which show analyses of a significant level of the lack of diversity. Most of them are on the subject of investigation of police integrity based on eleven scenarios and the author (coauthor) is most often the same. We cannot avoid the impression that globalization process was expressed in the subject of this scientific research. It is monotonous to approach the subject of police corruption in the same manner using the same methods, based on the same questionnaire. It seems that the problem of police corruption integrity is by far more complex and that it cannot be comprised by the same research technique or the same hypothetical situations. The problem of police integrity, police corruption and silence codex as its part cannot be reduced to only 11 hypothetical scenarios. The understanding of police integrity and integrity in general cannot be absolutely the same in the USA, the Arab world, Asia, Eastern Europe etc. We believe that new, more diverse methods for practical studying of police corruption and police integrity should be devised.

We do not intend to diminish the significance and quality of the mentioned researches by taking this stands. On the contrary, we are only advocating for diversity and versatility. One should approach any subject of research, as well as police corruption, from different angles using different elements to obtaining the data and different methods of analysis in order to observe the complexity of this phenomenon. Consequently, this complexity would be researched from different perspective and based on the results, different strategies of control and prevention would be defined. In general we prefer a mountain meadow with thousands of different flowers to a big farm with exactly the same plants.

REFERENCES

1. Aremu, A.O., Pakes, and Johnston, L. (2009), "The effect of locus of control in the reduction of corruption in the Nigerian police", *Policing: An International Journal of Police Strategies &Management,* Vol. 32 Iss 1 pp. 144 – 156.
2. Bayley, D., Perito, R. *(2011). Police Corruption*. United States Institute of Peace, Special Report 294, November 2011: 1-19.
3. Criminal Justice Commission (2001). *Is the Standing Commission of Inquiry a Successful Model for Anti-corruption Commissions*? Queensland Criminal Justice Commission (CJC), Canberra, http://www.ethicsinstitute.com/pdf/Corruption%20commission%20report.pdf
4. Fijnaut, C., Huberts, L. (2002). *Corruption, Integrity and Law Enforcement,* Kluwer Law International, ISBN 90-411-1866-7
5. Gottschalk, P., (2010),"Crime-based survey instrument for police integrity measurement", Policing: An International Journal of Police Strategies & Management, Vol. 33 Iss 1 pp. 52 – 68.
6. Huberts, L.W.J.C.; Lamboo, T.; Punch, M. (2003). Police Integrity in the Netherlands and the United States: Awareness and Alertness. *Police Practice and Research*, Vol. 4, No. 3, pp. 217–232
7. Jenks, D., Johnson, L. M., Matthews, T. (2012). *Examining Police Integrity: Categorizing Corruption Vignettes,*Working Paper No 40, January 2012, www.IPES.info, www.dcaf.ch www.coginta.org.
8. Kääriäinen, J.T., (2007). Trust in the Police in 16 European CountriesA Multilevel Analysis. *European Journal of Criminology,* Volume 4 (4): 409–435
9. Klockars, C.B. and Kutnjak Ivkovic´, S. (2003), "Measuring police integrity", in Piquero, A.R., Greene, J.R. and Hickman, M.J. (Eds), *Police Integrity and Ethics*, Wadsworth Publishing, Belmont, CA, pp. 1.3-1.20.
10. Knapp Commission, (1992). http://en.wikipedia.org/wiki/Knapp_Commission
11. Kolthoff, E., (2010). *The relation between Corruption and Human Rights in Police Work.* 32 EGPA Conference, 8-10 September 2010, Toulouse, France,http://www.law.kuleuven.be/integriteit/egpa/egpa2010/kolthoff_corruption-and-human-rights-in-police.pdf
12. Korupcija u Srbiji, iskustvo građana. Anketa UNDP, istraživanje sproveo TNS Medium Gallup Group, Izdavač, Republički zavod za statistiku Srbije, (2010), Beograd. Istraživanje je na sajtu: (http://webrzs.stat.gov.rs/WebSite/repository/documents/00/00/39/54/Korupcija_u_Srbiji_-_Iskustva_građana.pdf
13. Kutnjak Ivković, S. (2009). Rotten apples, rotten branches, and rotten orchards. *Criminology and Public Policy*, *8*, (4), 777-785.
14. Kutnjak Ivković, S., (2005),"Police (mis)behavior: a cross-cultural study of corruption seriousness", *Policing: An International Journal of Police Strategies & Management*, Vol. 28 Iss 3 pp. 546 – 566.
15. Kutnjak Ivkovic, S., (2009),"The Croatian police, police integrity, and transition toward democratic policing", *Policing: An International Journal of Police Strategies & Management*, Vol. 32 Iss 3 pp. 459 - 488
16. Kutnjak Ivkovic´, S. and Khechumyan, A., (2013). The state of police integrity in Armenia: findings from the police integrity survey, *Policing: An International Journal of Police Strategies and Management*, Vol. 36 No. 1, pp. 70 - 90.
17. Kutnjak Ivkovic´, S. and Sauerman, A. (2011), "Measuring the code of silence among the South African police: findings from a SAPS supervisor survey", in Gould, C. and Newham, G. (Eds), *Toward a Coherent Strategy for Crime Reduction in South Africa Beyond 2010*, Institute for Security Studies, Pretoria, pp. 74-87.
18. Kutnjak Ivkovic´, S. and Sauerman, A. (2013)."Curtailing the code of silence among the South African police", *Policing: An International Journal of Police Strategies & Management* Vol. 36 No. 1, 2013, pp. 175-198.
19. Kutnjak Ivkovic´, S. and Shelley, T.O. (2005), "The Bosnian police and police integrity: a continuing story", *European Journal of Criminology*, Vol. 2 No. 24, pp. 428-54.
20. Kutnjak Ivkovic´, S. and Shelley, T.O. (2007), "Police integrity and the Czech police officers", *International Journal of Comparative and Applied Criminal Justice*, Vol. 31 No. 1, pp. 21-49.
21. Kutnjak Ivkovic´, S. and Shelley, T.O. (2010), "The code of silence and disciplinary fairness: a comparison of Czech police supervisor and line officer views", *Policing: An International Journal of Police Strategies and Management*, Vol. 33 No. 3, pp. 548-74.
22. Kutnjak Ivkovic´, S. Kang,W. (2012). Police integrity in South Korea. *Policing: An International Journal of Police Strategies & Management*, *35*, (1): 76-103.
23. Meyer, M, Steyn, J. and Gopal, N. (2013),"Exploring the public parameter of police integrity", *Policing: An International Journal of Police Strategies & Management*, Vol. 36 Iss 1 pp. 140 – 156

24. Mollen Commission Report (1994). *New York City commission to investigate allegations of policecorruption and the anti-corruption procedures of the police department*. New York.

25. MORAN, J. (2005). 'Blue walls,' 'grey areas' and 'cleanups': Issues in the control of police corruption in England and Wales. *Crime, Law & Social Change*, 43 (1): 57–79.

26. Newburn, T., (1999). Understanding and preventingpolice corruption:lessons from the literature, *Home Office, Policing and Reducing Crime Unit Research, Development and Statistics Directorate 50 Queen Anne's Gate, London SW1H 9AT*

27. Police Integrity, England, Wales and Northern Ireland, securing and maintainingpublic confidence (1999). Home Office Communication DirectorateJune 1999.

28. Punch, M. (2000). Police Corruption and its Prevention, *European Journal on Criminal Policy and Research*, 8 (3), pp. 301-324.

29. ROYAL COMMISSION INTO THE NEW SOUTH WALES POLICE SERVICE FINAL REPORT, RCPS Report Volume 1.pdf - Police Integrity Commission, 1997.

30. Schafer, J., Martinelli, T., (2008),"First-line supervisor's perceptions of police integrity", *Policing: An International Journal of Police Strategies & Management*, Vol. 31 Iss 2 pp. 306 – 323.

31. Sellbom, M., Fischler, G., Ben-Porath, Y.S. (2007).Identifying Mmpi-2 Predictors of Police Officer Integrity and Misconduct. *Criminal Justice and Behavior,* Vol. 34 (8): 985-1004

32. Stinson, P., Liederbach, J., Brewer, S., Schmalzried, H., Mathna, B., Long, K., (2013),"A study of drug-related police corruption arrests", Policing: An International Journal of Police Strategies & Management, Vol. 36 Iss 3 pp. 491 – 511.

33. Strateško obaveštajna procena korupcije (2012). MUP Srbije. Twinning prijekat.

34. Tankebe, J. (2010). Public Confidence in the Police, Testing the Effects of Public Experiences of Police Corruption in Ghana. *British Journal of Criminology,*50, (2),296–319.

35. Väsquez, Carlos Ruiz, J. (2013), "Colombian police under fire: image, corruption and controls", Policing: An International Journal of Police Strategies & Management, Vol. 36 Iss 2 pp. 399 – 420.

36. Weitzer, R., (2002). Incidents of police misconduct and public opinion.*Journal of Criminal Justice*, 30 (5), 397– 408.

UDC: 316.653:343.352(497.7)“2013/2014“

ANALYSIS OF THE CITIZENS' ATTITUDES FOR DETECTION AND PREVENTION OF CORRUPTION IN THE REPUBLIC OF MACEDONIA

Cane T. Mojanoski[1]

University “St. Kliment Ohridski”, Bitola, Faculty of Security, Skopje

Abstract: The text represents the results of the surveys analysis conducted in 2013 and 2014, as well as other surveys conducted in the Republic of Macedonia which are associated with corruption. It is analyzed as a situation and practice of the society that adversely affects the overall social development, by slowing economic processes, exacerbating the social security and undermining notions and beliefs for the value of the principles, especially the principles of legality, equality, balance and freedom.

Corruption is established and expressed as a form of hidden and illegal reallocations and (mis)uses of the core of social power and authority. Using corruption and in conjunction with other mechanisms, party and state power are privatized and then converted into a market product. In this framework exchange or swap of the controlled part of political power and authority is conducted for material goods.

Corruption in modern states, despite being considered socially harmful, also is a reason for inefficiency of one state. Thus, main phenomenal forms of the corruption are: giving and receiving bribes, nepotism and abuse of the official position or function for personal benefit.

In this paper we will specifically analyze the assessments of the citizens about the ways to stop and prevent corruption. Namely, to the question “In your opinion how can corruption be detected and revealed, examinees in 2013 and 2014 responded as follows: by using the media was chosen by 19.83% of the respondents in 2013 and that number decreased to 19.17% in 2014. Then follows the opinion “using special investigative measures to detect corruption” with 14.88% in 2013 and respectively with 15.83% in 2014. Results are similar regarding the attitude “with inspection supervision of the administrative bodies” ranging from 14.13% in 2013 to 14.75% in 2014.

Keywords: Corruption, Prevention, Citizens, Research, Public.

INTRODUCTION

There isn't an international conference at which the problem of corruption was not mentioned, not only as a problem of individual states, but as a problem all over the world. Corruption threatens all modern states, especially states in transition. Effective control and fight against it involves the timely adoption of laws, building institutions (police, judiciary, law preventing money laundering, tax services, etc ...) and informing the community and the media about the dangers of corrupt activities. It is a factor that does harm the society. Together with other types of threats, corruption is a factor that binds all other forms of endangering society that seemingly cannot be connected.

The corruption exists in the society since ancient times. Despite this fact, the society has always denied the existence of corruption and corruptive practices in general. Corruption usually occurs in conjunction with greed, big social differences (e.g. poor public servants), decomposition and transformation of political and economic systems, war and post-war period, the change of political leaders, senior civil servants etc.

Globalization and global transition of all societies in the world are creating conditions for corruptive practices around the world. Corruption is a global problem. As a socially negative phenomenon, it has been defined already in Roman law. The crime of corruption is defined as the giving, receiving or soliciting used with the intent to influence officials in connection with their work (Pusič, 1989). The corruption is a sign of bleeding of the moral values of society. Therefore, corruption is regarded as immoral and harmful phenomenon in society because the bearers of social functions must advocate the common, not their own, private interests. The corruption can't only be considered as morally harmful, but also as the cause of the inefficiency of the state.

In terms of identifying the causes of corruption there are numerous approaches. It is estimated that in addition to the group of characteristics and contextual factors of corruption, such as poverty, war, isolation,

1 cmojanoski@fb.uklo.edu.mk

legal uncertainty and instability also there are two groups of factors that contribute to maintaining the high level of corruption that represent a kind of destructive mixture of open opportunities for corruption as systemic and institutional preconditions and at the same time present tendency towards corruption as political and cultural reasons (Stojiljković, nd, p. 11). Thus, the systemic and institutional corruption include: a) the poor state of public services in which dominates the "overpopulation and political domination logic loyalty of professional standards and the resulting measures of job insecurity and a modest salary; b) the widespread practice of avoiding payments of obligations to the state with the parallel c) limited offer resources that leads to the introduction of quotas and the existence of monopolies "(Stojiljković, nd, p. 12). The most devastating consequence seems, however, that is the existence of a mechanism of "money laundering", i.e. the formation of coupling between organized criminal groups and parts of the state apparatus,

Another factor that affects the maintenance of high levels of corruption was found in the traditionally formed political-cultural matrix and the way of people's behavior. For this there are numerous experiences and knowledge. We should mention the stories of Milovan Glišić, especially the anthological story about buying one and the same sugarloaf by which giving away the (local) powers are all right, as well as more than dramatic and far-reaching warning Archibald Reiss on the preferences of the Serbs to genuflect before power Warrants and loan sharks or in the Montenegrin tradition of strong anti-corruption the charge has a narrative about manhood Mark Miljanova. In modern speech the following slogan is used, "Big thieves have their cap removed, the small ones their head" or "politicians once had a vision, and now they have all reduced to the commission" (Stojiljković, nd, p. 12).

MATERIALS AND METHODS OF CORRUPTION'S REASEARCH

Furthermore a secondary analysis of a UNODC (United Nations Office on Drugs and Crime) has been conducted in the Republic of Macedonia in 2013 and a field research "Attitudes of the Republic of Macedonia on corruption." The investigations are done in the period from January 8-20 in 2013, 2014 and 2015 in the Republic of Macedonia. The selection of respondents was carried out by forming a research unit. In every research every fifth home (house) was elected, or every 20th appartment. The selection of respondents was carried out according to the principle nearest birthday in the family. A structured interview was conducted face to face. The instrument (Basis for discussion) was structured for several blocks of questions. In this paper we will present some of these results (Mojanoski, 2013, pp. 416-423).

The research instrument "basis for conversation" is structured in a way that includes six sets of data, namely: the first group includes demographic characteristics, the second includes knowledge about corruption, the third includes experience associated with corruption, the fourth state of corruption, the fifth part of preparedness and citizen commitment to the fight against corruption and the sixth part includes development and the fight against corruption. The structure of the question was different in the form (Mojanoski, 2013, p. 214).

The subject of analysis in this paper is the question of the assessment of contributions repressive and represive and repressive and preventive measures. They were given in the following form:

In your opinion, what could be the contribution of preventive measures in the fight against corruption? (Please answer YES or NO).		
	Yes	No
	1	0
1. the improvement and development of general legislation to eliminate or minimize the possibilities of corruption and the difference	□	□
2. the adoption and consistent implementation of personnel policies (selection, recruitment, promotion) in relation to the officials and civil servants which increases the integrity of the organs and institutions	□	□
3. the development of specialized anti-corruption education	□	□
4. the development of an information system and availability of information about corrupt acts and measures and activities in the fight against corruption	□	□
5. the implementation of protection against corruption of any organs and institutions	□	□
6. the adoption and implementation of a code of ethics among government officials and the personnel	□	□
7. Anything else, what?_____		

For the researchers (Interviewers) questionary diary and a mannual for accessing and securing approval for participation of citizens in the research were made. Also through training the principle of ranking was mastered.

RESULTS AND DISCUSSION

In the last decade, citizens and society in general in Macedonia became more aware of corruption and the fight against it became a priority in the political agenda of the country. The government pledged to fight corruption and key measures were undertaken to solve this issue, partly because of the obligations stemming from the EU accession process, partly because of the need to adapt the national legislation to the *acquis communautaires.*

The corruption occurs in the area of public, private and political sectors (Duyne, 1996). The subjects of corruption are the state officials at all levels, individuals in corporations and politicians at the local and state level. The most typical characteristic of corruption is concealed and covertly, but the influence of corruptive practices can be felt in everyday life. The corruptive activities in the field of public employees manifests favoring and services to people who are expected to have a benefit. The simplest form of corruption is bribery of public officials. The dominance of this practice in the institution, calls into question the integrity of the institution, or leads to the endemicity of corruption in state institutions. Corruption in the public sector greatly facilitates the spread of logic and understanding of public property and interests as "Alajbeg's straw", something in contrast to the private doesn't have the title, which is anyone's and everyone's, and mine (Stojiljkovic, nd, p. 12) .

Corruption in the private sector and politics is widespread throughout the world. Business people are motivated by the profitability of their business, and politicians want to preserve their power. The most typical form of corruption in this area is bribing in favor of political parties. It can occur in a variety of failures for an investment in some economic activities (for example, the distribution of grants, aid or other forms of state intervention in some sectors), or public-private partnership, whereby the coupling between private individuals and politicians reflects in the public justification of this act of the politicians ("Swedmilk"). The private business sector bribery does not just mean giving bribes to foreign public company clerks, but this implies bribery between companies in order to secure business transactions according to a survey of the Office of the United Nations Office on Drugs and Crime (UNODC), published in 2013. The results indicate that the lower incidence of bribe between the private and public sectors, the distribution of bribe-business business recorded a 3% and is an indication that there is a practice of this form of bribe in the Republic of Macedonia. This type of corruption is not to be equated with the usual marketing and related activity or relations with the public, but it is a practice whose specific aim is, through illegal means undermines the integrity of the recipient bribe in exchange for certain benefits of the bribe. The study confirmed that only 0.2% of the bribe giver have reported their experience to the authorities for this kind of business-business bribe. Also, about 5.3% of the surveyed company representatives decided, in the last 12 months prior to the implementation of this research that do not make large investments, which is estimated to be due to the fear that they were obliged to pay bribes to obtain needed services or licenses, thus bribe that can significantly influence the business activity of the company.

What is interesting is that the effects of conventional forms of crime are higher in farm businesses and economic activities, but it can also be significant both in terms of direct costs resulting from physical damage and indirect expenses in the form of insurance premiums, expenses for securing and lost investment opportunities. For example, in the Republic of Macedonia, nearly one of six companies, or 17.2% in various forms during the year, are a victim of the lure of external persons outside the company, and 5.4 times increase in the number of victims in this time period. Annual rates of theft in the private sector was 12.9%, 6.9% vandalism. It should be noted that 2.7% of the companies are victims of this kind of offenses. The rate of motor vehicle thefts is 0.5% of all cars in the possession of the company, from a victim who suffered are 2.4% of incidents were in companies. In addition, during the past 12 months of all the companies in the Republic of Macedonia 0.9% is a crime that can be linked to organized crime groups, or were victims of extortion.

56.3% of the companies in the Republic of Macedonia report the conventional offenses to the police. The results from the research suggest that the greater part, 82.6% of the representatives of the companies believe that the risk of crime for their company is stable compared with the previous 12 months, almost one in ten or 9.6% of them believe that it has risen and 7.2% believe that these forms are reduced. The fear of crime plays an important role in decision-making process among business leaders when talking about huge investments. Although there are some differences it can be noted that 68.7% of the companies in the Republic of Macedonia are using at least one security system to protect themselves from crime, and only 28.8% have some kind of form of insurance against economic costs resulting from the crime. Corruption along with other forms of crime represents a significant burden for the economic development of the country (Bisonjo, et al., 2013, p. 6).

The previous discussion suggests that perceptions of citizens in countries in transition "social pyramid of corruption" make small, everyday corruption whose actors were lower officials and citizens, and the main reason lies in widespread poverty and insecurity and its heights to which the predatory (predatory) new bourgeoisie which draws power from extralegal spillovers of public resources into private pockets. The predators of such forms consists of two major groups: a) those "big, successful entrepreneurs" who have come to their positions with the use of political support and monopoly privileges, and not through open market competition and b) the party workers and trustees at the forefront of non-privatized enterprises and public funds whose privileged position is determined by promoting party interests within which it is possible to "embed" their own interests (Stojiljkovic, nd, p. 14).

Contemporary analysis of state and political systems recognize that in parallel with the state system occurs and effectively acts as a criminalized, well organized, corruption system and as such it can be defined as a company that operates outside the control of the state and the public. As such, corruption system covers a number of criminals who operate in layered structures, similar to an entrepreneurial organization. These structures are governed by the rules and norms that are observed very strictly, which cannot be said of the laws of the country. In such an organization, the most important goals are to control the organization and the greater financial gain. Also, it is considered that, in these structures findings are harmonized with the latest techniques and forms of keeping the economy, i.e. they are oriented order to maximize profit (Barac, 2011, p. 18). The physical damage such tasks crashes and breaks down the foundations of the social system and morality. Thus, during the transition period, especially in a time of change of ownership relations, ruled unwritten principles "are fine." This formulation is basically related to the people from the economy and politics, which means avoiding legal procedures, but absence of state action mechanisms, creating tangible and financial benefits. For the Republic of Macedonia, it was a period when the country lived in the embargo by the southern neighbor, and such measures were taken over by the United Nations and to the northern neighbor. In such circumstances were created circumstances in which, despite all the capabilities of the police and other organs of the state fighting corruption was lukewarm or missing. And in the years that followed, corruption and corruption system have more or less freely developed, and the government saw them as a mechanism through which redistribution of national wealth was performed. The state is the most important and most powerful economic partner, and established mechanisms "licensing" and "legitimization" of work and business activities by government "licenses", or license, objectively good grounds for the flourishing of corruption. These and similar actions associated with the state and state organization have caused establishing a system of corruption that, by itself threatens the fundamental functions of the state. In such circumstances, the exercise of rights, but also the freelance game player is tied to the center of party power and the process of legitimization by the instrument of party patronage.

The absence of an organized action creates space for placing the question of how to prevent corruption. It is believed that a significant part of the new security concept is the prevention of corruption. It is generally considered that the state's response to combating corruption is building the system and creating a national policy of prevention and repression of corruption (Kaiser, 1996, p. 78). In this sense, it is expected that the country approaches the creation of anti-corruption policy in which all social institutions find basics and its role in the fight against corruption. The second area is the development of the world about the dangers of corruption. Therefore, activities associated with the development of awareness of the evil that corruption causes are undertaken, and institutions are encouraged to be responsible for troubleshooting. In this context the concern for internal security and the smooth social development of society, there must be responsible and synchronized actions of numerous state and social actors. Therefore, we can say that the anti-corruption policy is not just organs of detection, prosecution and trial, but it is a duty for the entire social policy of the society and all relationships arising from the economic sphere. Therefore, a more detailed analysis of the causes of corruption is impossible to determine if they do not perceive social, economic, political and other conditions, and in particular the situation in all areas of the state that are not directly confronted with corruption. As areas that are exposed to corruption and crime that occurs as economic, cultural, educational and environmental (Dobovšek, 2005). Each area is individually exposed to attacks.

Investing criminally gained money is a serious social problem. Today, as the biggest threat contemporary crime is considered to be investment of the criminally acquired money into legitimate businesses. This process is usually realized through money laundering and corruption. In such conditions, crime tends to enter the legal sphere of the economy and to become competitive economy within those industries that are more productive and more profitable. Such areas are construction, modern technologies, mining, oil and gas activities and related trade and intellectual services. A very interesting area is the education, especially high education. In reality many criminal enterprises do not have problem with money to start production, investments are covered by the proceeds of criminal activities, or occur as foreign investment from enterprises which have their headquarters in countries known as "tax havens". Such companies are competitive and destroy the healthy companies, bringing them to bankruptcy, liquidation or buying them. Such companies are coming to the various benefits, winning tenders for procurement, and their goals are typically generated by various pressures on policy and other state institutions, or use people to positions and through

their work and activities to generate immediate interests. This is so because for most of the activities of the criminal spectrum do not pay taxes, they become invisible and therefore do great damage to the country. Here when we add the fact that crime is increasingly internationally connected, then this activity for each country, especially for a small country like ours, the slightest action of international criminal organizations can cause significant damage to the economy. The interest of organized crime is to control and influence the policy of the state and its economic development. This interest is manifested through the creation of a social climate of uncertainty and social disorganization.

The area where corruption has fertile ground for development is lending. The new entrepreneurs need money. Landing is needed for opening the firm, but also for realizing a certain project. Related to this, there are criminal groups for higher purposes, such as groups for extortion and pressure, then the group of racketeering, a group of financial loan and usury and similar activities. These groups, ordinarily, are violent. Their goal was interest payments and high interest rates for loans and credits. So when situations occur due to high interest rates cannot repay the debt (to mention, Paying the debt is not the goal, the goal of the payment of interest and what follows) so the firm, house, car must be submitted to a criminal organization or, in turn, it must work as the criminal organization expects. In this connection, comes to collecting taxes from criminal organizations. This type of crime has not been sufficiently studied. Or better results about it are not visible enough. Therefore, it seems that this problem is bigger than we acknowledge, and its resolution requires the participation of the police, the judiciary and all state institutions, for example through programs to protect witnesses and their testimony. In the last decade of the twentieth century in some of the Eastern European transition countries at the scene was a "business" related to automobile theft and "offer good services to certain groups" to find such assets.

Corruption and money laundering is a secondary phase of the work of organized criminal groups. In the primary stage money is acquired, which is illegal, and by money laundering and corruption that money is invested they enter the legal sphere and thus criminals become directors of enterprises or even politicians. So now you can hear the statement that "every state has the Mafia," and that in some transitional countries, "the mafia has a country." In such conditions, crossing into the legal sphere is a modern trend of criminal organizations. It is a tendency in the whole world. Each technique aimed at converting unfairly or illegally acquired wealth to portray itself as an honest and legitimate income is called money laundering. Therefore it can be concluded that the primary objective of money laundering hides embezzlement and tax evasion, money order to become part of the legal system. Since money laundering is a complicated business, in the suppression of a criminal activity requires the participation of a significant number of entities, particularly state institutions, such as police, courts, banks, tax institutions, but also social subjects that will strengthen social and moral world.

The corruption can takes many forms. Most are manifested as bribery of persons who abuse their powers in the state or private sector. A particular problem is that corruption occurs in countries in transition, expressed through the abuse of civil servants, nepotism, embezzlement of funds, the machinations of the receipts and the like. In the private sector, most appears as favoring affairs, settlement, failure to report income and the like. However, corruption in this sector, gets special importance when it is associated with organized crime, which depends on the corruption and one without the other can not be developed.

The companies in the Republic of Macedonia as indicated by the research results of UNODC, 17.2% of them are victims of outside persons, 12.9% were stolen, 6.9% were victims of vandalism, 0.9% of extortion and 0.5% of theft of motor vehicles.The rate of crime reported to the police ranges from 100% for motor vehicle theft, 86.7% for theft, vandalism 52.9%, 34.6% for extortion and 12.1% for cases of fraud by external entities. 93.2% of the companies in the country are using at least one protective measure of security against crime. 82.6% of the companies stated that they considered that the risk of crime is stable for their business entity, and that 9.6% of them believe that the risk is on the rise, a 7.2% risk to be reduced in relation to the previous year (Bisonjo, et al., 2013, p. 8).

Data from Table 1 indicate that the bribe that companies pay in the Republic of Macedonia is in other forms, rather than in cash. The average value of the payment in cash is 17,349 denars or 282 euros or 82% of the average net wage in the country. Given the differences in prices in Europe and in the Republic of Macedonia, the average value of bribe amount corresponds to the value of 689 euros PKM 881 EUR-PPP which is less than the amount of the average value of bribe in the Western Balkans region, which is 881 EUR PKM. The table shows that citizens are at greater risk of corruption. The average amount paid by the lumber is 28,813 denars, or an average of 479 euros, that is expressed in the mean values of EUR 1,212 PKM (Bisonjo, et al., 2013, p. 20).

Table 1 *The average price paid bribe in cash from the companies and by private individuals (in money, euro in EURO-PKM) as a percentage of GDP per capita and as a percentage of the average monthly net salary, Republic of Macedonia (2010-2012)*

	Reference group	
Indicators	Population in Republic of Macedonia (2010)	Companies in Republic of Macedonia (2012)
Average value of bribe (MKD)	28813	17349
Average amount of bribe (MKD)	12000	8000
Average value of bribe (EUR)	470	282
Average amount of bribe (EUR-PKM)	1212	689
Average value of bribe as % of BDP *per capita* (2012)	12,6%	72%
Average value of bribe as % of average monthly net salary (2013)	136%	82%

Sources of additional indicators: national currency in the Republic of Macedonia Denar (MKD), EUR / MKD medium rate in 2012: 1 EUR = 61.5 MKD: National Bank of the Republic of Macedonia; EUR-PPP conversion and GDP per capita: Eurostat; average monthly net salary: Central Bureau of Statistics (CBS). See: (Bisonjo, et al., 2013, p. 21)

The biggest problem in preventing corruption is a shortage of professionals for its detection. The analyses showed that corruption brings profits to the one who offers some funding and the one who receives them, which is why no one will be logged. This is so because this particular man who would report corruption, he was not harmed, damaged the state, which, due to a variety of conditions in its organization or position of public officials lack adequate access and response in the fight against corruption. That is why many questions remain open and waiting for an answer.

The most significant forms of corruption are giving and getting bribery, nepotism - abuse of position (function) for private purposes. Proclaimed values - especially success at any cost - act as an incentive for the expansion of corrupt practices. When we talk about corruption, there are two types: (1) bribery which is given in exchange for licenses or services that are necessary for the exercise of legitimate activities and (2) a bribe in exchange for preferential treatment, for example, winning a contract to tender for the procurement even when you are not the best supplier. This second type of corruption is something completely different, because society as a whole pays the price, in the sense that one is not the best bidder gets permission to build, for example, theaters, monuments, highways, bridges, or airports, or what is the subject of the tender. This kind of corruption is actually stealing taxpayers. Preventing this form of corruption is impossible or insufficient only if it is done through the refinement of mechanisms of public procurement. Experience shows that the precise mechanisms are insufficient, if there are social conditions that corruption develops. The real answer to the fight against corruption was organized response of the state and the creation of social conditions for killing such forms (Lengviler, 2011, p. 20). Research results UNODC in 2013 saying that companies in the Republic of Macedonia, in 50.2% of cases bribe paid "to speed up the procedures that are associated with the business", in 9.6% "that can end the process" in 8.6% "to reduce consumes the proceedings or to obtain better treatment" and 2.8% "to obtain information". At the same time, almost one-quarter or 22.2% of bribes paid that is not used for a specific purpose, but according to the company The Company's responses to the "sweeteners" which is given to public officials, in the interest of the company, in order to improve communications in the future. In the last 12 months prior to the implementation of research, only 3.3% of the companies who paid bribes reported to official authorities. As the main causes of non-reporting bribe listed the following reasons: 21.6% believe that "a payment or gift is given as a sign of thank to public servant for doing the required service" in 20.0% answered that it was " it is report the bribery whwn nobody cares" and in 8.3% believe that," the company had (got) the benefit of the bribe "(Bisonjo, et al., 2013, p. 5).

Van Duyn (1999) divides corruption as the internal-external, individual-institutional and material, political and psychological. The dominant external corruption characterized by payment of services for the execution or non-execution of specific civil service jobs. Another form of external corruption is giving gifts to people in influential positions in society. Internal corruption is characterized by the activities of subordinate officers (bribe, giving gifts) to the clerk at the superior (employees) for achieving some advantage. For illustration, we will present the results of UNODC's research (Bisonjo, et al., 2013, p. 4) which says that 6.5% of the companies who had contacted with a public official paid a bribe to the public official. In Macedonia, the average participation in the provision of bribing between enterprises is almost equal to the share of giving bribe among citizens that is 6.2%.

The study confirmed that in the last 12 months, one of the ten companies had at least one direct contact with a public or a civil servant. Namely 6.5% of the companies have had contact with the public servant, and 4.8% responded that they had paid such a bribe. Broken down by sector, bribes 11.7% were paid in the construction sector , wholesale and retail 7.5% in electricity production, the supply of gas and water to 5.1% in the mucous industries - accommodation and food, transport and storage in 3.8%. When talking about the forms of corruption in the Republic of Macedonia, in 2013, 52% of bribes were paid in the food and beverage industry. However, the code word is payment in cash, out of high value paid bribe amount of 17349 denars, ie 689 EUR. If we observe the way of bribing then we can say that 36.1% pay bribes, in 8.9% payment has been implied. In 8.7% of the bribe was requested directly by public officials, and 18.5% in the name of servents 57.5% is offered by the company representatives without explicit or implicit constraint public servants (Bisonjo, et al., 2013, p . 7).

Individual corruption means the activity of the individual in the corruptive practices. This activity is discrete. It is done face to face, only between two people. Such acts characterize both participants giving and getting bribery (gifts). This type of corruption is the most widespread of all types of corruption.

From the perspective of the social damage the most dangerous is institutional corruption due to the impact of the breakdown of values in society. This form of corruption relates to processes in politics and in management of the state. The impact of this form of corruption on public opinion and public awareness is high. It causes a pronounced fear and uncertainty and the decline of morality among the majority population. It is manifested through certain forms of anomicity in society, especially of leave apaciteta institutions. Since the beginning of the transition, very gainful were proved to be jobs associated with the transformation of ownership and redistribution of wealth. In this way the contribution they made and certain points on the number of non-governmental organizations and foundations, which was oriented towards supporting various, not always clear to the end of the transfer. Thus, in the last period on the scene acted organization) usually nongovernmental, who performed at a certain level of economic activity (as an example of the construction of rural Water Supply, or were in operation to redistribute funds issued under imemnom donations). Here, one could point out certain level of international organizations, did not celebrate with the application of the principle of transparency about the method of selection of businesses, (as an example of specific training about the composition of public administration, public opinion research, to various forms of grants and ways of redistribution (Labovik , 2006, p. 56).

Corruption can be active and passive. Active corruption involves persons who provide some good and thus encourage a criminal offense. Passive corruption is characteristic for persons receiving "some good" in exchange performed a criminal offense in relation to the performance of their duties (McCormack, 1998). The most typical form of corruption is material corruption - giving bribe, which instantly brings benefits to both parties.

A special place takes the political corruption. It has multiple manifestation forms. Usually, lobbying encourages corrupt practices, but it is, in democratic states governed by law. Boundaries between lobbying and political corruption are not clear and insufficiently precise. The switching from one to another, usually is caused by the cultural characteristics of the social environment and are associated with representations and the principles of morality.

POSSIBILITIES FOR PREVENTING CORRUPTION

Opossing corruption is not based solely on repression. Contemporary trends in the field of combating all types of crime, turn toward prevention. The concept of prevention, according to Elvina Muratbegović (Muratbegović, 2007, p. 5) refers to the intervention as a primary form, that is, first, to certain events of the pre-prescribed substances and, second, it is bound to the prefix pre indicating temporary reaction, more precisely the reaction before manifest adverse effects. This term contains the totality of planned, designed and organizational measures taken which aims to eliminate or at least reduce direct or indirect causes of criminal behavior. Under the prevention imply only activities that are undertaken in the direction of preventing crime by the public, local communities, authorities and services in general, ie, they are activities that are associated with organized response to crime prevention. This opinion emphasizes that the concept of prevention gathers totality of all measures, tools and techniques beyond the scope of the criminal justice system. This response has an aim the company to reduce the various types of damage that are driven by the commission of the offense itself, or such other action that the country has marked and incriminated as criminal offenses.

When we talk about prevention primarily it is reffered to the social strategy. Social (social) reaction occurs as a constant in try to define not only prevention but also the policy of combating crime. Privacy crime prevention encompasses different levels of activity. Widest operating concept includes primary (ante delictum) activities. The aim is to prevent criminal behavior by them and to reduce their number before

some criminal act happens. Narrower concept of prevention is criminal and toolkit (post delictum). It acts preventively after committing the offense, (post judice) after conviction by final judgment, after postpenal help, and after applied criminal sanctions (Muratbegović, 2007, p. 5). So, under preventive activities involve a range of different measures, actions and procedures. It is the widest complex of modern criminal policies. Its interest does not end with just the phenomenon of crime (in the narrow sense), but the phenomenon of criminal behavior in general. Certain modern teaching and learning of prevention deals with the so called minor bad behaviors (especially in the treatment of minors) which can be classified into the domain of socio-pathological behavior in society (Muratbegović, 2007, p. 5).

Crime prevention includes the activities of the various entities that take preventive measures. That crime prevention measures can be taken by: the state bodies and the public authorities, non-governmental organizations' associations, private foundations, institutions, mass media, print, broadcast media, educational institutions, professional environment in the broadest sense of the word, religious institutions, as well as family fundamental social group of any society. The activity of the state itself in this area has focused on the adoption and expansion of legal projects, i.e. designing criminal legislation, and later operationalization through preventive measures and specialized police state agencies that deal with crime in the narrow and broad sense of its meaning. However, as we have noted prevention of crime is very often related to the implementation of certain measures by the citizens themselves, either individually or through some specialized organs, agencies, and associations formed spontaneous or planned, as well as other sectors of social life, such as sector information and the like (Krivokapic, 2006).

Preventing corruption is a challenge for every modern state. It comes to the fore especially in politically unstable systems. As indicators of instability are taken: Contempt opposition party blocks sharp conflict in society, disrupted ethnic relations, various forms of political friction and turbulence. In such conditions, especially when economic growth has decreased, then comes to the impoverishment of public officials but also to a weakening of the political, legal and economic control mechanisms of the state and society as a whole. There are many reasons why there is corruption, some of them are: (a) government with its policy on contracts, privatization and the granting of concessions, (advertising budget funds, subsidies to farmers, various social packages) provides financial benefits to individuals and companies (supports the development of several guests from different branches of the reduction of customs duties or taxes), and the subjects closer or "line" (financing of housing), who called his country of issue, approval for the exercise of the profession, for example, accountants, auditors, notaries, executors, police officers, to work in agencies ensuring etc.) of the Government of gain the greatest benefit; (b) tax evasion, especially when tax system discourages economic activity; (c) low salaries of civil and public servants (university staff is paid less than mediocre civil servant); (d) bribery of politicians in order to achieve best election results (in the period when elections are called, to "promote" projects of new jobs, which will be effective two months after the elections); (e) the courts do not respect the law, but they are selectively applied depending on the state and belonging to the ruling political structure (judicial function is becoming more and more familiar); (f) money laundering with comprehensive government assistance.

Preventive measures to reduce corruption (Council of Europe, 1998) include knowledge of the security factors based on the study of organized crime, terrorism, corruption and other sophisticated forms of crime. In the area of prevention of corruption must engage state institutions, local communities and individuals. The measures, which include the mentioned actors are: a) increasing transparency, checks and controls; b) promotion of competition and elimination of monopolies; c) informing the public; d) the creation of appropriate economic and social policies; e) the simplification and greater transparency of the various procedures; f) control of financial transactions; g) encouraging transparency and competitiveness in the political process; h) the introduction of a free press and independent media.

In the area of studying the perpetrator and victims of corruption, there are several problems due to specificity of corruption in which "there is no victim in the classical sense of the word," but as victim is considered the society as a whole (Ignjatovic, 2009). Similar problems are encountered in the analysis of the crime. Here occurs an objective problem that partially sentences these charges to the so-called "dark figure" (Arnaudovski, 2007, p. 147; Ignjatovic, 2009, p. 93). It is about the practice of the legal criminalization of "receiving" and "giving" bribe. In this case we have the intertwining roles of the victim and the perpetrator and the question is who would in practice report these crimes.

Important actors in the field of prevention of corruption are the state authorities who implement different strategies (changes in laws, limit the authority of persons with public authorities and stricter control of these individuals, changes in business practices and professional codes, control public announcements, the establishment of independent bodies to fight corruption and encouraging activities non-governmental organizations).

In a study of corruption in Macedonia in 2013-2015 was installed a battery of six questions dichotomous form, which asks citizens to declare what could be a contribution to preventive measures in the fight against corruption.

Table 2 *In your opinion, what could be the contribution of preventive measures in the fight against corruption? (Please answer YES or NO).*

	2013		2014		2015	
	yes	no	yes	no	yes	no
1. improvement and development of general legislation to eliminate or minimize the possibilities of corruption and the difference	1078	130	882	135	721	198
%	89,24	10,76	86,73	13,27	78,45	21,55
2. the adoption and consistent implementation of personnel policies (selection, recruitment, promotion) in relation to the officials and civil servants which increases the integrity of the organs and institutions	1030	178	842	175	700	218
%	85,26	14,74	82,79	17,21	76,25	23,75
3. the development of specialized anti-corruption education	986	223	804	213	664	254
%	81,56	18,44	79,06	20,94	72,33	27,67
4. the development of an information system and availability of information about corruptive acts and measures and activities in the fight against corruption	1013	194	813	204	696	222
%	83,93	16,07	79,94	20,06	75,82	24,18
5. the implementation of protection of the poor at corruption bodies and institutions	1071	136	850	167	712	206
%	88,73	11,27	83,58	16,42	77,56	22,44
6. the adoption and implementation of codes of ethics for the officials and the personnel of state	1015	193	837	180	631	281
%	84,02	15,98	82,30	17,70	69,19	30,81

The data presented in Table two shows that in 2013 a total of 1,208 respondents believe that crime can be prevented by "the improvement and development of the common law" as a prerequisite "for the elimination or minimization of corruption opportunities and difference". That year almost nine tens of respondents had a positive attitude for that in 2015, so at the beginning of this year, that number had dropped to less than eight tenths. Very interesting are the distributions associated with the view that crime prevention can be successfully implemented „with the adoption and consistent implementation of personnel policies (selection, recruitment, promotion) in relation to the officials and civil servants which increases the integrity of the organs and institutions." In 2013 was 85.26% have a positive answer, 82.79% in 2014 and 2015 drops to 76.25%. It is usually considered that education, training and awareness of public officials, private entrepreneurs and politicians on corruptive practice and its consequences can be positive influence to increasing the holy and responsibilities, and thus the prevention of corruption. Research results measured over the opinion under paragraph "with the development of specialized anti-corruption education", in 2013, the attitude of the check had four-fifths of the respondents, or 81.56%, 79.06% in 2014 and in 2015 dropped to less than three-quarters, ie 72.33%. It is common practice to educators across officials familiar with the permissible - illegal practices and consequences of corrupt behavior. Sometimes education in public schools varies greatly from practical work in the service. The impact of education must achieve a change in the professional (sub) culture (Dobovšek, 2005).

In every organized country a special attention is paid on the media and investigative journalism that significantly affect the transparency of corrupt practices. This process is not exempt from the sensational approach and highlights the prejudice which results in sentencing innocent people, institutions or corporations. The study particularly raised the issue assess how crime can be prevented if you pay attention to the development of "information system and the availability of information about corrupt acts, measures and activities in the fight against corruption"? Affirmative responses on this issue in 2013 would have been "yes" to 83.93% in 2014 with 79.94% of respondents in 2015 that number had dropped to 75.82%.

In relation to the assessment of how crime can be prevented if we increase the realization of "protection of the poor at corruption bodies and institutions", i.e. to improve the efficiency of treatment, affirmative answers to this paragraph indicate that in 2013 also identified 88.73% of the respondents, in 2014, that number was 83.58% in 2015 fell to 77.56%.

It is significant to mention that in transforming authorities, police reform on the model of community policing, include Dominica Labour infantry patrol, troubleshooting and testing the relationship between police and the community. This form of community policing was the result of estrangement between police and citizens. Police Activities under this model are oriented to increase cooperation with the citizens and the local community and increasing accountability in the exercise of police activities. Community policing is based on good cooperation with the citizens and the local community, joint identification and attempts to solve problems by consensus. A prerequisite for the exercise of such policing is the decentralization of police (Simonovic, 2006).

A significant factor of community policing is the decentralization of police activity. Community policing means hiring police officers who work for a long time in a particular community. This means that it would be good to hire a police officer who knows precisely living and working environment, problems and citizens and local communities. Community policing is based on close and tight relations with local communities and citizens in the neighborhood (neighborhood). One of the hypotheses community policing is a classic policing, which by itself cannot provide adequate results if there is too much distance and the ability to identify the real problems in the community. Distance influences that police officers patrolling in knots causing a decrease of contacts between police and citizens. Daily contacts between citizens and policemen must be constant and allow determination of the problems in the community and consensus in resolving minor or major problems. High quality work of the police in the community contributes to a greater willingness of people to cooperate with the police. (Simonovic, 2006).

This kind of work involves a redefinition of the objectives of the police activity that is related to the idea of determining and eliminating the root causes of problems in the community, and in this context the phenomenon of corruption.

CONCLUSION

The previous discussion has shown that corruption is a serious problem of modern society, especially in transitional societies. Such a society is ours. It is characterized by a transition process that takes too long to change the ownership relations, with underdeveloped legal regulations and the absence of dedicated social action and effort to fit in the way society, especially the problem of corruption. Such a practice was more pronounced in the gland decade of transition in which was the process of denationalization of ownership and the transition of ownership relations in the form of private property. Today, from a certain distance, it is estimated that the process in many of its features has criminal characteristics. The general organization of society is influenced to develop various forms of corruption. Corruption is divided into micro, mezzo and macro. In this respect an important role is that one of the police. Police usually can be partially successful in preventing and combating micro and mezzo corruption while macro corruption is too complex so that police officers could understand it, prevent and influence on it. Micro corruption includes minor crimes such as extortion in service, unjustified acceptance of gifts in the service and health care, schools, police and judiciary. Macro corruption refers to middle management, in customs, financial police, the police, the local community and so on. Macro corruption is related to the various activities of the government and public service announcements, construction of highways, airports, telecommunications, health centers, hospitals and so on.

The analysis of the results from the research confirmed that corruption is present in all parts of society in the Republic of Macedonia. In this context, the fact that one of ten companies in 2013 had at least one direct contact with public or civil servant which means that 6.5% of the companies were contacted. 4.8% of these, paid a bribe. Most bribes are paid in the construction sector to 11.7% in wholesale and retail 7.5% in electricity production, the supply of gas and water to 5.1% in the mucous industries - accommodation and food, transport and storage to 3.8%.

Forms of corruption in 2013 were 52% bribery charges in food and beverages, cash payments amounted to 689 EUR. According to ways bribery is estimated that in 36.1% of cases the bribe was paid explicitly, implicitly at 8.9%. Research results indicate that the social and organized activities should strengthen the mechanisms to prevent corruption. This does not mean that it should be reduced and repressive forms of prevention of corruption, but without a doubt it is a necessary response to organized crime. In this context, the role of the police is significant.

One of the issues that is an integral part of the debate about organized response to corruption is how much the educational system provides assumption as expert response to negative social phenomena and, in particular the corruption? The answer to this question is complex. And these research results indicate indirect knowledge, one of the main shortcomings in the fight against corruption and other forms of crime, the absence or insufficient definition of staff for these jobs. This especially sharpens in situations where the police work and the work on the fight against crime is treated as an omnibus profession. In this context,

society has an obligation to develop educational forms and to refer to specialist knowledge. In this context the form of recruitment in the organs for preventing and combating corruption should be seriously questioned. The current practice of acquiring specialized, specific knowledge through a form of education is incomplete, insufficiently effective. Therefore, it should be pointed out and it should be insisted on establishing and building a more complete education system at all levels, as well as on enriching the forms of lifelong learning.

The discussion of the results of the research showed that the company should increase its efforts to increase the overall security and trust in institutions for the fight against crime. This is achieved by strengthening the integrity of these institutions, increasing transparency and responsibility for the execution of tasks, as well as through the development of a broader concept of education of the population for support and participation in the fight against corruption and other negative phenomena. In that sense it is important to affirm the forms of community policing, and to encourage civic initiatives that lead to the creation of better living conditions.

REFERENCES

1. Clarke, R., ed., 1992. *Situational Crime Prevention: Successful Case Studies.* New York: Harrow and Heston.
2. Clarke, V. R., 2000. Situational Crime Prevention, Criminology and Social Values. In: R. Clarke, ed. *Ethical and Social Perspectives on Situational Crime Prevention.* Oxford: Hart Publishing.
3. Council of Europe, 1998. *Programme of Action against Corruption.* [Online] Available at: http://www.coe.fr/corrupt/eaction3a.htm [Accessed 04 May 2014].
4. Dobovšek, B., 2005. *Korupcija, lobiranje in neformalne mreže.* Ljubljana, Ministrstvo za notranje zadeve, Policija, Generalna policijska uprava, Uprava kriminalistične policije.
5. Ignjatović, Đ., 1992. *Kriminologija.* Beograd: Nomos.
6. Ignjatović, Đ., 2009. *Kriminologija.* Beograd: Pravni fakultet u Beogradu.
7. Ignjatović, Đ., 2009. *Metodologija istraživanja kriminaliteta.* Beograd: Pravni fakultet u Beogradu.
8. Krivokapić, V., 2006. *Prevencija kriminaliteta.* Sarajevo: s.n.
9. Muratbegović, E., 2007. *Prevencija kriminaliteta (Compendium of Crime Prevention and Crime Control).* Sarajevo, Priština: Fakultet za kriminalistiku, kriminologiju i bezbednosne studije.
10. Stojiljković, Z., n.d. *Karakter i logika korupcije.* [Online] Available at: http://media.institut-alternativa.org/2013/04/KARAKTER-I-LOGIKA-KORUPCIJE-dr-Stojiljkovic.pdf [пристапено на 4.05.2014]; [Accessed 04 May 2014].
11. Арнаудовски, Љ., 2007. *Криминологија.* Скопје: 2-ри Август-С Штип.
12. Бараћ, В., ed., 2011. *Корупција, власт, држава.* 275 ed. Beograd: Савет за борбу против корупције.
13. Бисоњо, Е., Јандл, М., Карбаљо, Л. М. & Реитерер, Ф., 2013. *Бизнис, корупција и криминал во Република Македонија: Влијанието на поткупот и другите форми на криминал врз приватните фирми,* Скопје: UNDOC.
14. Кајзер, Г., 1996. *Криминологија.* Скопје: Александарија.
15. Лабовиќ, М., 2006. *Власта корумпира.* Скопје: Де Гама.
16. Ленгвилер, И., 2011. *Политичка економија контролисања корупције.* Београд, Савет за борбу против корупције, pp. 19-23.
17. Мојаноски, Ц. Т., 2012. *Методологија на безбедносните науки - истражувачка постапка.* Скопје: Факултет за безбедност.
18. Мојаноски, Ц. Т., 2012. *Методологија на безбедносните науки - Основи.* Скопје: Факултет за безбедност.
19. Мојаноски, Ц. Т., 2013. *Методологија на безбедносните науки - аналитички постапки, Книга III.* Скопје: s.n.
20. Симоновић, Б., 2006. *Рад полиције у заједници (Community policing).* Бања Лука: Министарство унутрашњих послова Републике Српске, Управа за полицијско образовање, Висока школа унурашњих послова.

UDC: 316.752:316.624
316.64:316.48
32.019.5

THE ROLE OF TRADITIONAL VALUES AND ADVERTISING DISCOURSE IN CREATION OF MODERN CONFLICT[1]

Srdjan Milasinovic[2]
Goran Milosevic[3]
The Academy of Criminalistic and Police Studies, Belgrade
Zoran Jevtovic[4]
University of Niš, Faculty of Philosophy

Abstract: By careful analysis of the content of Archibald Reiss message in his book "Listen, Serbs", the authors study the significance and role of traditional values of Serbian people – patriotism, courage, hospitality, honesty and respect for opponents, faith and charity, aim to, together with comparative analysis with advertising discourse during the conflicts in ex-Yugoslavia, construct a modern model of crisis communication. From the context of the symbolic organization of messages and their hidden meanings, the authors stress the importance of communication control and information management during the conflict, as otherwise the moral panic and chaos arise. Developing McDougall's *instinct theory* that determines the behaviour of individuals and entire social groups, the authors remind us that Reiss was the first to realize the human mind as a centre of social activity responsible for further development of individuals and nations. Starting from the assumption that the social life is primarily political and preoccupied with the question of redistribution of power, the authors discuss the construction of the security framework within the community, warning it of the problem of unequal access to information. By influencing the modelling of media images of a group or society its propaganda activities is enabled, which is essential during the crisis or emergency situation, as their number will increase in the future.

Keywords: social values, propaganda, symbols, moral panics, public opinion, conflictology.

Modern society is under continuous reviewing process since its orientation values permanently transform, meaning that the concept of security and crisis is more dynamic and more dependent upon the ideas and performances that ensure continuity of internal stability and external political environment. Crimea, Ukraine, Afghanistan, Syria, Egypt, a number of "orange", "stuffed", "Umbrella" and similar revolutions, the "Arab Spring" of political unrest, acts of terrorism and corruption scandals, increased racial and religious tensions, nuclear accidents, drought and floods, in addition to the permanent economic crisis and strikes are just a part of everyday shakings that have changed the geopolitical architecture and threaten planetary stability. It has been confirmed that, in practice, the crises often occur when the core values of a society find themselves under threat, when the community creates a sense of urgency to react and when there is a high degree of uncertainty about the way of their addressing. Breaking the former Yugoslavia represents an illustrative example: the safety of citizens was firstly disrupted by the threat and the action of separatist-chauvinist republican leadership, followed by the series of crimes and murders as well as announcements of upcoming violence and harm, awakening a deep sense of fear and insecurity; at a time when it was still possible to prevent conflict, current political and military leadership did not have responsibility for the rapid decision-making at the operational level, while the essential information about the causes and consequences were unavailable to the general public. The following fractures in all areas and all parties showed the fragility of socialist societies, but also the inappropriate public bureaucracies to the conflicting actions. The signals of ethnic, religious, gender or any misunderstanding that preceded the conflict situations should only be identified, interpreted and appropriately responded on time!

In uncertain circumstances, people tend to see what they expect.[5] The interpretation of information is therefore the focus of security processes, as, in this way, the upcoming threats are adequately assessed,

1 The paper was written under the Project No. 179008, implemented by the University of Belgrade – Faculty of Political Sciences, and the University of Niš – Faculty of Philosophy as well as Project No. 179045 (The Academy of Criminalistic and Police Studies), which is funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia.
2 srdjan.milasinovic@kpa.edu.rs
3 goran.milosevic@kpa.edu.rs
4 zjevtovic@beotel.net
5 Jervis, R.: *Perception and Misperception in International Politics*, 1976, 144-152.

together with determination of the mechanisms and means of their elimination. In order to avert a crisis it has to attract the attention of wider public, prominent promoters that may affect the political and security processing, and create an institutional form in order to oppose it. Essentially, all the crises and conflicts hide information, a vast amount of diverse and often manipulative information targeting to undermine the psychological stability of the system. With their lack, politicians and crisis managers cannot make the right decisions, meaning that the information battle is a precursor of field activities. Hence, the crisis communication is caused by the political and security actors who deliberately influence the media and network communication, that, by agenda setting, framing and priming, produce certain mental projections. Thus, construction of meaning becomes a form of domination crisis, with a new paradox: the higher the role in establishing the specific interests and values the lower the need for resorting to violence (whether it is legitimate or not).[6] Starting from the fact that societies are not homogenous structure with generally accepted values and interests, the authors further studied the relation of conflicts and media discourse,[7] following the forms of power and domination. Redesigning the theory of instincts, William McDougall[8] that determines the behaviour of individuals and entire social groups, we remind that Rudolph Archibald Reiss had also seen the human mind as a centre of social activity from which the character of individuals and nations was further developed. Testifying "primarily on the moral staggering of the political and intellectual elite of the newly created Serbian state" the Swiss scientist focuses to, for that period still unknown phenomenon of "trapped state", indicating the systemic corruption that destroys invisible security order.[9]

FORMATION OF CONSCIOUSNESS AND THE POWER OF INFORMATION

In an increasingly turbulent, more urban and more vividly materialistic world social problems are accelerated and increased (arms race, crime, terrorism, violence, various forms of deviance ....), meaning also that the conflicting debates opportunities are growing, as well. However, instead of conventional weapons or nuclear missiles today wars are conducted in words, images and information. Collective notion creates symbolic confusion, moral panic and informative chaos, but in order to be on top of such strategies, it is necessary to have a perfect logistics.[10] The human mind is limited when it comes to the analysis of the complex and volatile situation, since the mass of data causes many stimuli, hindering the ability to process them and decide in time. The behaviour of individuals and social groups is increasingly shaping and directing using mass media propaganda, which provides the crisis communication with the role that has never had in its history. The roots of such interpretations should be sought during the Cold War. When America, using atomic weapons, bombed Hiroshima and Nagasaki, it has parallel engagement in two fronts: economic reconstruction and transformation of the Japanese consciousness. Our problem, it was stated in 1945 in an educational movie for the occupying forces, "rests inside the brain of the Japanese mind. There are seventy million of people in Japan, physically identical to any other brain in the world, made of exactly the same material as ours. These brains, like our brains may do a good and a bad thing, depending on the ideas that are embedded in them."[11]

McDougall notes that the mind is characterized by the ability to associate events with the network of neurons that activate the consciousness, but performance of the creative process requires communication. Simply, our brain thinks in metaphors that are discourse accessible, and their strengthening results in narratives distributed by the mass media construct public opinion! The problem is that, in a moment of confusion, in situations when there is a discrepancy between the beliefs of the individual and what the individual is offered by media (image of reality) there is a certain kind of dissonance that can be used for the expansion of social panic. For example, you have just passed the city's streets and made sure that the snow covers their surface slowly, but looking at media images that sensationally invite citizens to stay in their homes because

6 Manuel Castells observes that "the institutionalization of resorting to violence in the state and its institutions creates the context of the domination in which the cultural production of meaning can demonstrate its effectiveness" (2004: 32)

7 The media discourse implies "a collection of verbal, oral, written or printed, auditory, visual or audiovisual messages that the sender informs the recipient with the meanings" (Miletić, M. and Miletić, N.: *Komunikološki leksikon*, 2012: 45).

8 Famous English psychologist meritorious for the development of *the theory of instincts* and *social psychology*. He was an opponent of behaviorism, arguing that the man's behavior is always targeted, defending the thesis that individuals are always motivated by a significant number of inherited instincts. See more in: McDougall, William (1909): *An Introduction to Social Psychology* (2nd ed.), London: Methuen & Co, pp. 1–2 (n13–14 in electronic fields).

9 Uroš Šuvaković points out that Reiss was always treated as a criminologist, while the huge sociological contribution in "the study of social stratification, political sociology, sociology of elites and the sociology of religion" was neglected. (2012: 363).

10 The Pentagon, more than half a century, gave a remarkable statement: "Logistics is the procedure whereby a potential of the nation is transferred to its security forces, in time of peace as well as in time of war." Baron Antoine de Jomini, military theorist, historian and founder of the Military Academy of Imperial Russia was the first to realize the connection between Napoleon's long-range artillery and Chappe's telegraph, noting that in a complex system of vectors, production, transportation and confrontations the most important is *control of folders flows*, because only the power of quality information provides a good logistics!

11 The movie of American army, 1945, cited in: John W. Dower: *Embracing Defeat; Japan in the Wake of World War II* (New York; Norton, 2000), pp. 215.

"blizzard threatens with disaster" you check whether your friends or family members are safe, spreading euphoria away. That is the theory *of cognitive dissonance*, which in 1957 Festinger recognized as an important stage in the process of persuasion. The individual differences among the groups and the public are easy to eliminate by centralized activities, using combination of emotional and cognitive processing. In the media mediated society, crises and their flows depend on the information packets and their interpretation. The power of creating the dominant social structure and narratives becomes the part of the security activities, undeclared everyday war across the globe, hiding the battle for various forms of influence.[12] The picture of the world is being built based to the knowledge and relationships in a given time; by changing information the image is changing itself!

In a globalized world, the axe of social identification is embedded in a media platform with four semantic configurations: consumerism (consumption), cosmopolitanism (ideologically, politically and religiously), multiculturalism and networked individualism. Conceptual, religious, political, ethnic or interest conflicts are not only a struggle for power and the power of individuals and groups: they are also the ways to form a governing state policy which expresses a degree of unity of society, regardless of how unity is forcibly imposed and maintained. The signs, mediated by media messages, create software abstractions that are faithful copies of reality. When thousands or millions of people read the same newspaper or watch the same TV programs having the impression that they are the members of the same community, they gain a sense of monolithic power. The imposed opinion means the imposed reality, the reduction of reflective attitude, control of characters and meanings. The security is not emphasized, but is implied! The job of crisis services is hence complicated and responsible, caused by using the elasticity of the political elite and the support of the citizens; hence, they must work to eliminate unwanted processes. A number of challenges arises, from the rough form of physical violence by individuals and groups, and the spread of the various modified forms of terrorism (including cyber space), to the state interventionism and construction of internal conflicts and a climate of fear.[13] The free flow of goods and people – "laissez faire, laissez passer" theoretically spreads the freedom in general, but in practice it turns into opposite, by spreading subversive or modified forms of violence and terror.

Images, ideas and feelings in our minds are increasingly created as a result of projected media meaning as our experience, past, present and future are replaced. Thus, the structures of space and time define images that we use to decide on real conflicts, objects and events. Conflict can be created, glossed over, minimized or increased by propaganda, whereas it is important who manages the information flows, what the dominant activities are, whether the information sources are credible, how they echo in public and why certain measures represent the optimal solution. As pointed out by theorists "propaganda is always facing only nicer side of truth, with unpleasant facts being concealed or denied".[14] The propaganda war is never fair because all parties involved in the conflict present their views, strategies and objectives, using different means and methods. Video liquidation of hostages, cutting off their body parts or beheadings is today's integral part of the content of global networks. Fair play under the pressure of the market and profits is lost, while the battle for attention and influence changes the crisis paradigm. The problem is the lack of time that is also economized, because decisions about the war and the peace are made in minutes, even shorter! Crucial is the space of conflict that was dislocated to the time frames, never being the case before.

CRISIS COMMUNICATIONS AND MEDIA STATEMENTS

There is more misunderstanding and discord on the planet, both among countries and among crimogenic communities. We live in an age of fear that due to the huge production of signs and meanings colonize every moment of our lives. The media keep reminding us how the society in which we live is in a crisis, so that the information about earthquakes, tsunamis, terrorist actions, demonstrations, strikes, murder, rape and other crimes, roll like waves on TV screens or in the press. Inspiration is increasingly sought in the media content or activities of "Facebook", "Twitter" and similar social networks, while the battle for security often moves into cyberspace.[15] Evidence that illustrates these claims: four Muslims with British citizenship were arrested in Cardiff planning to blow up the London Stock Exchange, are members of Birmingham cell that had planned deadly attacks across Britain, as well as the foursome who was convicted of planning

12 Propaganda commonly used half-truths, misinformation, stereotypes, and rumors, everything that is not recognized by the legislation in a community. See more in: Milašinović and Jevtović: *Sociologija*, 2014: 355.

13 Fear is often defined as "an emotional reaction to the perception, real or exaggerated, of the danger," notes Dominique Moisi, noting a new connection between the fear that is increasingly present in Western societies and the weakening of democratic ideals. According to: Moisi, 2012, 112.

14 Paul Virilio and Sylvre Lotringer claim that "war machine are not only explosives, but also a communication". See in: *Pure war*, 2012, pp. 29.

15 "Surviving Boston bomber Dzhokhar Tsarnaev in the investigation admitted that he and his brother learned how to make a bomb from express-pots with the help of Al Qaeda online magazine "Inspire". The aim of the journal is recruiting young Muslims from the US, Britain, Australia and Canada for jihad and articles in the journal are titled such as: "How to make a bomb in my mom's kitchen" or "You have the right to freedom to light a fire bomb".

attacks with explosives "toy car" at a military base in Luton regularly read the online edition of the journal Al Qaeda. By addition to these digital terrorist workshops, the digital sermons of radical Islamic religious teachers available at many sites, a potential conflict of unimaginable proportions is created.

Crisis communication involves unexpected and security risk event that generates a high degree of uncertainty, panic, fear or threats. The power and potential of this communication are reflected in the procedures which eliminate or minimize the impact of the crisis. "The whole process involves several basic stages: 1) establishment of a crisis team; 2) establishment of a network of internal communication within the service; 3) determination of the team leaders for crisis communication (including the spokesperson); 4) development of the project and the simulation of crisis; 5) determination of the target groups; 6) creating key messages; and, 7) determining the most effective methods of communication."[16] All crises are characterized by unpredictability, severity, duration, lack of communication and a desire of their actors for publicity. The control of the flood strike in Vojvodina (threat to the tens of thousands of homes in the zone near Romania and Serbia border) or an explosion in ammunition factory in Užice (three workers were killed) imply different activities and media coverage. As long as the authorities are unaware of severity of the situation, analysts cannot treat a particular situation as a crisis situation. The failures could be caused by nature to humans, but the cause of conflict lies in the system's inability to master disorders. Hence, the information management in crisis and conflict situations is gaining in its importance.

The security environment media do not represent ordinary technological tools or neutral technical channels in the mission of redistribution of symbolic meanings. Douglas Kellner puts media in the centre of political life, stressing that "contemporary forms of culture with its attraction shape and stimulate the consumers' demand and create a system of consumer values", directly linking the modern society and media culture as a sphere of constant turmoil and change.[17] Internet, with social networks and a number of digital platforms has fundamentally reshaped the process of content management, articulating meaning in a given direction defined in the arcane power centres. Computer Data processing since the 1980s has significantly improved speed, range and data exchange in the security sphere. The digital age has redesigned social relations by bringing into focus the concepts of control, collaboration and supervision. Thus, the conflict paradigm is extended because the networked society is based on the production of conflicting images in order to overlap boundaries between real and mediated space in a more sophisticated manner. The will of individuals is created by selecting the testimonies, while the consciousness, emotions and actions are affected by combined methods and tools. Articulation of the media performances, through new forms and with new meanings and relational systems, creates a special kind of *visual thinking*.[18] It leads to the social commission, producing dialectical interdependence: the idea prepares the ground for practical operation, while the activities in the public space present only practical realization of promotional imposed opinions!

Powerful development of technology brings new opportunities for the emergence of crises and conflict events. As a consequence, our planet has become a house of risk, whereby the activities of a country or even ethnic communities have a dramatic impact on the overall population. This applies to the devastating crises such as natural disasters, international and internal disruptions in vital goods and services supplying, industrial and nuclear accidents, fires in warehouses and hotels, airplanes and ships, civil unrest and other social conflicts, terrorist attacks on prominent leaders and ordinary citizens, kidnapping, famine and epidemics. The already mentioned Dominique Moisi states that the modern world is governed by three basic emotions (fear, hope and humiliation). In conflictological sense they are more important than rage, despair, hate, resentment, anger, love, honour and solidarity. Their importance is in proximity to the concept of trust, which is critical in any crisis situation because it is the way in which nations and peoples respond to the challenges they face!

CONCLUSION

As a skilled psychologist and criminologist, Archibald Reiss noted that people in crisis situations rather *believe in what they want* but in reality, in which you reside and shape themselves. Exploring the predispositions and values of the Serbian people before, during and after the First World War (elements of symbolic politics), he noted the power of motivation as a way to significantly shape public opinion. Clearly stressing the virtues ("Your people are brave… patriotic… hospitable… democratic, clear minded...") and disadvantages ("You are danglers... you lose the pride ahead of wealth... you become terribly ungrateful… you are jealous to more educated, classier and more advanced than you..."),[19] visionary warned that the whole nations in hard times rather take the emotional than cognitive perceptions. The origins of this orientation were recognized in national bias and loyalty to the leaders, by identifying the institutional embeddedness

16 Milašinović and Jevtović, 2013: 80.
17 Kellner: *Medijska kultura*, 2004, pp.30.
18 Arnhajm, R., *Vizuelno mišljenje*, Univerzitet umetnosti u Beogradu, Belgrade, 1985.
19 Archibald, R. (2006): *Listen, Serbs*, 1997, pp. 2-14.

and tradition as the bonds of deep belief in already alienated and corrupted elite. He noticed that the traditional values misused in the propaganda patterns represent fertile ground for the emergence of crises, but also the permanent system instability. Mechanisms for dominant image framing Reiss was not able to recognize since, as a foreigner, was unaware of the power of spoken messages and their power in the sphere of public communication.

Almost a century later, but in terms of socialized communication, we talk about the relationship between the human mind and the decision-making processes in crisis and conflict situations. The desire for persuasion is as old as mankind, but in the last few decades, the technologies speeded up and the understanding of reality without their use is impossible. Thus, we come to the understanding of the existence of parallel processes: the daily *production of reality* and its *media representation*. The image that the media send during the conflict is extremely important to detect, transmit, increase and decrease crisis situations. The essence of the change is in the perception that the strength of the state is determined by the measure of creation and management information provided to the public. Experts recognize that in "thick mediated political context of crisis management the ability to win the public's attention and reputation for accuracy and reliability becomes the primary political and administrative priority."[20] Media narratives trigger and reinforce certain behaviours, interpretations and evaluations, linking thoughts, emotions and actions, leading to solutions that are suggested from crisis centres. The degree of control of the information flow increases with the dimensioning of a crisis situation while a potential inconsistency of data leads to the formation of moral panic and fear. The greater the discrepancy between the official and alternative media, the greater the rumours, half-information and spins as well as the conflict to expand.

Holistic nature of the information enables their direction in moments of decision-making, which represents a new kind of social power the sphere of security. Numerous occurrences over which man has no control (climate change, natural disasters, biological wars, terrorism...) will be explained by the media images, offering possible solutions. Conflicting paradigms will be based on information dominance, whereby the management of information flows will be the key to national security. The twenty-first century changes the traditional geopolitical relations, as the leading forces, by combining nanotechnology, biotechnology, information technology and neurotechnology transform social responsibility. The conceptions of crises and conflicts are significantly changed nowadays, but a small number of individuals understand that, in accordance with the new reality, qualitative changes at all levels must be done.

REFERENCES

1. Archibald, R. (2006): Listen, Serbs, Dečje novine, Gornji Milanovac, Serbian Historical Museum, The Union of Associations of 1912-1920Liberation Wars and Descendants, Belgrade.
2. Virilio, P. and Lotringer, S. (2012): Pure War: Twenty-Five Years Later, Center for Media and Communications, Faculty of Media and Communications, Belgrade.
3. Castells, M. (2014): Communication Power, Klio, Belgrade.
4. Miletic, M. and Miletic, N .: Komunikološki leksikon, Megatrend, Belgrade.
5. Moisi D. (2012): Geopolitika emocija, Klio, Belgrade.
6. Milašinović, S. and Jevtović, Z. (2014): Sociologija, ACPS, Belgrade.
7. Milašinović, S. and Jevtović, Z. (2013): Metodologija istraživanja konflikata i komuniciranje u savremenom društvu, edition: Asphaleia, vol. 6, ACPS, Belgrade.
8. McDougall, W. (1909): An Introduction to Social Psychology (2nd ed.), London: Methuen & Co.
9. Festinger; L. (1957): A Theory of cognitive dissonance, Evanstan II. Row, Peterson.
10. Šuvaković, U. (2012): Doprinos Arčibalda Rajsa sociološkom proučavanju međuratnog srpskog društva, Collection: Sto godina sociologije u Srbiji (ed. Antonić, S.), Sociološki pregled, Vol. XLV, no. 1, Belgrade.
11. Dower, W. J. (2000): Embracing Defeat; Japan in the Wake of World War II, Norton, New York.
12. Jervis, R. (1976): Perception and misperception in International Politics, Princeton University Press, Princeton.
13. Seymour-Ure, C. (2003): Prime Ministers and the Media: Issues of power and control, Blackwell, Maiden.

20 Seymour-Ure, C.: *Prime Ministers and the Media: Issues of power and control*, 2003: 137.

UDC: 502.3:504.5:621.43.068
629.3

SOME MODELS OF AIR POLLUTION ASSESSMENT IN ROAD TRANSPORT

Stevo Jacimovski[1]
Slobodan Miladinovic[2]
The Academy of Criminalistic and Police Studies, Belgrade
Snezana Stojicic[3]
Venezija Ilijazi[4]
The Ministry of Interior of the Republic of Serbia

Abstract: Motor vehicles are mobile sources of pollutants and their number has been increasing day by day, making them growing air pollutants both inside and outside urban areas, throughout the year. According to the IPCC (Intergovernmental Panel on Climate Change) the share of harmful gases emission compared to other potential pollutants is 13%. The combustion of gasoline and other petroleum products in motor vehicles in the air at low altitudes produces numerous hazardous ingredients of air pollution (soot, nitrogen oxides, sulfur oxides, carbon monoxide, organic peroxides, lead, cadmium, etc.). It is considered that exhaust gases from motor vehicles, perhaps contribute most to air pollution, especially in larger cities. In Serbia, poor quality of fuel causes high concentration of sulfur and lead in the air, which represents very serious health problem. Illustrative examples show the way in which the pollution concentration is assessed in urban areas.

Keywords: mobile sources, air pollution, traffic.

INTRODUCTION

Transportation of people and goods is closely associated with the economic development.Transport is significant and necessary part of contemporary society, but its prevalence and intensity are the factors which contribute to certain adverse effects. Traffic congestion makes the environment in cities less pleasant, reduce the level of life quality, but also reduce the effectiveness and efficiency of the transport system by increasing travel time, increasing fuel consumption and others.

From the environmental point of view a significant negative effect of transport is air pollution. Combustion of each spent liter of fossil fuel produces approximately 100 g of carbon monoxide, 20 g of volatile organic compounds, 30 g of nitrogen oxides, 2.5 kg of carbon dioxide and many other harmful and toxic substances such as lead compounds, sulfur and solid particles. All these compounds to some extent lead to air pollution, whether directly influencing the health or globally, for example, causing the greenhouse effect.

In recent decades, it is estimated that in cities (depending on the economic development and the number of mobile sources) share of air pollution originating from mobile sources ranges from 30% to 70%. In the US, the share of air pollution originating from mobile sources of total air pollution is 40%.

Car transport is the most massive form of road transport. The number of cars in the world is incessantly growing. Thus, for example, number of cars in 1900 was 11 thousand, in 1950- 54 million, in 1970-181 million, in 1982-330 million. It is estimated that there are about billion of cars in the world today. Unfortunately, car transport represents one of the basic sources of air pollution (especially large cities) and has a negative impact on health of the population. Practically, all contemporary cars have internal combustion engines. Each of them (if in use) emits around 3kg of harmful substances into the atmosphere every day. In the exhaust gases of motor vehicles around 200 of different substances are observed. The most common are: lead, nitrogen oxides, sulfur, carbon, carbon monoxide, hydrocarbons, soot, benz (a) pyrene, etc.[5]

The level of the combustion and composition of emitted exhaust gases depend on the type and characteristics of the engine.Most cars have petrol engines, although there arehave been more and more cars with diesel engines lately. Gasoline represents a mixture of liquid hydrocarbons-pentane, hexane, heptane, oc-

1 stevo.jacimovski@kpa.edu.rs
2 slobodan.miladinovic@kpa.edu.rs
3 snezana.stojicic@mup.gov.rs
4 venezija.ilijazi@mup.gov.rs
5 Жданов, 2012

tane, nonane, decane. Combustion of the fuel causes very many harmful substances, as a result of non-equilibrium conditions of combustion and the presence of various impurities that remain in the refining of oil and additives (tetramethyl and tetraethyl lead) which are added as anti-knock and substances that increase the octane value of fuel. In the diesel engine exhaust gases there is very much soot and dust, but no lead compounds and toxic oxides of carbon, since diesel fuel is practically completely burned. The amount of hydrocarbons (which does not burn or does not completely burn) in the exhaust gas increases significantly when the engine is running at low rpm or at a time of increasing speed when starting the vehicle (eg. at the traffic lights). In these situations, the number of unburned particles increases 10 times more than in the normal mode of operation. In particular, the negative impact on the ecological situation is the fact that in our country vehicles whose lifetime is mostly over 10 years are used[6].

MODELS OF AIR POLLUTION ASSESSMENT IN THE ROAD TRANSPORT

Assessments of air pollution distribution from mobile sources present a very complicated task. The process of combustion, emissions of harmful substances and their diffusion in the atmosphere around the source is extremely complex task and still insufficiently studied. Vehicles in traffic are regarded as linear mobile sources or as surface sources when convoy of vehicles is observed. These sources are nonstationary and inhomogeneous and operate in complex urban conditions. The use of accurate methods of calculating emissions of air pollution based on differential equations of hydro-thermodynamics is very problematic. Therefore, there is a relatively small number of methods and models which are treated by this issue[7].

The ecological calculations of air pollution from mobile sources apply simplified models based on experimental data and empirical relations.It is clear that these methods do not have a universal character and have limited application area. As a rule, the authors of different proposed models, regardless of the strong possibilities of information technology in terms of the application of numerical methods, create simple methods by which the essence of the analyzed process is often overlooked.

The first task that should be solved when creating the assessment theory of negative effects of road traffic on the atmosphere is the choice of assessment methodology of dispersion admixtures into the air environment.

To obtain the authentic characteristics of atmospheric pollution due to emissions of exhaust gases sources in road traffic it is necessary to conduct numerous tests and measuring of large scale concentration during the years, which is very expensive.

Therefore, the problem is in practice solved by creating physical and analytical (mathematical) models of the emission process and the dispersion of harmful substances into the atmosphere. These models must have adequate accuracy for the specific task being solved. If the calculation assessment, according to the chosen model, consistent with the appropriate accuracy to the measurement results, then the number of measurements can be reduced and in certain standard situations (eg. at point sources) completely eliminated.

When modeling the transfer of substances through the atmosphere three main aspects are analyzed:

- Source of pollution (its characteristics)
- The process of transfer by taking into consideration the chemical reactions that occur in the atmosphere, the existence of natural and artificial obstacles, the characteristics of the local terrain, weather conditions, water surface, the process of deposition of pollutants, etc.
- Data on the effect of these harmful substances on the environment (eg, concentration limits)

Methods of studying meteorological regimes and air pollution of the atmosphere are divided into:

– empirical - statistical;

– statistical;

– analog modeling;

– mathematical modeling.

The empirical-statistical and statistical methods connect different meteorological parameters and properties of the base surface. These methods include regression and autoregression models.

Statistical models are used, for example, for the calculation of mean values of atmospheric pollution. To find the regression equation, as a rule, Gaussian model is used.

6 Statistical Yearbook, 2012
7 Берлянд,1975

Mathematical models are divided into two categories: energy and hydrodynamic models.

Energy models are designed to study the meteorological regime in the ground layer of air above the observed settlement. The equation of heat balance makes the basis of the method.

Hydrodynamic modeling method is the most perspective. It is based on system of equations describing the meteorological regime of formation of air currents in the settlement depending on the vertical and horizontal components of the wind speed, temperature, specific humidity, horizontal and vertical pressure gradient, Coriolis force and other physical parameters.

Basically we can distinguish four main directions in which modeling of admixtures dispersion and solid particles in the atmosphere is developed.

1) Using statistical models based on the Gaussian distribution function. In these models dispersion models intended for planar base surface are used, and they are modified by introducing empirical coefficients, which include possible redistribution of concentration in the vicinity of buildings and obstacles.
2) Modeling of flows in street "canyons" based on transport-diffusion equations
3) Physical modeling in the aerodynamic tubes. Similar experiments enable evaluation of some characteristics of admixture dispersion for given weather conditions. At the same time this method enables determining the parameters used in the modeling, eg- airflow along the street for different wind directions can be estimated.
4) Creating a model based on a complex approach: comparative analysis of real experimental results of numerical modeling and physical modeling. In that way you can build parametric models of the distribution of admixtures in street "canyons" depending on the meteorological conditions: wind speed and direction, temperature and humidity of the atmosphere and so on.

MODELS WITH SOLVING THE EQUATIONS OF TURBULENT DIFFUSION

In the area G there is a homogeneous road of length L oriented along the axis y. It is assumed that all vehicles move at the same speed, which is constant and is V. The wind at angle α, with speed *U*, in relation to axis *x* is directed towards the road. It is assumed that the speed of wind in area G does not depend on the arrangement, speed and characteristics of vehicles. The concentration of admixtures in the vicinity of the road depends on the amount of exhaust gases emitted by all vehicles that are also located on the stretch of road L and which represent mobile point sources of admixtures of constant intensity q. It is assumed that the appearance of vehicles on a stretch of road L, is random series of events that is subject of Poisson`s distribution with constant events intensity λ. It is necessary to find the concentration of admixtures in the safe area G emitted by vehicles in traffic.

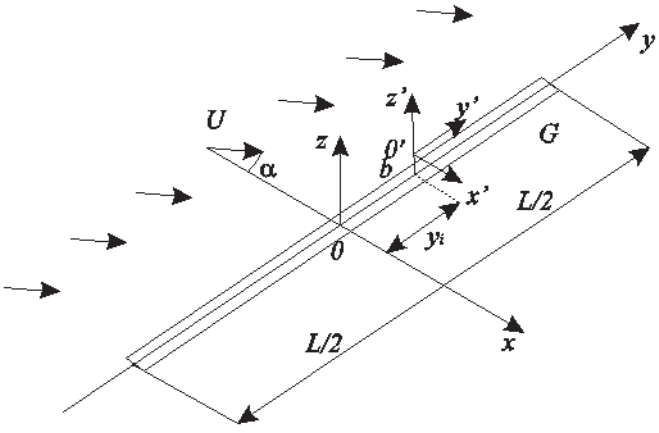


Figure 1 *Schematic presentation of the movement of vehicles on stretch of road of length L*

It is the nonstationary admixture dispersion from mobile sources. If using a moving coordinate system *O' x' y'z'* related to vehicle moving at a constant speed, you may transfer to a task that is described by the

stationary equation of admixture diffusion from point source located at the point with coordinates $x' = 0$, $y' = 0$, $z' = 0$

$$U_x' \frac{\partial C}{\partial x} + U_y' \frac{\partial C}{\partial y} + U_z' \frac{\partial C}{\partial z} = \frac{\partial}{\partial x}(K_x \frac{\partial C}{\partial x}) + \frac{\partial}{\partial y}(K_y \frac{\partial C}{\partial y}) + \frac{\partial}{\partial z}(K_z \frac{\partial C}{\partial z}) + q\delta(x', y', z') \quad (1)$$

where C is the admixture concentration, δ -Dirac, K_x, K_y, K_z coefficients of turbulent diffusion. Relative spreed of wind in moving coordinate system has components

$$U_x' = U\cos\alpha, \quad U_y' = U\sin\alpha - V \quad U_z' = W \quad (2)$$

Assuming that the wind speed does not depend on the height and that the coefficients , K_x, K_y, K_z are constant, the solution of the equation (1) is of the form[8]:

$$C(x', y', z') = q\exp\left(\frac{U_x' x'}{2K_x} + \frac{U_y' y'}{2K_y} + \frac{U_z' z'}{2K_z} - \frac{1}{2}\sqrt{\frac{x'^2}{K_x} + \frac{y'^2}{K_y} + \frac{z'^2}{K_z}}\sqrt{\frac{U_x'^2}{K_x} + \frac{U_y'^2}{K_y} + \frac{U_z'^2}{K_z}}\right) /$$

$$\left(4\pi\sqrt{K_x K_y K_z}\sqrt{\frac{x'^2}{K_x} + \frac{y'^2}{K_y} + \frac{z'^2}{K_z}}\right) \quad (3)$$

In the stationary coordinate system $Oxyz$, $x = x$, $y = y - y_i$, $z = z - b$ solution (2) can be written in the form

$$C^+(y_i, x, y, z) = q\exp\left(\frac{U_x x\cos\alpha}{2K_x} + \frac{(U_y\sin\alpha - V)(y - y_i)}{2K_y} + \frac{W(z-b)}{2K_z} - \right.$$

$$\left. \frac{1}{2}\sqrt{\frac{x^2}{K_x} + \frac{(y-y_i)^2}{K_y} + \frac{(z-b)^2}{K_z}}\sqrt{\frac{U^2\cos^2\alpha}{K_x} + \frac{(U\sin\alpha - V)^2}{K_y} + \frac{W^2}{K_z}}\right) /$$

$$\left(4\pi\sqrt{K_x K_y K_z}\sqrt{\frac{x^2}{K_x} + \frac{(y-y_i)^2}{K_y} + \frac{(z-b)^2}{K_z}}\right) \quad (4)$$

Here y_i is the position of a moving source in the system $Oxyz$. To calculate boundary condition $\partial C(y_i, x, y, 0)/\partial z = 0$ an imaginary source is introduced symmetrically in relation to the horizontal plane z, whose concentration is determined by the expression of

$$C^-(y_i, x, y, z) = q\exp\left(\frac{U_x x\cos\alpha}{2K_x} + \frac{(U_y\sin\alpha - V)(y - y_i)}{2K_y} - \frac{W(z+b)}{2K_z} - \right.$$

$$\left. -\frac{1}{2}\sqrt{\frac{x^2}{K_x} + \frac{(y-y_i)^2}{K_y} + \frac{(z+b)^2}{K_z}}\sqrt{\frac{U^2\cos^2\alpha}{K_x} + \frac{(U\sin\alpha - V)^2}{K_y} + \frac{W^2}{K_z}}\right) /$$

$$\left(4\pi\sqrt{K_x K_y K_z}\sqrt{\frac{x^2}{K_x} + \frac{(y-y_i)^2}{K_y} + \frac{(z+b)^2}{K_z}}\right) \quad (5)$$

Solution for concentration is of form $C(y_i, x, y, z) = C^+(y_i, x, y, z) + C^-(y_i, x, y, z)$. Overall concentration of admixtures $C_{uk}(y_i, x, y, z)$ in an arbitrary point with coordinates (x, y, z) from random number of vehicles $\tilde{N}$ which are located on the monitored stretch of road length L is defined as :

$$C_{uk}(x, y, z) = \sum_{i=1}^{\tilde{N}} C(y_i, x, y, z)$$

8 Марчук Г.И., 1982

The intervals between the appearance of the vehicle at the auto route are Δt, which are arranged according to Poison`s distribution

$p(\Delta t)=\lambda exp\ (-\lambda \Delta t)$. Mathematical expectancy of distance $\Delta y=V\,\Delta t$ between vehicles is $(\Delta y)=V/\lambda$.

Length of the column of vehicles is the sum of a random number of random variables $\tilde{L}=\sum_{i=1}^{\tilde{N}}\Delta y_i$. Mathematical expectancy of the length of the column is

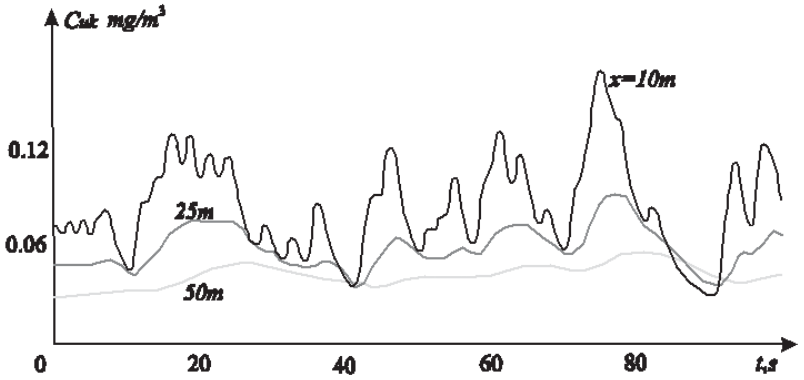


Figure 2 *The dependence of the concentration of admixtures on time at various distances x from the road*

$N=(\tilde{N})=(L)/(\Delta y)=\lambda L/V$. *Mean concentration of exhaust gases is* $\overline{C}_{uk}=\frac{\lambda}{V}\int_{-0.5L}^{0.5L}C(y_i,x,y,z)dy_i$

For the numerical determination of the concentration of carbon monoxide, according to relation (), following parameter values have been taken[9]:

$$L=1000\,m;\ b=0.5\,m;\ \lambda=0.5\,s^{-1};\ \alpha=0;\ V=12.5\,m/s;\ U=3\,m/s,$$

$$W=0\,m/s;\ K_x=K_y=67\,m^2/s;\ K_z=26\,m^2/s;\ q_{CO}=0.12\,g/s$$

If we want to approximate a non-stationary transmission and dispersion of admixtures for vehicles that accidentally appear according to Poisson`s distribution, using the model of admixtures diffusion at the straight stationary source of constant intensity, we have to solve the equation with the appropriate boundary conditions[10]

$$U\cos\alpha\frac{\partial C}{\partial x}+W\frac{\partial C}{\partial z}=K_x\frac{\partial^2 C}{\partial x^2}+K_z\frac{\partial^2 C}{\partial z^2}+Q\delta(x,z-b)$$

$$C\to 0,\quad x\to\pm\infty\quad z\to\infty\quad \partial C(x,0)/\partial z=0 \tag{7}$$

Here Q represents total source intensity. For this case, the solution is

$$C(x,z)=\frac{Q}{2\pi\sqrt{K_xK_y}}[K_0\left(0.5\sqrt{\frac{U^2\cos^2\alpha}{K_x}+\frac{W^2}{K_z}}\sqrt{\frac{x^2}{K_x}+\frac{(z-b)^2}{K_z}}\right)\exp\left(\frac{xU\cos\alpha}{2K_x}+\frac{(z-b)W}{2K_z}\right)+$$

$$+K_0\left(0.5\sqrt{\frac{U^2\cos^2\alpha}{K_x}+\frac{W^2}{K_z}}\sqrt{\frac{x^2}{K_x}+\frac{(z+b)^2}{K_z}}\right)\exp\left(\frac{xU\cos\alpha}{2K_x}+\frac{(z+b)W}{2K_z}\right)] \tag{8}$$

where K_0 is MacDonald`s function (Bessel`s function of imaginary argument).[11]

In this part, the setting and aproximate solution of the task for dispersion of admixtures and finding admixture concentration are given for the moving vehicles and whose occurrence on the observed road is a random process which is subject to Poisson`s distribution.

9 Русзкий А.В., 1996
10 Филиппов И.Г., 1995
11 Янке Ф., 1964

STATISTICAL MODELS

Different versions of Gaussian models are most widely used, such as, for example American models HIWAY-2, CALINE-4 (California Line Source Model), GM (General Motors), GFLSM (General Finite Line Source Model), Finnish model– CAR-FMI (Contaminants in the Air from a road, By the Finnish Meteorological Institute).

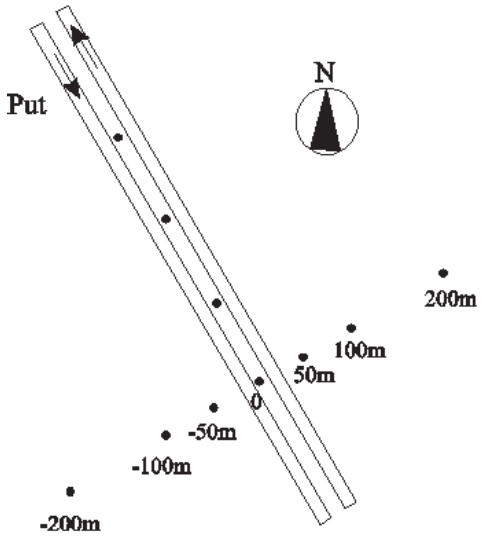


Figure 3 *Arrangement of receptors for measuring the concentration of admixtures by the roadside*

In models HIWAY-2 and CALINE-4 the concentration is calculated in case of final linear source with arbitrary wind direction ; in the calculation, the source is divided into series of elements for which the concentration is calculated which is then summarised. Model GFLSM is based on formulas for infinite linear source. Statistical models are based on the assumption that pollutants have Gaussian distribution and the concentration in the observed point in the wind direction can be calculated through generalised Gaussian equation.These models are widely used because of their simplicity and the solutions which are in accordance with the experiments. Gaussian models are officially recommended to meteorological services of the Union countries by the European Economic Comission.

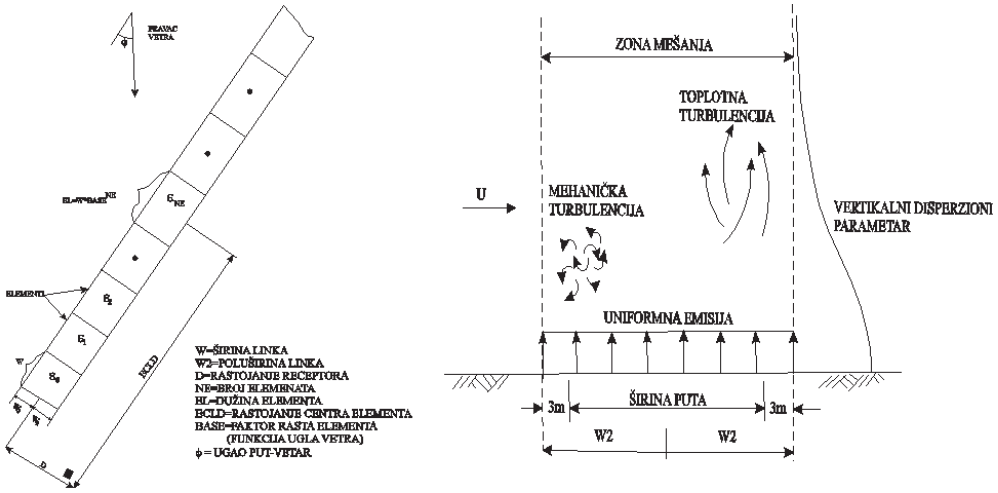


Figure 4 *Arrangement of road elements (left) and the zone of turbulence (right) which is used in tools CALINE4*

CALINE 4 divides the road into series of elements that are calculated for the single concentrations, and then the concentrations are summarised in order to determine the total concentration for certain receptors on the given locations. Position and length of the corresponding elemnts is determined by the formula[12]

$$EL = W * BASE^{NE} \tag{9}$$

where EL-element length, W-element width, NE- element number, BASE-element factor determined as

$$BASE = 1.1 + \frac{\varphi^3}{2.2 \cdot 10^5} \tag{10}$$

where angle is expressed in degrees.

Among the models that use Gaussian approach to calculating the concentration of admixtures one of the most famous is used in the software tool CALINE 4.

Među modelima koji koriste Gausov pristup računanju koncentracije primesa jedan od poznatijih se koristi u softverskom alatu CALINE 4. In the model CALINE-4 the concentration is calculated in case of final linear source with arbitrary wind direction ; in the calculation, the source is divided into series of elements for which the concentration is calculated which is then summarised. Dispersion of admixtures along the coordinate axis is observed according to Gaussian distribution.

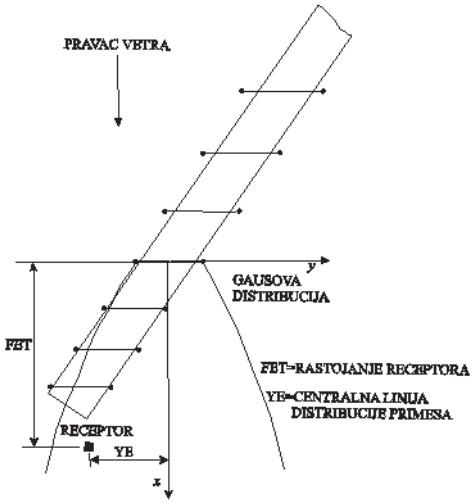


Figure 5 *Schematic view of admixture concentration dispersion with Gaussian model in the tool CALINE4*

Concentration which is registered by the receptor is according to this model

$$C = \frac{q}{2\pi u \sigma_y \sigma_z}\{\exp[\frac{-(z-H)^2}{2\sigma_z^2}] + \exp[\frac{-(z+H)^2}{2\sigma_z^2}]\}\int_{y_1}^{y_2} \exp(\frac{-y^2}{2\sigma_y^2})dy \tag{11}$$

here q is the intensity of admixture sources , u wind speed, H source speed, $\sigma_y \sigma_z$ horizontal and vertical dispersion parameters

In equation (11), are horizontal and vertical dispersion of admixture distribution. To determine these dispersions the following relations are used:

$$\sigma_y = Ax^a; \sigma_z = Bx^b \tag{12}$$

where *A, a, B, b* coefficients that depend on the stability of the atmosphere and surface relief and are determined experimentally.

Table 1 *Parameters for calculating the dispersion*

		A	a	B	b			A	a	B	b
Highly unstable	(A)	0,527	0,865	0,28	0,90	Neutral	(D)	0,128	0,905	0,20	0,76
Unstable	(B)	0,371	0,866	0,23	0,85	Stable	(E)	0,098	0,902	0,15	0,73
Slightly unstable	(C)	0,209	0,897	0,22	0,80	Slightly stable	(F)	0,065	0.902	0 12	0,67

12 D.L.Coe, 1998

As $\sigma_y \sigma_z$ are functions from x, but not from y, we can write $p = \frac{y}{\sigma_y}$

$$C = \frac{q}{\sqrt{2\pi} u \sigma_z} \{\exp[\frac{-(z-H)^2}{2\sigma_z^2}] + \exp[\frac{-(z+H)^2}{2\sigma_z^2}]\} \frac{1}{\sqrt{2\pi}} \int_{y_1/\sigma_y}^{y_2/\sigma_y} \exp(\frac{-p^2}{2}) dp \quad (13)$$

where

$$PD = \frac{1}{\sqrt{2\pi}} \int_{y_1/\sigma_y}^{y_2/\sigma_y} \exp(\frac{-p^2}{2}) dp \quad (14)$$

the function of normal distribution of density probability.

Total admixture concentration which is registered by the receptor is determined as a sum of single source concentration.The picture shows a screen form of tool CALINE4[13].

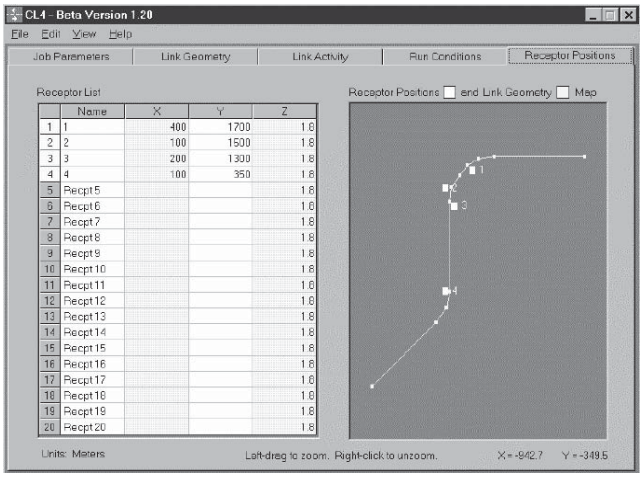


Figure 6 *A screen form of tool CALINE4*

To illustrate the capabilities of the software tool CALINE4, the highway that runs through the urban settlement is taken as an example. Arrangement of receptors and links is given in picture 7.

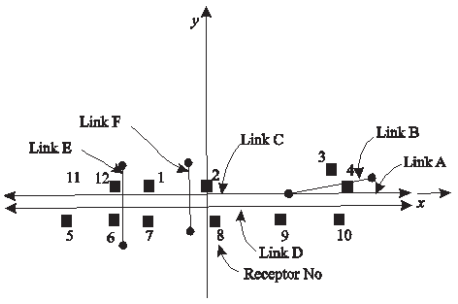


Figure 7 *The arrangement of links (elements) of the road and receptors near the highway*

If we adopt the necessary parameters, then in this case concentration CO i NO_2 can be obtained, one hour after they get into the atmosphere. Those concentrations are represented in 3D view in the pictures (). The parameters are as follows: wind speed 1m/s, class of atmosphere stability 6 (F), outside temperature 15 ^{0}C, aerodynamic coefficient of roughness of relief 100 cm, height at which thermal turbulence occurs due to solar heating of the soil 1000 m, existing background of relevant admixtures 5 10^{-6}.

13 D.L.Coe,1998

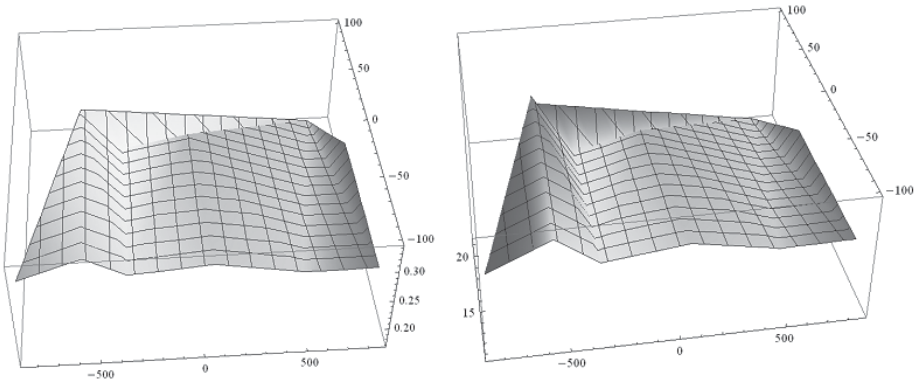


Figure 8 *3Dview of CO concentration (left) and NO_2 (right) for the given example*

SEMI-EMPIRICAL MODELS

In the ecological calculations of air pollution from mobile sources much simplified models based on experimental data and empirical relationships are applied. It is clear that these methods do not have a universal character and have limited application area. As a rule, the authors of different proposed models, regardless of the strong possibilities of information technology in terms of the application of numerical methods, create simple methods with which we often lose sight of the essence of the analyzed process.

One of the first models that have been proposed for estimating the amount of air pollution requires information on the amount of harmful substances emitted per unit of traveled road by each vehicle in the monitored area. Knowing the total traffic of the monitored area mass of harmful substances emitted into the atmosphere can be calculated. The amount of emitted substances is corrected depending on the technical regularity of vehicles and exploitation time. This model is significant because it allows us to shift from qualitative assessment of air pollution to the quantitative assessment of harmful substances emitted for an arbitrary period of time (month, quarter, year).

The later methods repaired the shortcomings of the original model in terms of the analysis of air pollution emission vehicles to individual groups of vehicles (passenger cars, trucks and buses). For certain groups their specificity has been taken into consideration: for passenger vehicles the volume of the engine, for trucks their capacity and for buses their dimensions. The mode of movement as a factor that contributes to the emission of harmful substances into the atmosphere has also been considered. Later models calculated the mass of air pollution emitted as the sum of the mass emitted in constant motion and mass emitted at a stanstill of vehicles. The mass of emitted air pollution is calculated based on traveled road during continual motion and based on the time of the vehicle at a standstill. Furthermore, in newer models mass of emitted air pollution is calculated in relation to the mode of transport in urban conditions (acceleration, braking, idling, delays at intersections). The improvement of this method is the fact that the parameters required for the calculation of air pollution can be obtained directly, and not from a statistical estimate. The latest models allow us to individually assess a wide range of emissions of harmful substances: oxides of carbon, nitrogen, sulfur, hydrocarbons, soot, lead compounds, formaldehyde, benz (a) pyrene.

Assessment of air pollution will be performed by computation on an illustrative example.

We will observe a city street without slope and rise of 2 km in length with an intersection where traffic is regulated by traffic light. Vehicles involved in traffic will be divided in eight classes:

I. local cars

II. Foreign cars

III. Vans and minibuses

IV. Buses with gasoline engines

V. Buses with diesel engines

VI. Freight vehicles with gasoline engines

VII. Freight vehicles with diesel engines up to 12 tons

VIII. Freight vehicles with diesel engines over 12 tons

Calculation for estimates of emission of harmful materials is carried out for the following materials: carbon monoxide, nitrogen oxides, hydrocarbons, particulate matter, sulfur dioxide, formaldehyde and benz (a) pyrene.

Emission of i substance in g/s during the transport of road vehicles along the road length L(km) is determined with the formula[14]

$$M_{Li} = \frac{L}{3600} \sum_{i}^{k} M_{k,i}^{P} G_k k_{v_{k,i}} \quad (15)$$

where:

$M_{k,i}^{P}$ (g/km) emitted mass of i substance of the vehicle of k group of vehicles, which is determined from the Table 2.

k-vehicle class number

(1/hour)-number of vehicles of k class which pass through an imaginary cross-section of road per unit of time in both direction

$k_{v_{k,i}}$ - correction coefficient, which includes an average speed of vehicles v_k (km/hour) and which is determined from Table 2

Table 2

Class	Emission (g/km)						
	CO	NO_x	CH	PM	SO_2	formaldehyde	benz(a)pyrene
I	5,0	1,3	1,1	0,03	0,03	0,005	0,4 10^{-6}
II	2,0	0,7	0,4	0,02	0,03	0,002	0,2 10^{-6}
III	12,0	2,0	2,5	0,08	0,06	0,011	0,8 10^{-6}
IV	35,0	5,2	8,5	-	0,04	0,04	1,2 10^{-6}
V	7,0	6,0	5,0	0,3	0,07	0,025	2,0 10^{-6}
VI	60,0	5,2	10,0	-	0,05	0,05	4,0 10^{-6}
VII	9,0	7,0	5,5	0,4	0,10	0,025	2,0 10^{-6}
VIII	12,0	8,0	6,5	0,5	0,12	0,03	2,4 10^{-6}

Traffic intensity is determined from Table 3

Table 3

	Speed of movement V_k (km/hour)												
	10	15	20	25	30	35	40	45	50	60	75	80	100
$k_{vk,i}$	1,35	1,28	1,2	1,1	1,0	0,88	0,75	0,63	0,5	0,3	0,45	0,5	0,65

Table 4

Ulica	Number of vehicles								Speed of movement km/hour		
	I	II	III	IV	V	VI	VII	VIII	I,II,III	IV,V	VI,VII,VIII
	171	88	67	12	-	-	1	-	60	40	40

The emission of harmful substances in the area of the intersection regulated by traffic lights is determined by the formula[15]

$$M_{Ri} = \frac{R}{40} \sum_{n=1}^{N_c} \sum_{k=1}^{N_{kl}} M_{R_{i,k}} G_{k,n} \quad (16)$$

where:

R (min)- the duration of the red and yellow traffic lights

N_c - number of cycles at traffic lights of red and yellow lights for a period of 20 minutes

N_{kl} – Vehicle class number

14 Молодцов, 2014

15 Молодцов, 2014

(g/min)- the emitted amount of *i* harmful materials from *k* vehicle class which are at a standstill at the traffic light

$G_{k,n}$ - number of vehicles of *k* class which are at a standstill at the end of cycle *n*-tog at the traffic light

Values $M_{Ri,\,k}$ are determined from Table 5

Table 5

Class	Emission (g/min)						
	CO	NO_x	CH	PM	SO_2	Formaldeh.	Benz(a)pyr.
I	0,8	0,02	0,12	0,02	0,006	0,0005	0,4 10^{-6}
II	0,3	0,01	0,05	0,01	0,006	0,0003	0,2 10^{-6}
III	2,0	0,04	0,25	0,04	0,012	0,0011	0,8 10^{-6}
IV	4,0	0,08	0,9	-	0,009	0,4	1,2 10^{-6}
V	1,1	0,11	0,6	0,2	0,015	0,0025	1,6 10^{-6}
VI	10,0	0,12	1,2	-	0,009	0,005	4,0 10^{-6}
VII	1,5	0,12	0,6	0,23	0,02	0,0025	2,0 10^{-6}
VIII	12,0	8,0	6,5	0,5	0,12	0,03	2,5 10^{-6}

Number of of vehicles that are stopped at an intersection for a period of time of 20 minutes is given in Table 5

Table 6

Intersection	Time of a standstill in min	Number of vehicles in classes							
		I	II	III	IV	V	VI	VII	VIII
	0,77	237	120	74	9	-	12	3	-

Using the formulas (15) i (16) and data from Tables (2)-(7) we find the amount of harmful substances emitted for our example. Results are given in Table 7.

Table 7

	Emission (g/s)						
	CO	NO_x	CH	PM	SO_2	Formaldeh.	Benz(a)pyr.
Street	1,268	0,23753	0,2761	0,00617	0,0057	0,00126	0,082 10^{-6}
Intersection	0,1739	0,00371	0,0025102	0,00312	0,00106	0,001254	1 10^{-6}

To determine the level of concentration of harmful substances from the vehicle at low altitudes at different distances from the road Gaussian admixture distribution model in the atmosphere is applied[16]

$$C_L = \frac{2M_{Li}/L}{1000\sigma \sin\varphi u\sqrt{2\pi}}; \quad C_R = \frac{2M_{Ri}/L}{1000\sigma \sin\varphi u\sqrt{2\pi}} \tag{17}$$

where φ -is the angle which makes the axis of the road with the observed point, u- wind speed at the observed moment, σ the standard deviation of the Gaussian dispersion in the vertical direction (Table 8)[17]

Table 8

	Emission (μg/m³)						
	CO	NO_x	CH	PM	SO_2	Formaldeh.	Benz(a)pyr.
Street	337,28	99,83	73,44	1,64	1,52	0,34	2,18 10^{-5}
Intersection	46,26	0,98	0,67	0,83	0,28	0,33	2,66 10^{-4}

For the selected example, all the values of the concentration of harmful substances at a distance of 10 m along the road are below the limit values.

For the case when it is day and it is cloudy at a distance of 10 meters from the road in the direction perpendicular to the road, the concentration of harmful substances are given in Table 9.

Table 9

Day and night		Distance from the road (m)					
		10	20	40	60	80	100
Day	Clear	2	4	6	8	12	16
	Cloudy	1	2	4	6	8	10
Night	Clear	0,1	0,2	0,4	0,8	1	1,4
	Cloudy	0,3	0,6	1	1,8	2,5	3,1

16 Lazaridis, 2011
17 Sportisse, 2008

CONCLUSION

Assessment of distribution of air pollution from mobile sources is a very complicated task. The process of fuel combustion, emission of harmful substances and their diffusion in the atmosphere around the source is extremely complex task. In this study we have analyzed some models of assessment, which are often used in practice and which are based on software tools. Models based on the Navier-Stokes equations for viscous, compressible and thermally conductive gases take into account the diffusion of particles and the effect of phase transitions caused by the presence of moisture in the atmosphere, dynamics of raising the particles and their convection.

Navier-Stokes method assumes the numerical solution of the equation of turbulent diffusion. The great importance of such models is that the equation of turbulent diffusion naturally reflects and connects the physical processes that occur in the atmosphere. Unfortunately, these models allow a forecast of spatio-temporal images of pollution of the atmosphere only under normal weather conditions (which is rarely fulfilled) and does not allow the analysis of the extreme impact of negative effects of road traffic on the surrounding environment.

For the modeling of air pollution and the determination of the concentration of pollution on small and medium distances from the source of pollution (which closely reflects the physical picture of air pollution from road transport), there are two approaches based on dispersion according to Gaussian formulas (which assumes the assessment of the distribution of concentrations of air pollution along the coordinate axes) and based on the theory of mass transfer (gradient models or K models) that are based on solving the equations of turbulent diffusion.

The European Union (EU) has pledged to reduce its emissions of pollutants and energy consumption, which originate from transport activities, in order to reduce the negative impact on the environment. Another challenge is to achieve sustainable development of transport. In order to harmonize the aforementioned challenges, short-term goals are set which should be achieved over the next five years[18]:

- the introduction of stricter regulations in terms of air quality;
- raising the awareness of the new improved fuels, favoring environmentally favorable fuel in accordance with the new requirements in terms of environmental protection;
- introducing the market with vehicles with lower emission of pollutants, complying with the more strict requirements regarding emissions
- standardization and harmonization of databases related to transport and transport statistics of all EU Member States;
- conducting research to improve the database of the factors that affect emissions.

Until today the territory of the Republic of Serbia has not completed a comprehensive study in order to determine the amount of emitted gaseous pollutants originating from road transport. Only partial, limited researches are conducted in this area.

To determine the amount of emitted gaseous pollutants originating from road transport, a software tool COPERT 4, a tool based on MS Windows setting, is used. The development of COPERT is funded by the European Agency for Environmental Protection (EuropeanEnvironment Agency - EEA) within the activities of the European thematic center for air and climate change (European Topic Centre on Air and Climate Change) and it is the only recognized tool for this purpose at European level. The application of software tools for calculation of pollutant emissions from road transport means enables creating transparent, standardized and comparable databases and reporting procedures on the emission of pollutants, in accordance with international treaties and EU legislation.

In 2007, the Integrated cadastre of pollutants was established in the Republic of Serbia. After that the establishment of regular annual reporting on emissions of pollutants into the air and water and waste generation began. The adoption of the new Law on Air Protection in 2009, it should be pointed out, was harmonized with the relevant EU legislation. This law regulates the management of air quality and determines the measures, organization and control of implementation of protection and improvement of air quality as natural values of general interest. This picture is necessary to complement with the data on emissions from diffuse sources, including traffic.

Overcoming the problems of pollution from road traffic is carried out in several directions

1) The use of better quality fuel that meets European standards
2) Reducing the toxicity of exhaust gases using a neutralizer and filter of solid particles
3) Construction of adequate transport infrastructure-such as construction of bypasses around major cities

18 The Insistute of Faculty of Traffic and Transport Engineering, Belgrade 2010

4) Adequate regulation of traffic in order to avoid large concentration of vehicles in urban areas, congestion, crowd, etc.

5) The use of alternative forms of transport and fuel (biofuel, gas)

6) Planting the surface around roads

To minimize the negative impact of road transport on the environment it is necessary to:

– improve the system of collecting data on the concentration of harmful substances in the air

– Conduct continuous research that would include

- The structure of the vehicle fleet
- The structure of the of traveled pathway by type of road (distance in the city, outside the city and highway driving)
- The average speed.
- Average trip length

High quality and accurate data are the basis for modeling and assessment of adverse effects on the environment, in order to reduce the amount of pollutants.

Acknowledgements: This work was done within the project of the Ministry of Education, Science and Technological Development of the Republic of Serbia, No. TR34019 and OI 171039

REFERENCES

1. М.Е.Берлянд (1975), *Современние проблемы атмосфеной диффузии и загрязнения атмосферы*, Гидрометеоиздат, Ленинград, pp. 11-78
2. D.L.Coe, d.S.Einsinger, J.T.Prouty, User's guide for CL4, Caltrans-U.C. Davis air quality project, 1998.
3. Insistute of Faculty of Traffic and Transport Engineering, Belgrade, *Determination of the amount of emitted pollutants originating from road traffic using the COPERT IV model of the European Agency for the Environment,* University of Belgrade, Faculty of Transport, 2010
4. ФилипповИ. Г., ГорскийВ.Г., Швецова-ШиловскаяТ.Н.*О рассеянии примеси в приземном слое атмосфери* // Теорет. основы хим. технологии. 1995. Т. 29, Но.5., pp. 517-521.
5. Янке Е., Эмде Ф., Леш Ф., Специальные функции, Наука, Москва, 1964.
6. Lazaridis M. (2011),*First principles of Meteorology and Air Pollutant*, Springer, New York, pp.201-232
7. Г.И.Марчук, *Математическое моделирование в проблеме окружающей среди*, Наука, Москва, 1982, pp. 175-187
8. Молодцов В.А., Гусыков А.А. (2014), *Определение выбросов загрязнающих вещуств от автотранспорта*, ТГТУ, Тамбов, pp. 6-20
9. РузскийА.В., Донченко в. в., Петрухин В. А. и др. *Методика расчетоввыбросов*
10. *в атмосферу загрязняющих веществ автотранспортом на городских магистралях,* Москва, науч.-исслед. ин-т „Атмосфера", 1996.
11. *Statistical Yearbook* (2012), Republic Institute for Statistics, Belgrade, pp. 303-316
12. B.Sportisse (2008), *Fundamentals in Air Pollution*, Springer, New York, pp. 239-241
13. Жданов В.Л.(2012), *Экологические проблемы автомобильного транспорта в городах*, КГТУ, Кемерово, pp. 46-54

UDC: 377:351.74/.75(477)
371.398:351.74/.75(477)

TECHNOLOGY OF OFFICERS OF INTERNAL AFFAIRS OF UKRAINE CAREER MANAGEMENT

Zoriana Kisil[1]
Lviv State University of Internal Affairs, Faculty of Psychology

Abstract: This article is dedicated to the consolidation of the problematic aspects of educational system's development in different spheres of its representation as the component of multidimensional organization of national education, as well as to the problem of further system of staff preparation for the needs of bodies of internal affairs development in the context of services in the bodies of internal affairs to the standards of EU adaptation and reformation of the Ministry of internal affairs of Ukraine.

Keywords: official staff strategy, personal trainings, conception, bodies of internal affairs of Ukraine.

PROBLEM FEATURES

With the reform of law enforcement bodies of Ukraine the problem of law enforcement officers (police officers) training gained its particular importance. Introducing of multilevel training of bodies of internal affairs personnel provides high efficiency of their operational performance, high reliability, psychological ability to self-improvement and continuous professional development. That is why the problem of police professionalism, their skills level increase has become tremendously important in the theory and practice of their special training.

Undoubtedly, the prominent position in the process of optimization of training in the police institutions belongs to the profile training associated with self-actualization of the professional, its capacity for professional growth, self-reliance, initiative, creative and independent thinking skills formation, desire and ability to learn throughout life.

During the democratization of the society and establishment of "the rule of law", of course to ensure the rights and freedoms of citizens, one of the major priorities of the police was to create a highly skilled apparatus able to effectively carry out the functions entrusted to police by the society and the state. The scope and complexity of the tasks performed by prosecutive structures requires radical transformations of organizational and legal foundations of police officers training. This task includes not only the implementation of modern professional programs at various levels and direction in the field of law enforcement, but also the formation of the policemen, provided with the high moral and ethical standards that affect the professional development of employees, their awareness of the public purpose during professional activity.

Requirements for training professionals of Ministry of Internal Affairs of Ukraine has qualitatively changed: special higher education designed not only to give certain knowledge applications to the policemen, but to teach them to think creatively to make quick and correct decisions, especially in complex, extreme situations, hard to overcome difficulties and temporary setbacks in official activities. Solving this problem is necessary due to various objective phenomena and processes. Firstly, it is determined with the general course of reforms in higher education, its democratization, individualization and humanization in the aspect of which the interests of personality in education are at the forefront. The Law of Ukraine "On Education" defines education process as the foundation of intellectual, cultural, spiritual, social and economic development of the society and the state. The goal of education is defined as the full development of human personality and the highest values of society, the development of person's talents, mental and physical abilities, production of the high moral characteristics, forming citizens able to make a deliberate choice on this basis enrichment intellectual, artistic and cultural potential of the nation, simultaneously increasing its educational level, the supply of national economy with qualified specialists. Secondly, specific operational performance and service activities of policemen requires not only the highest level of professional skills and expertise but also a highly-developed moral person, capable of continuous self-improvement and self-development. Thirdly, the existing trainings of police officers require the introduction of such forms and methods of management in the field of educational influence as self-education, professional self-improvement etc.

1 Doctor of law; Professor; *Dean of the Faculty*

Problem of professional training in various spheres of social production, including the police officers preparation, is the prior object of attention of scientific analysis because of its significance both in theoretical and practical aspects.

Exploring the variety of modern issues of practical training of the internal affairs officers caused the need to overcome the contradictions that arise between the current realities of operational performance, educational level, intellectual and physical development of this category of officials and the specificity of their professional development. Also practical organs and departments of internal affairs pay insufficient attention to the optimal organization of training on duty that should ensure the readiness of policemen to accomplish duties, associated with the state of permanent professional risk. Urgent resolution of these conflicts requires the review of the specific educational activities in the field of training of policemen.

STATE OF PROBLEMS RESEARCH

Scientific researches of the practical police departments functioning show that achieving excellent results of operational and service work is possible only under the condition of the high level of professional training of employees and departments of internal affairs of Ukraine, which is the basis of their professionalism. The named problem was represented in the publications of the following authors: M. Anufriev, G. Budahyants, S. Butov, G. Vasilyev, G. Vasyanovych, M. Hawryluk, A. Zaporozhanov, A. Kovalchuk, A. Kolokolov, V. Korj, A. Lushchak, V. Synov, A. Starodubtsev etc.

General conceptual aspects of professional training in higher educational institutions in the context of continuity and the new techniques introduction was also widely analyzed in the works of M. Galuzinsky, M. Evtukh, I. Zyazyuna, A. Lihotskoho, V. Synova, L. Sushchenko, M. Chobitka.

The problem of efficiency of different forms of employment in the system of professional education of students in departmental educational establishments of Ukraine were discussed in the researches of G. Budahyantsa, V. Babenko, S. Butova, G. Vasilyev, O. Zaporozhanova, Y. Irkhin, A. Lushchak, V. Pliska, S. Reshko, V. Synova, M. Chunosova, G. Jaworski and others.

The analysis of the latest researches in general, legal and social psychology, occupational psychology and pedagogy in the context of the professional activity of the officers of internal affairs shows the necessity and possibility of purposeful formative police officers as competent professionals who fully accomplish the current requirements of Law Enforcement (V. Androsiuk V. Barco, V. Kazmirenko, L. Kazmirenko, M. Kostytsky, E. Lukyanchikova, S. Maksymenko, O. Manoha, V. Medvedev, L. Frost, A. Morozov, V. Synov, O. Stolyarenko, V. Tatenko, A. Timchenko, L. Udalova, O. Hohlina, O. Tsilmak, M. Shvalb, S. Yakovenko). These features of the system of professional development are not fully used. This is evidenced by the following outstanding issues:

- current approaches and methods for preparing police officers do not properly provide formative professional coherence of the officers individuality, their willingness to practice, especially in extreme conditions;

- theory and practice training is not perfect and does not use the scientific potential of permanently-developing education. It should also be stated that there is no modern methodological and procedural framework for the implementation of student-centered training of the police officers.

These problems lead to the development of conceptual relevance of legal and psychological foundations of personality-oriented training as technology that provides professionally appropriate personality changes of the policemen.

THE PRESENTATION OF THE ARTICLE'S ESSENTIALS

The concept of student-centered training will allow avoiding the deficiencies inherent in traditional educational systems. Its objective will cover not only training in the mastery of knowledge, skills and abilities, but also the complex process of a professional education, based on purposeful implementation of a range of abilities and other individual psychological characteristics formation. Personality-oriented training should be purposeful and systematic process of creative subject-subject (equal) interaction of the policemen, aimed at development, personal self-mastery of professional and personal competence, formation of service and combat skills, promotion of spiritual, intellectual and personal police officers potential.

Personality-oriented training is a combination of structural components that define the process of personality-oriented police officers training as the implementation of two interdependent and interrelated components - classroom (basic and optional components of training) and extracurricular (add-training) [1]. In addition, represented components display: content of the pedagogical methods that are being used

for student-centered impact on participants of the educational process in order to enhance their professionalism, to provide the subjective involvement of employees in the educational process, which positively affects their motivational factors goals and actions transformation, fixing the dynamics and results of the process of gradual increase of professionalism of the police units officers in their personal development as a crucial condition for improving of their professional training.

Professional activities of all police officers are closely associated with direct influence of various psychological factors. Depending on its affect, O. Stolyarenko distinguishes four main activities in the bodies of internal affairs [2]:

1) activities that are characterized by social and psychological influences and acts (contacts with citizens during the process prosecution of authority);
2) activities that are characterized by psychological support of the performance of tasks, functions and areas of work (guidance, psycho-prophylaxis and investigation activity, public relations and media);
3) types of psychological and pedagogical activities (teaching and research activities, working with staff, crime prevention and social peace security, working with minors);
4) legal and psychological activities of the psychological support service (psychological personnel selection, psychological support and ensuring operational performance).

Psychological infrastructure of law enforcement, according to Y. Sharanov covers primary (basic, organizational) components of the subject and secondary psychological education in rights and duties.

Primary (basic, organizational) level includes the following groups of factors:

– organization of the service staff (professional and informative contacts, forward planning, strategic decision making, staffing, etc.);
– services (production of current decisions, sharing and communicating tasks, mobilizing forces, placement, maintenance of the efficiency etc.).

Secondary psychological education in the field of rights and duties consists of the psychological infrastructure of law enforcement based on stable organizational forms that support the functioning and development of psychological and legal structures that represent a well-organized system to perform functions of professional activity.

The approach, defined by Y. Sharanovym and supported by G. Sukhodilsk, who believes that any activity should be viewed only through the prism of the relationship of all the elements of the psychological infrastructure [3].

V. Vasilyev proposed the scheme of activity approach that involves following psychological components of the police officers operational activities [4]:

1) cognitive (cognitive) - receiving, perception, learning and processing information that constitutes professional or operational interest;
2) search - the invention of new (alternative) approaches to problem solving, requesting and obtaining information necessary for the successful implementation of operational performance;
3) communication - building and establishing the right relationships with subordinates and objects of professional activity;
4) educational - the formation of the basic principles of loyalty, respect to the constitutional rights and freedoms of citizen, moral standards and discipline development, law-abiding, respect for the society and the government, public safety and security support etc.;
5) constructive - making final decisions, taking immediate measures and ensuring continuity of the operational performance of subordinates;
6) certification - legal regulation and consolidation of powers, judicial decisions and other professional activities within the statutory functional legal realm (orders, instructions, opinions, etc.).

The effectiveness and success of the application of these components depends entirely on the personal qualities of a police officer.

Introducing multilevel training of personnel of internal affairs bodies of Ukraine will increase the efficiency of their operational performance, reliability, and psychological ability to self-improvement and continuous professional development. That is why the problem of the policemen professionalism, improvement of their skills gained great importance in theory and practice of performance training of servicemen and police officers in Ukraine.

Prominent place in the optimization of training of the police officers is still occupied by the profile training associated with self-actualization of the individual professional, its capacity for professional growth, self-reliance, initiative, creative and independent thinking, desire and ability to learn throughout life.

Theoretical and methodological analysis of persons professional abilities formation in the current situation of building a democratic society and legal system, in the process of law reformation and legal state enforcement gives arguments to state that the study of purposeful formative policemen acquires relevance.

It is commonly known that professional knowledge, abilities, skills and professional personality features are formed and developed during the relevant activities, including teaching and learning which have a professional orientation. Therefore, the efficiency of formation and development of these qualities of the policemen and hence their professional preparedness generally determined by the characteristics of this type of activity. Thus, the main problem that should be resolved by the experts in psychology and pedagogy is associated with finding effective means of training of policemen, personalization and mobilization mechanisms of personality development. One of the main means of upgrading the police officers training process is the usage of new educational technologies. In this case there is no such methodology that can be used to just any of the aforementioned factors, that's why all of the principles or methods of educational technology should be always used in complex. Typically, the learning process is based on certain educational technology that integrates a number of different elements based on identified prior ideas.

Focusing on the development of law enforcement officers as an individual, individuality and an active participant of professional activity can be realized only on psychological-humanistic principles.

Based on these principles the organization of the so-called "student-centered" training which aims to create an environment operational performance, which would facilitate the development of personal qualities of employees in mastering the content of the educational plan.

Personality-oriented approach is one of the important means of training police officers for the future operational performance. In our view, this approach makes it possible to perform complex tasks and to promote the development of a competent professional official and their abilities transformation in the conscious paradigm of practical usage of their knowledge and skills in practice, to improve a person's mental qualities and properties.

The main areas of functional and structural parameters of the police officers professional training improvement are: the development of its legal structure that ensures the adequacy of the goals and objectives of training highly qualified personnel with different skills and profile the needs of law enforcement. This will be possible on the basis of measures aimed at further improving the functional and organizational structure of professional training of military, its resources and legal support, improving oversight and evaluating the effectiveness of its operations.

CONCLUSIONS

Consequently, the "personality-oriented" training of the police officers should be provided in accordance with the development and substantiation of the theoretical and methodological framework, based on the conceptual position of interpretation of the police officers in the spirit of the permanent gradual increase of their professionalism (individual and differentiated approach), the nature, structure and content of professional police officers development.

REFERENCES

1. Тимченко А. В. Основные направления снижения уровня психических потерь и психической недееспособности среди личного состава подразделений особого риска : [учеб. пособие] / Тимченко А. В. – Харьков: Ун-т внутр. дел, 1998. – 32 с.

2. Теоретико-методологические основы юридической психологии: энцикл. юрид. психологии / [под. ред. проф. А. М. Столяренко]. – М. : ЮНИТИ-ДАНА, Закон и право, 2003. – 607 с.

3. Суходольский Г. В. Основы психологической теории деятельности / Суходольский Г. В. – Л. : Изд-во ЛГУ, 1988. – 157 с.

4. Васильев В. Л. Юридическая психология / Васильев В. Л. – [3-е изд.]. – СПб. : Питер, 2000. – 624 с.

UDC: 343.123.1:343.352

CRIMINAL INVESTIGATION OF CORRUPTION AND BRIBERY CASES

Darko Marinkovic
Goran Boskovic
The Academy of Criminalistic and Police Studies, Belgrade

Abstract: Research on the perception of corruption in the European Union Member States has shown that corruption is a serious and widespread problem. It can be said that most cases of corruption represent a specific form of exchange between two parties, wherein both parties give something and receive something else in return. Due to its covert nature, investigating corruption frequently calls for specific operative and evidential activities, such as engaging an informer, simulated transactions, sophisticated surveillance techniques and integrity testing, but also the testimony of offenders as cooperating witnesses. Integrity testing is of particular importance in investigating corruptive practices and it has to be devised in such a way as to ensure that the person tested has equal chances to pass the test and to fail. As far as suspects are concerned, it should be noted that allegations of corruption against officers with clean professional records may be made from base motives.

Keywords: corruption, bribery, crime investigation, simulated bribery, integrity tests.

INTRODUCTION

Corruption is a concept the content of which is difficult to define, given the fact that it has been changing over time, adapting to different social and political environments. In the broadest context, corruption occurs if the principle of impartiality in decision making is deliberately violated in order to obtain a benefit.[1] Generally, corruption involves abuse of public service for personal benefit. A classical notion of corruption starts from the idea that it represents a manifestation of deteriorating ethical values in a society, whereas modern democracies increasingly emphasise *systemic disfunctionality of corruption* – it is regarded not only to be detrimental to society, but also one of the causes of inefficiency of the state. Corruption is therefore the behaviour which constitutes a departure from the legally prescribed manners of executing public duty, performed for personal benefit – it is a violation of norms guiding the state or public affairs for the purpose of achieving personal interest. Essentially, corruption comprises numerous activities, such as *bribery* (acceptance of money or other benefits, resulting in exerting influence on decisions of public authorities), *nepotism* (situations in which someone uses public authority in order to achieve an advantage for a family member or a relative), *cronyism* (situations of using public authority to secure advantage to one's friends and colleagues) or abuse of office for personal benefit (illegally using public goods, services, etc.).

The study on the perception of corruption in the European Union Member States conducted by the European Commission in 2013 showed that as much as 76 % of the member state citizens regarded corruption as a serious and widespread problem.[2] A quarter of Europeans thought it was acceptable to do a favour to the representatives of state administration or services in return for something they wanted from the public administration or public service. More than a half of respondents expressed belief that bribery and abuse of positions of power for personal gain were widespread within political parties and among politicians at national, regional or local level. A quarter of the Europeans pointed out that they had recently been affected by corruption in their daily lives. Politicians and managers of tender procedures were regarded to be the most corrupted, whereas the police, judiciary and customs authorities were regarded as the most corrupt institutions. Although the general feeling appears to be exceptionally negative, it must be pointed out that the findings varied significantly from country to country, with a particularly indicative difference between old and new EU-members – while corruption is one of the gravest negatively received social phenomena in Bulgaria, Cyprus and Romania, it is perceived as an important issue in Denmark, Finland and Sweden.

The Serbian *Anti-Corruption Agency Act*[3] *defines corruption as a relation based on abuse of office or social status and influence, in the public or private sector, aimed at acquiring personal benefits for oneself or another.*

1 Tanzi V., *Corruption Around the World – Causes, Consequences, Scope and Cures*, International Monetary Fund (working paper), May 1998; Available at: http://www.imf.org/external/pubs/ft/wp/wp9863.pdf
2 *Special Eurobarometer 397 - Corruption*, European Commission, Publication: February 2014; Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_397_en.pdf
3 *Службени гласник РС* (The Official Gazette of the Republic of Serbia), nos. 97/08, 53/10, 66/11, 67/2013 and 112/13.

The findings of the international nongovernmental organisation Transparency International indicated that corruption was widespread in the Serbian society; according to the organisation's study of 2013, Serbia ranked 72nd among 175 analysed countries.

BASIC PHENOMENOLOGICAL ASPECTS OF CORRUPTION AND BRIBERY

Corruption occurs at different levels. Distinction is usually made between serious and petty (administrative) corruption, where the former refers to the corruptive practice which influences legislative acts and subjects of political and state (public) decision making, while the latter, in most cases, boils down to bribery. Serious corruption is boosted by the lack of independent and efficient supervisory bodies in crucial areas, such as financing political parties, conflict of interests, public procurement and privatisation. Petty corruption affects the daily life of citizens through their contacts with public officials for different reasons, from the need for healthcare services or enrolment into a school or university, to issuing a new passport or a driving licence. In any case, corruption has a devastating effect on the rule of law, since it hampers equal access to public services, affects public confidence in state institutions, and is an impediment to economic and social development. Corruption can be described as *a complex form of crime without clear contours*, in which it is frequently hard to distinguish between the perpetrator and the victim. This means that a corruptive relation does not necessarily imply a one-dimensional interaction in which the perpetrator coerces a passive party to do something – both parties to such a relation can benefit from it, whereas the victim of the offence is actually a third party or the wider community.

In everyday speech, laymen tend to treat the terms corruption and bribery as synonymous. However, the content of the phenomenon of bribery is significantly narrower than that of corruption and encompasses only one of its modalities, i.e. offering and accepting bribe in terms of criminal law.

Bribery can take various forms and proportions and it may occur in different contexts. The complexity of corruptive practices is manifested in the cases where citizens offers bribe, public officials explicitly demand bribe, public service employees implicitly let the citizens know that bribe is required, or the citizens receive such a request through a third person acting as a mediator. Citizens offer bribe to police officers in order to avoid citation or to have the fines reduced, while they do the same to physicians and nurses in order to shorten the time of waiting or to ensure better treatment, both of which constitute important aspects of using healthcare services and resources.

Most corruption cases can be said to represent a specific form of exchange between two parties, wherein both parties give something and receive something else in return. This justifies the claim that offering and accepting bribe (corruptive practice) is characterised by *consensuality*, i.e. mutual agreement of wills of the parties to the criminal act. Neither of them feels hurt, which classifies bribery as *a crime without a victim*. However, the aforementioned willingness is to be understood only conditionally – the citizens can frequently be in a situation where they have the right to certain official acts which serve their interests, but the officials in charge refuse to perform such acts before they are bribed. In other words, the citizens are compelled to pay in order to obtain something that they are entitled to by law, to which they have right. Thus, for instance, it is a widespread practice that a doctor evades (postpones) providing medical assistance to a patient until the patient or his close relatives give him money or do a favour.

As bribe is given for different purposes and may occur in various forms and contexts, certain sectors of public administration are more or less affected by corruption. Some of the public officials ask for bribe more often than others, although there are certain situations and activities in which the users of public services are more inclined to offer bribe in order to bypass bureaucratic procedures or successfully bring a procedure to an end. Public officials who come into contact with citizens more often are more frequently subject to bribery. Yet, certain sectors of the public administration, such as the judiciary or customs authorities - although the interaction of their staff with the citizens is relatively restricted - have significant experience of bribery nevertheless. Therefore, in defining the potential *centres of corruption* we should take into account not only the officers who most frequently have contacts with the citizens due to the nature of their services, but also the ones in relation to whose powers there is a high risk of bribery.

In practice, bribe is most often given to physicians, nurses, police officers, representatives of the local governments, communal service employees, etc.

CORRUPTION AND ORGANISED CRIME

Corruption and bribery, as its most representative form, represent the instruments used by organised crime in order to function as effectively and as profitably as possible and they are not the objective in themselves – whether we observe it in the short or the long run, corruption involves losses for a criminal organisation, since large sums of money are set apart for bribing the government representatives. Yet, on one hand, corruption ensures strategic positions for performing specific illegal operations in future and, on the other, factual immunity against criminal prosecution. [4] In this context, corruption cannot be treated as a form of organised crime, such as trafficking in illegal drugs or weapons, or other activities directly aimed at gaining profits. It is a method of operation of criminal organisations whose function is to perform lucrative illegal operations effectively, or a specific *modus vivendi* of organised crime.[5]

Exerting influence on the public administration, politicians, the criminal justice system and the media, but also on the representatives of the private sector, represents one of the prevalent traits of organised crime and its functioning. It may take the form of corruption not only in terms of bribery, but also other forms based on nepotism, unjustifiable favouring, kinship, friendship, ethnic origin, relationships with persons in positions of power or politically exposed persons, etc. In this respect, financing individual politicians or political parties and election campaigns by organised crime may play an important part. Creating a *symbiosis* between corrupt representatives of the state authority and criminal organisations, based on their mutual interest, is far more viable and reliable for organised crime than the use of force and intimidation. This underlines necessity for cooperation and engagement in joint and systematic national and transnational activities against organised crime and corruption, as the United Nations have done since adopting the Convention against Transnational Organised Crime (2000)[6] and the Convention against Corruption (2003).[7]

Organised criminal groups involved in drug trafficking use corruption to obtain information on investigations led against them by the judicial organs; those who engage in vehicle thefts demand information on vehicle owners and manners of vehicle protection from the technical inspection services, registration authorities and mechanics; groups involved in human trafficking and prostitution corrupt immigration services; cigarette smuggles bribe the customs officers and border police.

Corruption is increasingly used in a highly professional way, by engaging legal and business experts as mediators or brokers in relevant political or economic positions. Corrupted officials tolerate criminal activities or take part in them, protect the culprits from the police or, in the case of higher-ranking officials, favour legal economic structures behind which there is organised crime and its *soiled money*. In some of the transition countries, corruption has penetrated most structures of public life, including the judiciary and police.[8] Low salaries, unemployment, uncertainty and poverty, but sometimes even the examples set by the prominent public figures will make civil servants *easy targets* and reliable partners of organised crime. In more prosperous countries, such as western democracies, which have stable institutions of authority, corruption is also intensively used by organised crime, but it rarely reaches so high. However, it should not be forgotten that the funds at disposal to organised criminal groups are so abundant that they can offer bribe which is hard to resist.[9]

STARTING POINTS IN COMBATING CORRUPTION

Corruption and bribery, as one of its forms, occurs, as a rule, where two key factors exist – *opportunity and interest*. Therefore the strategy of suppressing it has to be directed to both of these factors. Opportunities must be eliminated by system reforms and the interest by measures increasing probability of detection and sanctioning of perpetrators, together with restricting the benefits from corruption. In other words, the strategy is to encompass three crucial elements:

– effective implementation of anticorruption regulations, including the repressive ones;

– prevention, which implies removing the opportunities for corruption;

4 This is why the bosses of organised crime consider the money paid in bribery as one of the best investments. According to: Корж В. П.: Коррумпированные связи организированных преступных образований: криминалистический анализ, *Государство и право,* Москва, no. 8, 2002, p. 56.

5 Маринковић Д.: *Сузбијање организованог криминала - специјалне истражне методе*, Нови Сад, 2010, p. 51

6 *United Nations* Convention against *Transnational* Organized Crime; Available at: https://www.unodc.org/unodc/en/treaties/CTOC/

7 *United Nations Convention against Corruption*; Available at: http://www.unodc.org/pdf/crime/convention_corruption/signing/Convention-e.pdf

8 *Organized Crime Situation Report 2004 - Focus on the threat of cybercrime*, Council of Europe, Strasbourg, 2004, p. 41.

9 Transparency International held an international anticorruption conference in Athens in 2008 under the title Combating Corruption for Sustainable Future hosting more than 1300 participants from 135 countries. Most of them took the view that combating corruption was the most important problem – *If the 20th century was the century of wars and developing democracy, the 21st century leaves us to fact the omnipresent corruption as a global issue.* Available at: http://www.transparency.org/news_room/latest_news/press_releases/2008/2008_11_02_closing_iacc

– raising awareness and education of the public, in order to obtain the public support for the implementation of anticorruption strategy.

Generally, it can be said that the incidence of criminal offences reported by the plaintiffs, i.e. the victim, is proportionate to the synergic effects of three factors:

– perceived gravity of the criminal offence;

– trust that the competent authorities will find the offender;

– immediate benefit if the criminal act is reported.

The impression is that each of these three factors determines reporting the act of corruption in a negative sense - the victims, if they see themselves as victims, do not perceive bribery as an act which is detrimental to them; conversely, they may often obtain certain benefits from it. Even when suffering detriment from an act of corruption, the victim does not believe that competent authorities will manage to resolve it, which implies that there is little chance to be compensated for possibly suffered damage. Similar reasons apply to possible witnesses, i.e. citizens who have certain knowledge of corruptive practices manifested in their surroundings.

Classical forms of bribery are generally performed person-to-person, and money is offered most frequently. In these situations there is no evidence because it is in the interest of both parties to this criminal offence that their actions are kept secret – verbal evidence is scarce, whereas physical evidence is most often obtained by catching the perpetrator in the act. Combating corruption therefore calls for using special investigative methods, which are most suitable for dispersing the *aura of secrecy* and information deficiency accompanying acts of corruption, as well as for their continuous perfection and adjustment.

Elements of the corruption-curbing strategy nowadays increasingly include numerous actions at the state level or the level of certain public administration departments, which use the media, posters placed in the public institutions, notices, etc., to raise awareness of the civil servants and other employees of the harmful effects of corruption, while, at the same time, citizens are advised to report bribery cases by making free phone calls, anonymously, if they wish so. Reports and other information related to corruptive practices can be submitted through the Internet or in any other way.

If an act of corruption is not detected, its perpetrator will continue his illegal activities. There is a real danger that the system of promotion will help such a person be appointed to a higher position in the service he is affiliated to, so that they may cause even more harm. On the other hand, when a ramified corruption network is detected, measures are taken for its eradication, which mostly consists of criminal prosecution of the perpetrators and firing them from the service. However, almost as a rule, new corruption cases occur after some time. Therefore the corruption combating strategy has to be continuously applied as a synergic effect of preventive and repressive measures, so that state organs would not *become lulled* by achieved results following successfully performed actions. Demands for introducing and continuously upgrading normative solutions and their operationalisation in order to suppress corruptive practices have nowadays become an integral part of international relations in the processes of political, economic or military integrations.

It was formerly believed that removing *rotten apples*, i.e. corrupt officials, was sufficient to keep the problem of corruption under control. But it is not enough – it is necessary to develop such a system which will ensure that corruptive practice does not repeat. For this purpose, the emphasis is to be placed on effective implementation of measures of internal/external control and integrity tests. The integrity tests appear to be particularly useful for *cleaning* the public services from the corrupt, as well as for maintaining *purity* once it is achieved.

CRIMINAL INVESTIGATION OF BRIBERY – TACTICAL ASPECTS

Corruption investigations frequently involve specific operative and evidential activities, such as engaging informers, simulated deals, sophisticated surveillance techniques and *integrity testing*, but also the testimony of offenders in the procedural role of collaborating witnesses, in which way crucial evidence is obtained on the corruptibility of officials, especially the ones ranking high in the hierarchy of a public institution or state organs.

The criminal offences of offering and accepting bribe involve a two-sided relation in which one party demands or receives, and the other offers or gives the bribe, which represents a classical example of incriminations that can be simulated, and hence be proved by simulated transactions as a specific evidential activity (simulated giving and acceptance of bribe). On the other hand, due to a lack of knowledge about the perpetration of specific criminal offences, primarily in the form of reports by victims, a crime investigator is obliged to perform proactive inquests, using both of their modalities – the problem oriented one and the

one targeting specific persons. In this case, the reason for launching such investigations is the existence of general suspicion of corruption in a certain institution or corruptibility of certain officials thereof.

The most frequently used procedure in detection and resolving bribery cases involves situations in which a citizen reports to police and the prosecutor's office those officials who demand money for doing certain favours or performing some official duties. The criminal investigation depends on whether the bribe has already been given to the seeker or it is yet to ensue.

In the former case, when the criminal offence is reported following the giving of bribe, the investigator will, based on the available facts, launch an investigation aimed at securing evidence of the suspect's culpability. If the victim/plaintiff possesses some evidence on the bribery, the evaluation of such evidence will take place in order to establish its credibility, as well as a check to establish whether other facts significant as evidence or indications can be found, that the plaintiff is not aware of or underestimates their value. Likelihood of such findings can lead to a search of the suspect's abode or office, as well as the search of his person, in an attempt to find the money or other valuable objects used for bribery, as well as various receipts, orders and other written documents that confirm the perpetration. An insight into official registers and documents can be particularly significant, especially if they are made by a competent authority in relation to public duties within which the action that is the occasion for bribery has been performed. The same significance can be attributed to gaining an insight into money transactions between the plaintiff and the suspect, in case the bribe has been paid by transferring money from one account to another. Additionally, some special evidentiary actions can be taken against the suspect, such as tapping his/her phone and recording conversations if they are expected to provide evidence of the committed criminal offence.

The investigation based on a bribery report may fail to find valid evidence on the suspect's culpability. On the other hand, there may be operative intelligence regarding an individual or a group of people suspected of being corrupted, but there may be no evidence on concrete acts of corruption. In these situations, the suspected persons will be subject to *proactive investigations*, aimed at establishing facts and securing evidence that certain criminal offences have been planned or perpetrated. The investigation will mostly consist of secret surveillance of communications, covert surveillance and recording, as well as simulated offering and acceptance of bribe. The objective of these measures as well as other operative-tactical and evidentiary measures and activities is to gather information based on which the crime investigator will decide in which way to obtain crucial evidence of corruption. It is almost invariably obtained by simulating offering bribe and/or catching the offender in the act.

A simulation of accepting bribe as a special evidential activity involves engaging an official and faking the environment in which the act of corruption is to take place. In such cases, the investigation does not encompass the giver and the taker of bribe, as the role of the latter is assumed by an official, who contacts the suspect and demands performing or refraining from performing an official duty, waiting to be asked for bribe in return or, in another modality, offering bribe for performing/refraining from performing an official duty. In the latter case, special care should be taken to ensure that activities of the official faking the bribe offer do not involve elements of instigation (to commit a criminal offence). The objective of the simulated bribery is to establish a corruptive relation in controlled circumstances and it most frequently ends in catching the perpetrator red-handed and/or in recording the incriminated activity, thereby securing crucial evidence on the offender's culpability.

Catching the offender in flagrante involves the situations in which the citizens report a certain official to the police or the prosecutor as a person requesting the bribe, but in which the bribe has not been given yet. [10] Together with the person who reports the case, the crime investigator prepares money or other valuable objects used as means of payment, making a list of serial numbers of the banknotes in question. For other valuable objects, the minutes shall be made containing the statement of their individual features, such as serial numbers of other individual characteristics, and there is also a possibility of taking photographs. The person asked to give the bribe is instructed on how to contact the official seeking the bribe and how to simulate consenting to a corruptive relation. As soon as the money is handed over, the police will react energetically and search the person or premises in which the criminal act has taken place in order to find and seize the notes and/or objects used as payment, securing in this way the crucial *corpus delicti* (lat. evidence of crime, the object that proves guilt).

Apprehending the giver/taker of bribe in some situations implies that both parties to the act of bribery are subject to an investigation aimed at securing definite evidence on their culpability. In the course of such an investigation, significant evidence may be gathered regarding the origin of the corruptive act, the offer of/demand for bribe, specifying the amount, place and time of the transaction, possible mediators, etc.

Criminal investigations of bribery must take into account ambivalent actions related to reporting corruption – on one hand, it is vital to ensure protection for those who report unlawful conduct, while, on the other, care must be taken of the personality of suspects, especially at the onset of the investigation, when the

10 According to the provisions of Criminal Code, the criminal offence of accepting bribe is accomplished not only by accepting gifts or other benefits, but also by demanding them.

findings on their culpability are limited in terms of both quantity and quality. In the former case, the situation is additionally complicated by the report on corrupt police officers by the offenders themselves. Such allegations, as a rule, have small credibility, and little attention is given to the protection of the informer. Speaking about the suspect, it should always be borne in mind that allegation of corruption against officers with impeccable professional careers may be motivated by unethical reasons. It is the incorruptible officers who are usually targeted by the offenders because they disrupt corrupt practices, and organised crime in particular, by acting lawfully. Fabricated physical evidence and false witnesses may be provided to support such false allegations.

INTEGRITY TESTING AND COMBATING POLICE CORRUPTION

Integrity testing is a term which includes a range of acitivies designed and performed in order to check morality and/or lawfulness of activities of an individual or the compliance thereof with the expected and previously defined demands and standards. It involves placing the individual in a simulated, controlled situation which essentially corresponds to a real one and in which a person responsible for the testing is to check whether the individual acts in accordance with certain rules. Certainly, from the aspect of the tested person, the simulated situation is real. Integrity testing is most frequently performed by persons who are in position to and/or who have legal authority to control certain duties and the persons in charge of such duties. The persons tested in simulated situations may act completely in keeping with the integrity standards of their professions or focus on illegal material gain or something else, to the detriment of the standards. Depending on what is tested, a failure in the integrity test can result in a disciplinary procedure, termination of employment or criminal proceedings.

Integrity tests can be performed for different purposes and cover a very wide range, from checking the loyalty of employees to the owner or manager of a company in which they are employed to establishing whether a person in public authority or holding certain public powers performs duty in keeping with legal provisions. Thus, for instance, the loyalty of employees can be tested in such a way as to simulate a situation in which a representative of a competitive company (whose role is played by the person in charge of the testing) offers them an amount of money in return for revealing business plans of their company. Testing the integrity of public authority or service personnel is frequently performed, also in simulated circumstances, in such a way as to check whether the civil servants are corruptible, e.g. whether they will refrain from citation in case of speeding for an amount of money.

Literature on criminalistics relates this concept almost exclusively with detecting corruptive practice, most frequently among police officers.

An integrity test has to be designed and applied in such a way as to grant the tested person equal chances to pass and to fail. In other words, the outcome of the test must be free choice of the tested person. Just as in case of undercover investigation of organised crime or drug trafficking, in this case we must not treat the suspect in such a way as to *encourage* him to act unlawfully. The ambience in which the integrity test is performed and the manner in which it is done should be such as to define the time and place of manifestation of offence (prohibited, illegal conduct), but not the decision on its perpetration. The crucial thing is that the *temptation* placed before the tested person is not such that even an honest person could succumb to it – the objective of the test is to check honesty of officials, not to convert an honest officer into an offender (by instigating corruption or another form of illegitimate conduct in a prepared trap).[11] In order to avoid possible denials of the validity of evidence obtained during integrity tests by the defence of the accused, but also to additionally strengthen the obtained evidence, the practice involves documenting the simulated activities with elements of corruption by audio/video recording.

Typical *scenarios* of testing the integrity of police officers include the following[12]:

- an operative assumes the role of a citizen and gives a street officer a wallet containing a sum of money, which he has allegedly found, or takes it to the police station, and monitors the follow-up – whether there is any mention of the retrieved wallet in the official records and, in case there is, whether any of the money is missing;
- placing valuable objects or money in the premises or facilities where a simulated criminal act has taken place, i.e. a burgled house or a stolen vehicle, so as to test the police officer in charge of securing

11 For more information on the criteria under which culpability of suspects can be proved through contacts with undercover agents see: Маринковић, Д.: *Сузбијање организованог криминала – специјалне истражне методе*, Нови Сад, 2010.

12 Compare: *Inquiry into Integrity Testing*, Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity, November 2011, p. 4; Vincent H.: Lifting the Blue Curtain: some controversial strategies to control police corruption, *National Police Research Unit Review*, 1990, no. 6, p. 51.

the crime scene or members of the crime investigation team by observing whether they will take or hide such valuables from the crime scene;

– an operative plays the role of a citizen who commits an offence or applies for a licence, offering a police officer bribe in exchange for avoiding citation or bypassing legal procedures;

– a situation is simulated in which illegal drugs or other valuable objects are seized and the follow-up is monitored in order to establish whether the police officer in charge of handling these items makes a record thereof or whether a certain quantity of the seized goods goes missing;

– placing untruthful information marked as classified to a police officer suspected of unlawfully disclosing such information or placing such information in a database and checking whether the officer communicates it to a third party.

Integrity tests are one of the modalities of secret operations or *sting operations* with elements of simulation that mislead the targeted individuals. They involve the active participation of undercover agents or police officers responsible for internal control, designing scenarios of simulated situations in which they perform, engaging support teams, electronic surveillance and audio/video recording, etc. One of the most important elements of each integrity test is a realistic scenario. Testing that follows a scenario which is not well-designed and realistic cannot be successful. Besides, a bad scenario may warn a suspected officer that there is an undercover investigation against him, because of which he may become more alert or give up unlawful activities for a longer or shorter period of time.

Integrity testing as an inquiry method has a strong potential as a key component of criminal investigation of corruption, since it ensures concrete evidence and has powerful preventive effects. Witnesses of corrupt practices among the police are frequently citizens who tend to violate law themselves or, occasionally, the colleagues of the corrupt officers, due to which there may be a lack of cooperation on the part of such persons in the course of criminal investigation or a disciplinary procedure (peer support or belief that the word of an offender against a police officer will not be taken seriously). Still, integrity test as part of inquiries on certain persons for their alleged misuse of office or powers can from time to time ensure crucial evidence of corruption in the police ranks.[13]

CONCLUSION

Studies on the perception of corruption in the European Union member states have shown that corruption is a serious and widespread problem – a quarter of Europeans consider it acceptable to do a certain favour to the representatives of public administration or service in exchange for something they want from the public administration or public service. According to the classical concept of corruption, it represents a manifestation of deterioration of ethical values, whereas modern democracies increasingly emphasise *systemic disfunctionality of corruption*. In other words, corruption is the behaviour which constitutes a departure from the legally prescribed performance of public duty for personal benefit, which renders the society, the state and its institutions insufficiently effective. This particularly applies to its bondages with organised crime.

In everyday speech, the terms corruption and bribery are treated as synonymous. However, the content of the phenomenon of bribery is significantly narrower than that of corruption and encompasses only one of its modalities, i.e. offering and accepting bribe in terms of criminal law.

Most cases of bribery can be said to represent a specific form of exchange between two parties, wherein both parties give something and receive something else in return. This justifies the claim that offering and accepting bribe (corruptive practice) is characterised by consensuality, thus classifying bribery as a crime without a victim. Corruption, and hence bribery as one of its manifestations, generally occurs where there are two crucial factors – opportunity and interest.

Due to its covert nature, inquiries of corruption frequently call for specific operative and evidential activities, such as engaging informers, simulating transaction, using sophisticated surveillance techniques and integrity testing, but also testimonies given by offenders in the procedural role of collaborating witnesses. A particular problem in the investigating acts of corruption concerns abuse of public authority by civil servants ranking high on the hierarchical ladder of a public institution or a state organ. Most frequently, the procedure of detecting and resolving bribery cases involves situations in which the citizens report to the police or the public prosecutor that certain officials demand money for doing some favours or performing official duties. In investigating corrupt practices, integrity tests are of particular importance as an investigative method that has a strong potential as key component of securing evidence and at the same time has powerful preventive effects. In practice, integrity tests have to be designed in such a way as to grant the

13 IAB's integrity testing program; the Internet source: http://www.nyc.gov/html/ccpc/assets/downloads/pdf/iab_integrity_testing_program_march2000.pdf

tested person equal chances to pass and to fail. In other words, the outcome of the test must be free choice of the tested person.

Criminal investigation of bribery must take into account the ambivalence of actions related to reporting corruption cases – on one hand, it is vital to ensure protection for those who report unlawful conduct, while, on the other, the personality of suspects should be taken into account, especially at the onset of the investigation, when the findings on their culpability are limited in terms of both quantity and quality. As regards suspects, it should always be borne in mind that allegations of corruption against officials with impeccable professional careers can be guided by base motives – discrediting them by accusations them of corruption is an effective method of eliminating them.

REFERENCES

1. Tanzi V., *Corruption Around the World – Causes, Consequences, Scope and Cures*, International Monetary Fund (working paper), May 1998; Available at: http://www.imf.org/external/pubs/ft/wp/wp9863.pdf
2. *Special Eurobarometer 397 - Corruption*, European Commission, Publication: February 2014; Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_397_en.pdf
3. *Службени гласник РС* (The Official Gazette of the Republic of Serbia), nos. 97/08, 53/10, 66/11, 67/2013 and 112/13.
4. Корж В. П.: Коррумпированные связи организиранных преступных образований: криминалистический анализ, *Государство и право,* Москва, no. 8, 2002, p. 56.
5. Маринковић Д.: *Сузбијање организованог криминала - специјалне истражне методе*, Нови Сад, 2010, p. 51
6. *United Nations* Convention against *Transnational* Organized Crime;
7. Available at: https://www.unodc.org/unodc/en/treaties/CTOC/
8. *United Nations Convention against Corruption*; Available at: http://www.unodc.org/pdf/crime/convention_corruption/signing/Convention-e.pdf
9. *Organized Crime Situation Report 2004 - Focus on the threat of cybercrime*, Council of Europe, Strasbourg, December 2004, p. 41.
10. *Transparency International,* 2008; Available at: http://www.transparency.org/news_room/latest_news/press_releases/2008/2008_11_02_closing_iacc
11. *Inquiry into Integrity Testing*, Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity, November 2011.
12. Vincent H.: Lifting the Blue Curtain: some controversial strategies to control police corruption, *National Police Research Unit Review*, no. 6, 1990.
13. Nash J. R.: *Dictionary of Crime*, London, 1992.
14. IAB's integrity testing program; Available at: http://www.nyc.gov/html/ccpc/assets/downloads/pdf/iab_integrity_testing_program_march2000.pdf

UDC: 343.985

THE ROLE AND IMPORTANCE OF CRIMINALISTICS STRATEGY IN CRIMINALISTICS[1]

Nenad Radovic[2]
Zoran Djurdjevic[3]
The Academy of Criminalistic and Police Studies, Belgrade
Shang Fangjian[4]
National Police University of China, International Office, Shenyang

Abstract: Criminalistics is a relatively new and unique science that consists of more disciplines. There is still an old tripartite division of criminalistics in criminalistics tactics, methodology and technique. At the same time, one more branch - criminalistics intelligence developed studying the contents of the field of criminalistics without being concerned with the three disciplines. Considering the fact that the progress and development of society as well as technology caused changes in lifestyle, in the same way there has been a change and development of certain types of crime that did not exist in the past. The manner the police used in fighting crime using traditional methods proved to be inefficient at one point and there was a need for certain changes in the police approach and work. In this regard, the term 'criminalistics strategy' was used for the first time in the 80's of the last century in the Republic of Germany, and it was referred to as an independent discipline of criminalistics involving a comprehensive approach in preventing and combating crime. The authors of the paper tackle the concept of criminalistics strategy as well as its importance in the system of Criminalistics as a science.

Keywords: criminalistics, strategies, criminalistics strategies.

THE TERM OF CRIMINALISTICS STRATEGY

In science and social practice the word strategy means: 'scientific concept, 'method', 'theory', 'theory and practice', 'wide system of scientific knowledge', 'a branch of the art of war', 'military or scientific discipline', 'doctrine', ' idea', but it also means ' specific development plan', 'skills' or 'action', and even 'social game' or only as a guide for action in 'game theory'. If the term strategy is very complex and diverse, then talking about the strategy as of a concept and a social phenomenon is even more complex, because it depends on the level of scientific knowledge as much as it depends on the ideological postulates and pragmatic political interests.[5]

It is indisputable that the British theorists changed the theoretical approach to the strategy from traditional and prevailing understanding strategy as a concept in military science to the understanding of the strategy and the theory of the state and law. By the end of 20th century in the USA and the UK, the strategy with its subject of study on the scientific knowledge is related to very different scientific areas: demographics, economics, security, mathematics, criminalistics, management, so that it is more and more referred to as a multidisciplinary science. Lately, within the Russian Academy of Sciences and as well as in China the approach to strategy has been also changed by leading economists and political scientists and it has been discussed in a multidisciplinary way. It is a multidisciplinary science that studies the problems of governance, territory, natural resources, population, economic development, culture and religion, science and education, the armed forces and foreign policy, crime.[6]

Etymologically, the term strategy comes from the ancient period, from two Greek words, *strategos autokrator*, which loosely translated means 'general ship'[7]. This linguistic inconsistency of a literal translation of the complex Greek word 'stratos'–'army' and 'ago'–'lead', which means 'to lead the army,' was pointed out

1 This paper is the result of the research on project: "Crime in Serbia and instruments of state responce", which is financed and carried out by the Academy of Criminalistic and Police Studies, Belgrade - the cycle of scientific projects 2015-2019.
2 nenad.radovic@kpa.edu.rs
3 zoran.djurdjevic@kpa.edu.rs
4 fangjian345@163.com
5 Stojkovic, B, Different approaches to the use of the term strategy from time to age, 2009, p.241
6 Ibid
7 Military Encyclopaedia, (1975), Editorial military encyclopaedias, Belgrade, p.190

by an Austrian theorist Erich Eder, who referred to the deep and hidden meaning of the term strategies and it meant 'the art of leading the army'[8].

Today, when we talk about strategy[9], we can find a variety of concepts which in their name have the word strategy; like strategy transport, agriculture strategy, national strategy, security strategy, corporate strategy, the strategy of infrastructure, environmental strategies, strategy, marketing strategy, military strategies and so on.

The concept of crime strategy is proportionately new, appropriate content was not given to it before Schafer. He was a German director of Criminal Police who wanted to find a new approach in the investigation of the terrorist group Bader Meinhof[10], which committed crimes in the territory that was under his jurisdiction. After breaking up the group, the interest in criminalistics strategy ceased to exist for some time only to be re-awakened after the 90s, especially in German-speaking countries. According to some scholars there is a prevailing opinion that this is today's fastest-developing field of criminalistics.[11]

According to Simonovic, criminalistics strategy in a broader sense consists of operationalizing criminal-political concepts of combating crime in whole or in certain forms, but also of the application of law enforcement measures and by the holders of Criminal Activity. The same author emphasizes its division in general, particular and special criminalistics strategy. General is engaged in establishing, improving and methods of implementation of general preventive concepts relating to the suppression or placing under the control of crime in general. Particular criminalistics strategy deals with combating and prevention of certain types of crime, whereas special strategic criminalistics approaches deal with strategy of implementation or optimization of certain measures in fighting crime.[12]Simonovic also indicates that it is necessary to bear in mind that the term 'criminalistics strategy' may lead to confusion, and perhaps is better to use the term 'strategic behaviour criminal police' or 'strategic measures taken by the criminal police' or 'strategic action of criminal police'. The term strategy, by its nature, suggests a target orientation. The same objective can be achieved by different routes, using a variety of measures available to the criminal police. The basics of the strategy are not made by the methods and means, but by strategic objectives which subjects want to achieve. Therefore, it is more correct to speak about the strategic conduct of criminal police in order to achieve 'higher' goals that are not operational and tactical, and which are in accordance with the mission and vision of the criminal police and which, ultimately, are used in order to have more efficient and effective impact on crime.[13]

Škulić indicates that criminalistics strategy is a common, general and systematically developed and directed view at the basic characteristics of crime, both in general and in relation to its particular form, and the systematic study of the root causes and forms of crime, as well as global planning, and then the concrete realization of general forms and the ways of reacting of competent state authorities to crime as a phenomenon or some of its forms, whether with respect to the type of offenses (such as, for example, organized crime, economic crime, etc.), either with respect to the category of offenders (such as, juvenile crimes, crimes of serial perpetrators or habitual perpetrators, etc.), and it is possible that it is a combination form, both by type of crime , and according to the category of typical perpetrators (where, for example, include certain distinct criminal acts of violence, such as, for example, domestic violence), along with developing the most general methods suitable for the suppression of crime, or the appearance of certain forms and types of crimes. [14]

According to Klink and Kordus, criminalistics strategy is the study of methods of the targeted impact on criminal activities to the entire crime and on its specific area. Furthermore, criminalistics strategy is often seen as a scientific area, which explores the ways of achieving preventive and repressive measures aimed at combating crime, with the help of global, planned (in the medium and long term) measures taking into account the principle of efficiency (Klink &Kordus 1986, 22, according to Dvoršek, 2008: 20)

8 Eder, E .: Definition und Gebrauch des Begriffes, "Strategie" ÖsterreichischeMilitaerischeZeitshchrift, 2/98, p.121

9 According to the length of the period to which they relate, strategies can be short, medium and long term, although they may relate to specific forms of crime, different levels of government organizations, or geographic area. (Vukovic, S. (2010), Prevention of Crime, Criminal Police Academy, Belgrade, p.77)

10 A gang was attacking banks and department stores, public parking lots, warehouses of weapons and ammunition and dealt with the abduction of important politicians. The investigation of individual criminal acts by the principles of criminology tactics and methodology proved to be ineffective. The crimes that the group committed were committed in a wider area, they did not know that connect, even if they could, due to traditional methods of investigation that would not help in solving cases. Manual of the gang was found in one of their hidden location, which was the reason for a different approach to investigations.

11 Dvoršek, A, Crime Strategy, University of Maribor, Faculty of Sciences, SAFETY, Ljubljana, 2008, p.17

12 Simonovic, B, Crime, Law Faculty in Kragujevac Institute for Legal and Social Sciences, Kragujevac.2004, p.5

13 Simonovic, Two Theoretical Concepts "Criminalistics strategy" and / or "Strategic Approach in Criminal Police Work" - Which of These Two Gives More "Archibald Reiss Days", Academy of Criminanalistic and Police Studies-German Foundation for International Legal Cooperation (IRZ), 2014, p.310

14 Škulić, M, Fundamentals of Criminal Investigation, Journal of Criminology and Criminal Justice, Serbian Association for Criminal Law Theory and Practice Institute for Criminological and Sociological Research, Belgrade, 2011, p.76

According to Dvoršek, criminalistics strategy is considered to be the area of scientific research which deals with issues that try to solve in which way criminal measures and actions can be limited globally, taking into account the criminal-political and legal frameworks, and the principle of effectiveness. [15]

According to Masleša, criminalistics strategy represents a blue print for optimal path or the optimal use of law enforcement resources for achieving certain objectives. This means that the area of the criminalistics strategy includes measures that relate to overcoming crime as a whole and its individual parts. [16]

Angeleski states that the strategy of action in a particular area means the most effective tactics that are implemented within the framework of a general platform and concept. Optimal criminalistics tactical preventive and repressive actions must be based on a global platform that represents a criminalistics strategy. Global criminalistics strategies, as the most general programme-oriented and a deliberately designed general framework for meaningful and scientifically-based preventive-repressive fight against crime, at the same time includes both theoretical foundation, and practical implementation of certain tactics and strategies of operational process actions. Moreover, he points out that tactical and operational actions should be embedded in a wider strategy, comprehensive strategic approach. The criminalistics strategy is a scientific and specific action against crime at a global level or against a group or specific types of offenses.[17]

Taking into account the above definitions, we believe that criminalistics strategy is a global concept of implementation of all available preventive and repressive measures and actions of the state authorities in order to limit all forms of crime in whole or individually.

In the Anglo-American area, since the term criminalistics has different meaning there, we cannot find the concept of the criminalistics strategy. In classical criminology textbooks, the term strategy does not appear in combination with the word criminalistics. The closest notion of criminalistics strategy are the terms 'crime control strategies' or 'strategies for controlling crime' that can be found in the criminological literature. It is understood that the term also covers the strategies that are not connected with the police, even less with criminal work (e.g. social strategies, integrative control strategies, etc.). In the police professional literature we find the term 'police strategies' which is synonymous to German "Polizeistrategie," and which has, as we shall discover a broader notion than criminalistics strategies.[18]

IMPORTANCE OF CRIMINALISTICS STRATEGY IN CRIMINALISTICS

The origins of the beginning of criminalistics as an independent scientific discipline go back to the late 19th century. The longest period of the first formal criminalistics research is referred to as the pre-scientific era in the study.[19] Scientific researches in today's terms were not widespread, but what is considered as the beginnings of systematic approach to criminal investigation that led to the emergence of science are manuals on the study of crimes from the beginning of the 19th century published by numerous authors. The famous lawyer Ludwig von Jagemann from Baden published an extensive work in 1838, and the work was composed of a book that dealt with the theory and the other book which dealt with the practice of investigation of criminal offenses with extensive casuistic. However, the beginning of criminology as a science is linked to the name of Hans (Johann Gustav) Grossa, an Austrian investigative judge who published the work "Handbook for investigating judges"[20]in 1893.

The pragmatic definition of criminalistics is that it is a science that studies, finds and improves the scientific and practical-experience-based methods and tools, which are best suited for revealing and clarifying the offense, detecting the apprehension of the offender, securing and positioning all of the evidence in order to establish (objective) truth as well as to prevent the execution of planned and unplanned future criminal acts. Briefly put, it is the study of techniques, tactics and methodology of operational, investigative and other court actions and also the prevention of such crimes.[21]

Criminalistics is a unique science, regardless of the generally accepted division on the criminalistics tactics, criminalistics methodology and criminalistics technique. This division has educational significance, since its objective is easier comprehension, understanding and learning the unique criminalistics science, the one more reason for it is that it is based on a theoretical basis and has no practical importance, because the practice requires a unique and systematic application of methods and means of all three disci-

15 Dvoršek, A .: The importance of criminalistics strategies for crime prevention, Proceedings of the Police Academy in Belgrade - The place and role of the police in crime prevention, status, opportunities and prospects, Police Academy, Belgrade, 2002, p.75
16 Masleša, R .: Crime Strategy, Faculty for Criminal Justice, Sarajevo, 2006, p.32
17 Angeleski, M, Crime tactics, "St. Cyril and Methodius University" Skopje, 2003, p.125-128
18 Dvoršek, op.cit.p.22
19 Pavišić, B, Criminalistics -Book first, Golden Marketing, Zagreb, 2006, p.14
20 Karas, F .: (2012), Introduction to Criminal Justice, Croatian Ministry of the Interior - Police Academy, Zagreb, 201
21 Vodinelić, V.: Crime, Department of textbooks and teaching aids, Belgrade, 1996, p.3.2, p.20-22

plines[22]. However, there has been the development of new disciplines in criminalistics; primarily criminal operations, then prevention and forecasting of crime, crime analysis as well as the crime strategy. While criminalistics tactics aims to develop methods and means that are far more specific (criminal tactical rules for certain evidentiary or investigative action), a methodology of crime is directed at developing methods particularly suitable for detecting, proving and resolving certain types of crimes, criminalistics strategy is reduced to the advance planning, the way of response, especially the police but also other relevant authorities, the development of organizational concepts that are focused on creating conditions for general crime prevention and by which the joint action of all available forces can be achieved for the purpose of general crime prevention.[23]

In the beginning, the criminalistics strategy was being developed exclusively as 'anti-strategy for the strategy of criminals'. Some researchers found that criminals and their criminal activities more frequently used certain strategic elements. Before that the criminological research at the Institute of Criminology at the federal criminal office in Wiesbaden in the beginning of the nineties became criminalistics-criminological activities, which means that the research studies have given more emphasis to limitation of crime using criminalistics measures. In 1997 researchers were focused only on the criminalistics research and for that purpose section 'K1 Criminalistics Strategy' was organized, which dealt largely with questions of possibility to limit crime by using the criminalistics strategy (Stubert, 1999: 379-387, according to Dvoršek, Criminalistics strategy as a New Branch of Criminalistics).

In countries that belong to the English-speaking world the terms like criminalistics strategy and criminalistics are not used in the way they are used in continental Europe. Fortunately, there are many expressions which comprise somewhat similar, though slightly wider content (crime control, strategic policing or similar). It should be noted that in these countries it is not in dispute that crime police must cherish strategic approach in their work. B.Simonović was the first one in Serbia who published works on criminalistics strategy (under the influence of the German school of criminalistics). The subject of consideration of these works was strategic planning as a part of learning about planning in criminalistics.[24]

We can say that the criminalistics strategy as an independent scientific and educational discipline being studied in some countries of our region at universities which deal with crime-related security issues. Hence, the criminalistics strategy is being studied in Montenegro, Bosnia and Herzegovina, Slovenia[25] while in Serbia, Croatia and Macedonia there is not a subject called criminalistics strategy which can be studied by students.

Given the current socio-political and economic situation in the Republic of Serbia, and considering the fact that many national strategies have been made and among other things some of them are primarily criminalistics character, such as strategies to combat human trafficking, illegal migration strategies of opposition and strategies against drugs, etc., we believe that the introduction of the criminalistics strategies in certain colleges in the country which deal with security issues, would be significant for more than one reason. The pressing problems that the country is facing are primarily organized crime and corruption. By using the strategic approach of criminalistics police, which involves pooling criminal theories and practical operational criminal activities, it is possible to achieve satisfactory results in terms of limiting these types of crime.

The question is why there has been a general development of criminalistics strategy. The reasons for this are numerous, among them the leading ones are: the emergence of new forms of crime or existing forms become more sophisticated, organized crime groups are easier to adapt to social and economic relations, combating organized crime represents one of the basic priorities of each state. Having this in mid, criminalistics strategy is not the only one which is experiencing its prosperity, but also leads to the development of numerous strategies whose aims are to improve the conditions for life and work of the entire community.

Despite the limited capabilities of statistical comparisons, the research shows that in the period from 60's to 90's of the last century, the level of registered crime in European countries increased by more than three times. Investigation (solving) of crime has fallen from about 55% to 40% of a certain offenses against property such as home burglaries, bicycle theft or pick pocketing even fell at about 10%. Then the organized crime appeared, and its dominant form became drug trafficking. Due to inadequate investigations using classic methods, increasing number of crimes remained undetected. Terrorism emerged in some countries. One of the new emerging forms of crime is environmental crime. The most afflicted territory was Europe. The reason for this was strong currency, a large concentration of wealth, excellent infrastructure and a liberal philosophy, with limited opportunities for funding some behaviours that could be hidden under

22 Bošković, M .: Crime teaching methodology, Police Academy, Belgrade, 2005, p.6
23 Škulić, M.: Fundamentals of Criminal Investigation, Journal of Criminology and Criminal Justice, Serbian Association for Criminal Law Theory and Practice Institute for Criminological and Sociological Research, Belgrade, 2011, p.76
24 Simonovic, B, Two Theoretical Concepts "Criminalistics Strategy" and / or "Strategic Approach in Criminal Police Work" - Which of These Two Gives More "Archibald Reiss Days", Academy of Criminalistics and Police Studies-German Foundation for International Legal Cooperation (CDI), 2014, p.303-307
25 The first scholars who wrote about crime strategy in Slovenia were Maver and Dvoršek.

the cloak of everyday market behaviour[26].There was an increase in the number of homicides in which the victim and the offender had no direct connection, which could rarely be random, reflecting an increase in the rate of violent offenses, some of which were contracted. The increase of manifestation of certain forms of very complex criminal offenses, or complex forms of crime, especially one that is characterized by harsh discovering and proving, as arms trafficking, drug trafficking, human trafficking and so on. The increase in high-tech forms of crime, which is associated with very rapid advances in technological development of mankind, and in particular, the rapid introduction of completely new or substantially improved and applied technologies, such as, for example, was the case with the expansion of computer use, the Internet use, creating the so-called cyber space as a relatively new and highly specific 'environment' for carrying out numerous criminal offenses. Highlighted effects of social and legal transition in many countries, such as Serbia, which was between other things, reflected in the rapid change of the traditional approach to social problems.[27]

According to Boskovic, criminalistics strategy aims to:

– identify priority areas of criminalistics activities;

– by analysing define meaning and 'new' value of criminalistics-relevant data;

– contribute to the selection of objectives;

– enable the selection of the best strategy;

– define the financial basis for the its implementation;

– provide a good basis for making decisions for the management;

– create a base for creating changes that will allow the development and prosperity, i.e. Effective solving of criminalistics problems.[28]

Theoretically speaking, at the highest levels, crime strategy transfers to a greater or lesser extent in some other strategies, or overlap with them to a greater or lesser extent, or (apparently) lost, that fits into the strategy at a higher level. At the higher level criminalistics strategy may exceed to police strategy, or general security strategy, and so on. For example, human resource matters, remuneration in the police, the strategy of motivating police officers, anti-corruption strategies in the police are not criminalistics strategies in the narrow sense of the word but they have an impact and its reflection on the work of law enforcement agencies and revealing and suppression of criminal offenses. Because of that, it is sometimes difficult to distinguish (or it is not even possible, often there is no need) the so-called 'criminalistics strategy' from the so-called 'police strategies" or 'strategies of police management'[29].

Along with the criminalistics strategy and criminal field of work, the development of criminal intelligence work[30] first starts to be used in Britain and America.

The concept of policing based on intelligence work represents the basis of efficiency, from patrolling to organized work in investigations, especially of organized crime. Intelligence, collection and analysis or the provision of relevant, objective information represent a precondition for making adequate decisions on work priorities, operational, tactical and strategic options. When the sources of information are people, there are additional risks and problems in the administration and management of these resources, and the information received. It is therefore very important that officers understand the role they have in the process of criminal intelligence work and how they can achieve the best results by finding out the following key aspects.[31]

Strategic criminalistics intelligence work is focused on future events and it deals with predicting trends. In the area of prevention, criminal intelligence works within the framework of the so-called secondary soft, indirect prevention which is a typical predictive approach. Predictive approach means that intelligence and analytical activity are primarily directed towards predicting future criminal activities and attempts to prevent them rather than to react to actual crimes and perform standard police work which is mainly the task of local police forces. The objective of strategic criminalistics intelligence work is to provide an assessment based on the prediction of current and new risks and threats that generate crime. This estimate is

26 Dvoršek, op.cit.p.20

27 Skulić, op.cit. p.76

28 Bošković, G.: Organized Crime, Criminal Police Academy, Belgrade, 2014, p.131

29 Simonovic, B, op.cit.p.310

30 When we talk about criminal intelligence work it is necessary to point out the fact that the essence of its activity is aimed at secretly collecting data. That means that the investigators who are engaged in intelligence work should not take specific operational and tactical measures and actions, that their work should not be seen, i.e. the distance in relation to those who commit criminal activity. The role of criminology that secretly collects operational information is to observe and monitor events, performs appropriate conclusions, strategic planning and learning through practical and theoretical work (Radovic, N., Djurdjevic, Z., Vukovic, S. (2014), Crime and crime intelligence analysis, Proceedings of International Thematic Significance "Archibald Reiss Days", Academy of Criminalistics and Police Studies, Belgrade, Volume I, p.357)

31 Practise Advice Introduction to Intelligence-led Policing .: Produced on behalf of the Association of Chief Police Officers by the National Centre for Policing Excellence, 2007, p.3

produced in the form of a review of criminal resources, threats, trends and intentions, in accordance with organizational strategic objectives and principles. Strategic criminalistics intelligence work provides data that provide long-term vision of the context and issues relevant to the work of the police[32].

The detailed comparison of the model "Kriminalstrategie" (criminalistics strategy, and criminalistics intelligence work) points out to some differences. The concept of the criminalistics strategy does not emphasize so strongly the role of crime analysts. In this concept of criminalistics strategy the greater part of the job of solving problems is for those who make decisions. The reason is probably in the approach to identify and solve the problem of combating crime. The concept of the criminalistics strategy emphasizes the superiority of crime policy, which sets goals for criminalistics strategy, which means choosing a strategic level, and the concept of criminal intelligence work are equally important products for tactical, operational and strategic levels. It does not matter at what level is the product used (assessment, analysis, sample), what is important is its usability. Proactivity emphasizes both models.[33]

CONCLUSION

While talking about crime strategy, we can recognize that it has not developed equally as a scientific discipline in the world, as well as in our region. However, we can conclude that the appearance of a criminalistics strategy as a discipline of criminology was actually the need of society to provide a response to the overall crime as well as the answer to the strategies of criminals i.e. to the strategies of organized crime groups. Although there are a lot of differences between theorists when it comes to the concept of 'criminalistics strategy', we believe that a strategic approach to detecting and solving crimes is more than required. Although the criminalistics as a science is itself a kind of strategy, we believe that it is necessary to introduce specific teaching subject-Criminalistic Strategies- in all higher education institutions that deal with criminal security issues, so that the future of criminalist investigators could strive to achieve higher goals in the criminalistics operational activities. The government of the Republic of Serbia adopted a number of strategies in the fields of economy and finance, infrastructure, agriculture, forestry, environment, education, science, defence and foreign policies that were largely limited to the time period of four years or more, and among them there were also criminalistics strategies. Since we have mentioned this, we will single out certain strategies that are essentially and primarily criminalistics even though some of them have ceased to be valid while others are still current: Strategy for combating illegal migration, the National strategy for combating corruption, Strategy for combating drugs, National strategy for fighting organized crime, the National strategy for combating money laundering and Terrorism financing strategy for combating trafficking in human beings, National strategy for prevention and protection of children from violence, the National strategy for preventing and combating violence against women in the family and partner relationships. If you look at these strategies, we can clearly conclude that they are primarily related to certain types of crime which can threaten society and the economy, as well as certain categories of persons who are most vulnerable and those are actually women, children and irregular migrants. Problems that occur during the implementation of the strategy relating to the prevention and combating of crime are primarily seen in their incomplete implementation or to failure achieve the previously set objectives that are defined as a priority. Although criminalistics strategy involves a comprehensive approach of society and response to the particular state of crime in the country or region, the response of the society is not complete and it is not unusual that strategies remain only 'a dead letter'.

REFERENCES

1. Bošković, M.: Kriminalistička metodika, Policijska akademija,Beograd, 2005.
2. Bošković, G. Organizovani kriminal, Kriminalističko policijska akademija, Beograd, 2014.
3. Dvoršek, A.: Značaj kriminalističke strategije za prevenciju kriminaliteta, Zbornik radova Policijske akademije u Beogradu – Mesto i uloga policije u prevenciji kriminaliteta,stanje,mogućnosti i perspektive, Policijska akademija,Beograd,2002.
4. Dvoršek,A.: Kriminalistička strategija-nova grana kriminalistike, Sarajevo, 2002.
5. Dvoršek, A.: Kriminalistička strategija,Univerza v Mariboru fakulteta za varnosne vede, Ljubljana, 2008.
6. Dvoršek, A.: Kriminalistički obaveštajni rad i njegove perspektive u kriminalistici, Kragujevac, 2009.

32 Fatić, A, Korac, S, Bulatović, A, Ethics of criminal intelligence, Institute for International Policy and Economics, Belgrade, 2013, p.149.
33 Dvoršek,op.cit,p.34

7. Fatić, A, Korać, S, Bulatović, A, Etika kriminalističko-obaveštajnorada,Institut za međunarodnu politiku i privredu, Beograd, (2013),
8. Karas, Ž.: Uvod u kriminalistiku, Ministarstvo unutrašnjih poslova Republike Hrvatske – Policijska akademija, Zagreb, 2012.
9. Masleša, R.: Kriminalistička strategija, Fakultet kriminalistčkih nauka, Sarajevo,2006.
10. Pavišić,B.: Kriminalistika –Knjiga prva, Golden Marketing, Zagreb, 2006.
11. Radović,N., Đurđević, Z., Vuković, S., Crime intelligence and crime analysis, Thematic Proceedings of International Signifince "Archibald Reiss Days", Academy of Criminalistics and Police Studies,Belgrade,Volume I, 2014.
12. Simonović, B.: Kriminalistika, Pravni fakultet u Kragujevcu-Institut za pravne i društvene nauke, Kragujevac, 2004.
13. Simonović, B, Two theoretical Concepts: "Criminalistics strategy" and/or "Strategic Approach in Criminal Police Work" – Which of These Two Gives More", "Archibald Reiss Days", Academy of Criminanalistic and Police Studies-German Foundation for International Legal Cooperation (IRZ), 2014
14. Škulić,M.: Osnovi kriminalističke istrage,Revija za kriminologiju i krivično pravo,Srpsko udruženje za krivičnopravnu teoriju i praksu-Institut za kriminološka i sociološka istraživanja,Beograd, 2011.
15. Vodinelić, V.: Kriminalistika, Zavod za udžbenike i nastavna sredstva, Beograd, 1996.
16. Vuković, S., Prevencija kriminala, Kriminalističko policijska akademija, Beograd, 2010.

UDC: 343.37(497.7)
343.53(497.7)

SCOPE, STRUCTURE AND DYNAMICS OF ECONOMIC CRIMES IN THE REPUBLIC OF MACEDONIA

Svetlana Nikoloska[1]
University "St. Kliment Ohridski", Bitola, Faculty of Security, Skopje

Abstract: Economic crime is always of interest for the scientific research, particularly the emergent forms and types of economic crimes, the scope, structure and dynamics of economic crimes in relation to the reported, accused and convicted perpetrators. In recent years, there have been a number of reforms in the criminal law area in the Republic of Macedonia, mainly performed by redefining the existing economic crimes and introducing new penal and criminal procedure laws, and by introducing a completely new concept of running the criminal investigation. New measures and activities have been introduces, and the list of special investigative measures has been expanded for the purpose of improving the criminal investigation and providing the relevant evidence for the smooth running of the criminal proceedings. Changes in legislation have brought about an improvement of the situation in terms of detecting, clarifying and proving of economic crimes, which can be analyzed by the data for reported, accused and convicted perpetrators of economic crimes, as well as analysis of the type and amount of criminal proceeds from these criminal acts. This paper is an analysis of the emergent forms of economic crimes in accordance to the nomenclature of the Ministry of Interior made on the base of the characteristics of these criminal offenses which distinguished them from the classic crime. The analysis has been done based on the statistical data for the reported, accused and convicted perpetrators of economic crimes for the period 2007 - 2013, and comparison is made with research from the period 1997 - 2006. The analysis of the dynamics of reported, accused and convicted perpetrators of economic crimes has been performed by separate groups and years, outlining the structure of the share of certain groups of economic crimes in total economic criminality. It has brought out indicators for the contribution of reforms in economic crime to improve procedures in order of final court cases which commenced criminal proceedings, and indicators to improve the procedures in terms of providing relevant evidence throughout investigation.

Keywords: economic crime, suspect, accused, convicted, criminal investigation.

INTRODUCTION

The need for monitoring and study of economic crime as a socially negative phenomenon, a phenomenon with a negative sign, in a systematic way, with appropriate scientific methodology is determined by two essential components in the society. The first component is that it is a crime with its phenomenology expressed through multiple manifestations of criminal activities and with the sole motive of the perpetrators acquisition of illegal profit. The perpetrators of this crime are distinguished by their special status and professional properties arising from their positions in society, the power, the function, workplace, and their legal authorizations. The situation with economic crime in terms of its scope, structure and dynamics can be seen by the indicators of social, political, legal, economic and financial conditions in the society. The situation with economic crime, the increase or decrease of the effectiveness of law enforcement agencies, analyzed by statistical data indicates the policy of suppression of this type of crime that covers all major areas of society. The other component is determined by the need for monitoring of economic crime in its essence and nature. By nature, the economic crimes are invisible, yet perceptible. The economic crime is essentially a hidden phenomenon, where perpetrators tend to stay unknown, they don't want their criminal activityto be discovered, and after that follows state repression for discovery and proof of the offense. They previously take the measures to remain undetected, unknown to law enforcement agencies, and their criminal fruits to remain to them asacquired wealth, for which they know the origin, but for the law enforcement agencies it is enigma until its discovery, clarification, proving and imposing the final sanction.[2]

The research of the phenomenological characteristics of economic crimeis significant, because it recognizes danger and harmfulness, especially if we take into account that this type of crime violates the rights - economic relations, the damages suffered by the State and of all its citizens. If with the crime related to

1 svetlananikoloska@hotmail.com
2 Арнаудовски Љ., *Методолошки проблеми на статистичкото евидентирање и следење на економскиот криминалитет*, МРКПК, бр. 2 - 3, Скопје, 2008, p. 454.

the classic crime, suffers individual, with the economic crime suffer all citizens. To recognize the dangers of economic crime, we should first define the notion of economic crime and to determine its manifestations and forms, and the consequences are rubbed. It is especially important to study the statistical data on the structure of the economic crimes in order to obtain indicators for the most performed criminal offenses, their perpetrators, in order to make a comparison on how many of the reported perpetrators are convicted to perceive penal policy towards the perpetrators of these crimes. If we take into account that the perpetrators of economic crimes are not common criminals, they are criminals who are in a position to influence the actions of providing evidence and especially in judicial proceedings and broker acquittals or minimal prison sentences.

The economic crime in its essence is a crime that occurs less legally, avoiding or disrespect for legislative regulations that regulate legal economic relations. In conditions the ever-changing legislative regulations governing the legal, the economic and financial relations, complex the separation of the legal from the illegal, it is difficult to draw the line between what is the legal and what is the illegal operation. This is a particular difficulty in relation to the discovery of criminal activity of the economic entities, detection and classification of criminal activities in specific crimes. The economic crime, basically has a tendency to be installed in the existing economic and commercial system, already established structure of economic entities and institutions in the country, and is exercised in organized forms that simultaneously allow hiding the already existing forms of organized economic - financial and legal work. If we take into account that this crime is done in the exercise of the economic (business) running between economic entities, and among the economic entities and state authorities and institutions, then we can understand the danger of this crime and the difficulty of its detection, especially difficulties in its proof and the sanctions. Because the economic crime has the characteristics of the crime of "white collars" and the crime that is between legal and illegal, crime located which are not only in the penal code, but also in other laws complicates the identification of crimes you need to include in the definition of this crime. The defining of eeconomic crimes is an important prerequisite to investigate, because the definition should include the general elements and characteristics of the economic crimes and their characteristics that allow differentiation between them and classic crimes. The successful definition of economic crime, especially its manifestations and forms, should serve as a basis for its statistical monitoring and research.[3]

Special difficulty in terms of determining the manifestations of economic crimes are new manifestations and forms of criminal behavior that were not criminalized in the Macedonian penal system, the introduction of computerization in the work of economic subjects and all state bodies and institutions provides great opportunities for criminal activity. New forms of criminal activity, which is manifested in practice have conditioned the need for redefining the economic crimes and criminalizing new offenses, and the introduction of criminal liability of legal persons and the introduction of the measure confiscation of criminal proceeds and the property acquired. Reforms started with amendments to the Criminal Law of 2004[4] and major reforms in terms of redefining the economic crimes made in 2009[5] with amendments to the Criminal Law and the introduction of new crimes and it accepted the recommendations of the international conventions (Vienna and Strasbourg Convention, the Palermo Convention, etc.) and accepting the recommendation of the Committee of Ministers of the Council of Europe in 1996 and the Recommendation of the Committee of Ministers in 2001 that recommended incrimination of several forms and techniques of money laundering and criminalizing more criminal activities in customs and fiscal offenses, computer and other offenses.

NOTION AND DEFINING OF THE ECONOMIC CRIME

In professional literature there is no unique definition for the economic crime. We use the terms corporate criminality, criminality of white collars, crime of corruption, criminality of the curves zones etc. The Committee of Ministers of the Council of Europe Recommendation No. R (81) 12 defines economic crime through individual criminal behavior: cartel criminal acts fraud and abuse of economic situation by multinational companies, fraud and abuse of obtaining national and international donations, computer crime, false companies, falsification of the balance legal persons or accounting offenses, fraud given the economic situation and corporate capital companies, breaking the security standards and protect the health of the employees, fraud detrimental to creditors (bankruptcy, breach of bank or industrial rights), of consumer fraud, disloyal competition, fiscal offenses, customs offenses,offenses targeted control of money and offenses of market stock market. These criminal behaviors include almost the all criminal behavior of economic - financial field, and the perpetrators of this crime in society are mostly reputable and respected citizens and the damages that are inflicted are larger. A characteristic of this crime is that it is protected or directives

3 Ibid, p. 471.
4 Сл. весник на РМ, бр. 17/04.
5 Сл.весник на РМ, бр. 114/09.

of the government, which belongs to the group of criminal behaviors that are difficult to detect and even more difficult to elucidate and prove by the authorities because in most cases there is a connection with these structures, as serious organized crime networks. Almost there is no area of human life where it is not present economic crime in the name of acquiring great wealth. This type of crime is happening in the area "abuse of the confidence", which is the guiding principle of the work in this area and they are offenses which with its overall coverage endanger general and individual interests.

Usually for economic crime is said to be socially - negative criminal phenomenon that is carried out by persons who possess a certain quantum of knowledge of the economy and payment operation and who on the criminal manner by utilizing trusted authority and positions are obtained primarily with certain economic means, thus inflicting damage to the budget of the state and citizens in general. As phenomenon the economic crime takes a high position in overall crime, noting through its extensive quantity, structure and dynamics, but also the huge damages which it caused.[6]

One of the most frequently cited definitions of economic crime originates from Edwin Sutherland president of the American Sociological Association, who in his speech to the Society in 1939 for economic crime uses the term crime of "white collars" or (white - collar crime).[7] Sutherland defines this crime that appears in the area of economic operation, which forms are most often manifested in mismanagement in connection with the sale of various actions, false advertising of goods, false presentation of financial situation and operations of individual corporations, bribery of business partners, direct or indirect bribery of state officials, in order to ensure a favorable business arrangement, embezzlement, improper spending of funds, tax evasion, etc.

But later, Sutherland gave a new definition of the crime of "white collars", designating it as a "crime within their professional activity, carried out by people with high social prestige." This definition of economic crime as a crime of the rich and privileged social strata which includes the economic, financial and political oligarchy, or as a set of offenses performed by people who have a higher social status in the exercise of their profession. "Crime of "white collars" is a form of professional crime which covers crimes performed by persons belonging of the upper, ruling circles in business life, state administration or the free professions using their influence and connections in the society. These offenses are designated as professional criminal offenses because they are performed in the conducting or twisting professional role. As it is shown by the term "crime of white collars" (as opposed to the so-called "crime of blue collars"), they are offenses of those people included in the "fine" or "urbane" world, those who belong to the higher social - economic strata. It is assumed that they in their behavior, in general, are not so different from the "little people", except that they know how to represent themselves in "better light." Because of the non-violent performing of the crimes within their profession and the reputation that these perpetrators have, they can skillfully avoid the criminal responsibility."[8]

Except the theoretical attempts for defining the economic crime, the definition should be made for the practical work of the relevant government authorities and services which in accordance with their needs record statistics for the economic criminal offenses, as well as individual working (operational) definitions that are determined at the theoretical - empirical research and analysis of specific economic crime.[9]

The term economic crime is defined, commonly, according to the legislation for protection of the state and the private property and property rights and interests of citizens, or they are a certain number of criminal offenses defined by the law.

The economic offenses are non-violent illegal acts which are characterized by fraud, concealment, events of default, avoiding or evade laws etc., and are executed with the aim to get to the money, property or services; to avoid payment or loss of money, property or other services and provide other personal or business benefits.[10]

According to the above definition, the economic crimes are non-violent illegal acts, which means that the perpetrators in their criminal behavior do not apply the physical force or violence. In these cases they apply skills in evading or circumvention of certain regulations, acts, agreements etc. These crimes are carried out by a certain category of perpetrators from the group of experts and professionals who have particular social, political or social position and who are in situation with only one of their signature, decision, etc., to gain (illegally) financial assets for personal, party or business benefits. The most appropriate defining of this term should be the definition that will include elements of socio - economic living conditions, criminal - legal regulation, the object of the attack and the possible perpetrators of the economic crimes.

---

6 Арнаудовски Љ. , Нанев Л. и Николоска С., „*Економскиот криминалитет во РМ*", Македонска ревија за кривично право и криминологија, бр. 1, Скопје, 2009, p. 179

7 Бановић Б., *Обезбеѓене доказа у криминалистичкој обради кривичних дела привредног криминалитета*, Београд – Земун, 2002, p. 13.

8 Кралев Т. , *Криминалистика – лексиконски курс*, Селектор, 2007, p. 373.

9 Бановић Б., *op. cit.* p. 13.

10 Димитров Д., „Економски деликти", Скопје, 1998, p. 4 – 5.

Today this definition experiencing significant changes since, using new technology and mass communication growing number of members from all layers social an opportunity to engage in illegal economic activities. In economic crime, which many scientists call "unconventional crime" there is a high degree of agreement that it becomes major problem in modern society, primarily because of its close association with the economic and political activities, and the fact that the elements of so-called unreal criminal acts which includes this term are set on the borderline with legal activities.[11]

Using the special position in society indicates that these acts are non-violent in terms of physical force or psychological violence, which sometimes can be stronger than the physical violence and the reduction of the risk is through indenting and connecting criminal activity with the legal sphere of business, finance, banking, politics, the functions of the state and other social spheres and is the most effective way to eliminate the risk of detection and prosecuting, because the general confusion of the permissible and the forbidden leads to blinded some and block the sensor power of penal legislation and criminal justice. While the formal system of protection consists in helping or allowing the criminal activities by the state authorities or the blocking of the bodies of criminal prosecution and criminal justice and putting them through corruption in order to protect or tolerate criminal activity because of the expected economic or political benefit, the informal system is a form of self-organization of the criminal underworld against the system of criminal justice.

For economic crime somewhere it is noted that it is a professional crime or crime which is carried out in the exercise of a profession (accountant, banker, treasurer etc.), but the crime within the performing function (director, officer, chief), activity or duty (doctor, notary, lawyer, etc.). This categorization differs from classic crime where the perpetrator has specialized in committing crimes - crime becomes his profession, - cheater, thief,racketeer etc.. In the economic crime perpetrators performed the activities within their profession, activity or duty (already acquired, possession of a diploma, a decision to work, certificate, etc.), while the classic professional criminal offender has long been engaged in performing the same criminal offenses so he perfects its delinquent tactics and technique.

The economic offenses are classified based on their criminal characteristics certainly include the building of a criminal attack, the method of execution, and what is important in these offenses are properties of status of the offenders who are defined by law, and the law provides sanctions for abuse legal or statutory properties, powers, benefits etc. According to Dimitrov[12] considerations in determining the purpose of accepting the notion of economic tort and leaving the term commercial tort is that the need to protect and enhance the integrity of government institutions to protect and enhance the integrity of the system of free enterprise, competitive market and the state economy as a whole, to protect and promote the welfare of the citizen as an individual, including his health, safety, physical environment and the ability to exercise political, the economic and other basic rights and to promote respect for and compliance with state laws by public, according to the concept of economic tort was not covered, or the notion of economic tort included attacks on social property performed within the organizational unit. Private property rights to a healthy environment, human health was not covered by this term.

SCOPE, STRUCTURE AND DYNAMICS OF THE ECONOMIC CRIMES IN THE REPUBLIC OF MACEDONIA

The need for research on the scope, structure and dynamics of the economic criminal offenses isimportant by the more aspects because of the getting indicators for the number of reported perpetrators of these criminal offenses is essential, above all that it is a criminal offenses that is done by the perpetrators with status properties in performing criminal use of their position, function or powers. The situation with the manifestations of crime or perpetrators reported for individual economic criminal offenses gives indicators of what are the crimes that are most committed and how to build a strategy to prevent those criminal types, and building strategies for legislation to check the personal capacities and values of those who aspire to compete or perform official duties and powers. After the presentation and analysis of statistical data for the economic criminal offenses is required for comparison with the same or similar offenses abroad and developing common strategies and policies for cooperation in criminal and financial investigation of the crimes. Precisely because in 2003, the UN adopted the Dublin Declaration that contains the ten recommendations, the sixth recommendation is determined by the need to build a European system for crime statistics and developing a strategy aimed at producing information necessary for analysis and monitoring of movements (trends) in the crime. "Recording, monitoring, detection, elimination of crime, setting the programs and actions to prevent, is directly related to the possession of empirically verifiable knowledge of the phenomenological characteristics of crime. To be able to resist the society must have scientifically checked knowledge

11 Камбовски В., *Кривична одговорност на правните лица,* МРКПК, бр. 2-3, Скопје, 2008, p. 319.
12 Димитров Д.,op. cit. , p. 8.

of the appearance that we call crime. Consequently its characteristic as mass phenomenon, obliged chooses the statistical methods and proceedings, their recording, keeping, monitoring, processing of the collected statistical data, presenting them in a way that they give the opportunity to review the phenomenological characteristics, to identify some occurrences, relations with etiological significance the emergence and of that foundation to set programs for the prevention, the disposal and prevention."[13]

The thesis that economic crime, its scope, the prevalence, the phenomenological forms and structures emerge as its bearers are the best and most reliable indicator of the situation in a given society which causes multiple empirical verification and confirmation of the place so the determined this criminality and the history of development of society. With certainty it can be argued that there is no period, no stage, or development stage of the human society, in which there was no economic crime, whether it be a class or a class free society. Not far off allegation that economic crime is one of the important elements of the structure of crime and determinant of the overall structure of crime, the structure of society as it emerges and is determined by economic, legal, political and social structure of society.[14]

In this paper it is made a research of reported, accused and convicted perpetrators of economic crimes according to data maintained in the State Statistical Office of the Republic of Macedonia for the period 2007 - 2013. According to the data registered in the annual reports may be concluded that for a huge number of economic crimes there are not registered offenders, while in certain chapters of the Criminal Code is evident data only for some crimes, and for a huge number of crimes there are not reported perpetrators, so they are not included in the analysis. Analyzed data by chapters of the Criminal Code, where there is registered data, can be seen the situation per years by the reported, accused and convicted perpetrators of economic crimes. Also based on these data can be analyzed the structure of economic crimes by groups in order to extract indicators for whichof the economic crimes are most committed and also analysed by years in accordance with their dynamics or their movement.

The research data are extracted from the following groups - Chapters of the Criminal Lawin the Republic of Macedonia:

- Chapter 15 - Crimes against the rights and freedoms of man and the citizen
- Chapter 17 - Crimes against labor relations
- Chapter 22 - Crimes versus environment
- Chapter 23 - Crimes against property
- Chapter 25 - Crimes against the public finances, payment operations and the economy
- Chapter 30 - Crimes against official duty
- Chapter 31 - Crimes against the justice
- Chapter 32 - Crimes against legal traffic
- Chapter 33 - Crimes against the public order

Scope, structure and dynamics of economic crimes systematized under Chapter of the Criminal Code in the Republic of Macedonia for the period 2007 – 2013

Year	Ch. 15			Ch. 17			Ch. 22			Ch. 23			Ch. 25		
	Re	Ac	Co	Re	Ac	Co.	Re	Ac	Co	Re	Ac	Co	Re	Ac	Co
2007	/	/	/	42	14	5	136	138	117	12	33	3	569	365	268
2008		//	/	56	18	14	152	59	49	15	16	16	596	312	251
2009	29	/	9	48	25	7	214	89	71	29	38	7	543	266	204
2010	40	12	12	43	30	19	182	90	82	37	27	24	620	263	203
2011	14	20	20	51	31	18	174	88	70	45	9	9	472	308	240
2012	6	20	16	26	19	12	253	106	92	23	25	21	493	285	212
2013	14	8	8	53	15	10	217	97	64	46	36	30	510	336	255
Total	103	60	65	319	152	85	1328	667	545	207	184	110	3803	2145	**1633**

Ch. 30			Ch. 31			Ch. 32			Ch. 33			**Total**		
Re	Ac	Co	Re	Ac	Co	Re	Ac	Co	Re	Ac	Co	**Re**	**Ac**	**Co**
930	256	153	39	25	6	70	51	39	63	47	41	1861	929	632
1112	291	175	52	18	5	89	43	25	64	45	41	2136	802	576
1061	343	167	25	17	9	68	40	25	140	30	29	2157	848	528
1067	262	142	38	8	4	67	43	35	60	25	24	2154	760	545
825	365	133	48	20	11	59	43	30	71	90	70	1759	974	669
843	317	150	36	26	15	59	51	28	177	56	51	1916	905	597
927	247	137	16	20	11	73	31	22	112	137	20	1968	927	638
6765	2081	1057	254	134	61	488	302	204	687	430	276	13954	6155	4036

13 Арнаудовски Љ., op. cit., p. 454.
14 Арнаудовски Љ. , Нанев Л. и Николоска С.,op. cit. p. 175.

The economic crime is mainly comprise by the criminal acts in the two chapters or two large groups of crimes, including: offenses against the public finances, payment operations and the economy and crimes against official duty, but also includes a crime against labor relations, and crimes in other groupings which according to their manifestations are represent with the smaller number as crimes as well as perpetrators of these crimes.

According to the data presented in Table 1, in the research period 2007 - 2013 reported perpetrators on committed economic crimes are a total of 13,954 of which 6,155 have been accused and convicted perpetrators have been 4,036. The percentage of the accused was 44.1% compared to the reported perpetrators. The convicted against the accused offenders was 65.6% and convicted offenders were 28.9% compared to the reported perpetrators.

These data compared with the previous analysis period indicates an improvement of the situation in the conviction of perpetrators of economic crimes. According to research for crimes against official duty for a period 1997 - 2006 year convicted was 12.7% compared to the reported perpetrators and if we know that more than half of the economic crime is precisely these crimes.

The improvement in the percentage of sentenced is due to the multiple factors, but as the most important to stand out are the organized approach to criminal and financial investigation of economic crime through the process of planning, coordination and comprehensive approach to conducting the pre procedures are preconditions for successful conduct of criminal proceedings and adopting of court judgments against the perpetrators but also imposing measures of confiscation of criminal proceeds and the property acquired from crime.

According to data presented per years the largest number of reported perpetrators are observed in 2009, 2,157 perpetrators. The analysis of the economic crime indicates that the total number of reported perpetrators is 13,954, which means 48.5% were crimes against official duty, 27.3% crimes against the public finances, payment operations and the economy 9.5% crimes against environment, 4.9% are crimes against the public order, 3.5% are crimes against legal traffic, 2.8% are crimes against labor relations, 1.8% are crimes against the judiciary, 1.5% are crimes against the property, and 0.7% are crimes against the freedoms and rights of human and the citizen.[15]

According to the studies conducted between 1997 and the first six months of 2006 total of 8,504 crimes were committed, and total of 10,486 perpetrators were reported. As regards the structure of the crimes of the total 48.4% of the reported perpetrators of crimes against duty in the Chapter 30, 39.9% were reported perpetrators for offenses against the public finances, payment operations and the economy in the Chapter 25, and the remaining 11.3% economic crimes against labor relations in the Chapter 17, economic crimes against environment and nature in the Chapter 22, economic crimes against the property in the Chapter 23, economic offenses against the justice in the Chapter 31, economic crimes against legal traffic in the Chapter 32 and economic crimes against the public order in the Chapter 33.[16]

According to the research of economic crimes against official duty for the period 1997 - 2006, total economic crime is represented by 49.9% and economic offenses in total crime is represented by 5.8%. Although the percentage of economic crime in the total crime is probably low, the danger of the crimes is very highly expressed in millions denars harm or earned illegal profit. According to the analysis of individual crimes most run offence in the research period was "Abuse of official position and authority", art. 353 with 64.1% of the representation; "Forgery of official document" with 19.2% representation; "Embezzlement in office" with 7.8% representation and the remaining 8.9% are of other criminal acts in the chapter.

According to the research conducted by the Arnaudovski, Nanev and Nikoloska[17] for the period 1995 - 2007 at the two Chapters of the Criminal Code that are most common in the structure of economic crime - Crimes against office and Crimes against the public finances, payment and the economy with the total number of 1,499 reported adult perpetrators, 930 were offenders against official duty, or 62.04% and 569 or 37.94% were offenders of crimes against the public finances, payment operations and the economy. In criminal acts against duty the most represented was crime, "Abuse of official position and authority", with 88,06% and from the crimes against the public finances, payment operations and the economy the most present crime was ",Tax Evasion" with 36.4 %, crime "Falsification of money" with 23.6% of the total number of reported perpetrators of these crimes. The economic crime in the total crime according to research for the period 1986 - 2007 has been different in years and the lowest incidence with 4.99% was recorded in 2000, and 23.63% in 1989. In the years since independence and implemented transformation of socio - economic system or 1992 - 2007 the largest representation was in 1992 with 14.32% and the already mentioned 4.99% in 2000. According to the analysis, the number of reported perpetrators for economic crime is higher or their participation in the overall crime was higher in the years after the parliamentary,

15 Николоска С. , *Кривични дела против службената должност*, Графотранс, Скопје, 2008, p. 118.
16 Џуклески Г. и Николоска С., Економска криминалистика, График Мак Принт, Скопје, 2008, p. 163.
17 Арнаудовски Љ. , Нанев Л. и Николоска С. , *op. cit*., стр. 189.

presidential and local elections because after each shift of a set of power were reported their previous illegal or criminal actions.

CONCLUSION

The research of economic crime through analysis of statistical data for the reported, accused and convicted perpetrators indicates that this crime is carried out in the area of abuse of office and in the area of public finance and payment operations. The other groupings of economic crimes are under-represented in total economic crime committed by offenders in the country. At the very beginning of the paper, this criminality was defined in order to have a clear view which crime is being investigated, which are the dangers of committed the economic crimes and in which areas they are mostly performing. Based on the research period 2007 - 2013 and the comparison with the period 1997 – 2006 we can perform the following conclusions:

- In both these periods of research are most represented crimes against official position in the overall economic criminality in the country, the percentage of representation of 48.5% in the period under study, and researched in the previous period was 48.4%. They are identical results, so it can be concluded that the crime of abuse of office in the country is evident problem.
- The performance of economic crimes damage the state budget, and the crimes are performed by officials and responsible persons who are elected, appointed or law entrusted to them performing activities in government agencies, institutions and public enterprises.
- In the research period 2007 - 2013 the percentage of convicted offenders is higher – 28.9% in comparison with the number of the total economic crimes in the previous period that was 12.7%, which gives a clear indication for the situation regarding the quality of conducting the investigation and judicial procedures and the provision of relevant evidence. This indicator can mean reducing judicial corruption wherever they performed evidence provided in the pre-trial and investigation. It can be an indicator of quality improvement the conduct of the preliminary investigation (criminal) proceedings and the conduct of financial research criminal the acquired yields (type and height).
- On the second place by the representation, are the crimes against public finances, payment and commerce with 27.3% in the period 2007-2013 and 39.9% in the period 1997 - 2006. This is an indication about the reduced number of perpetrators of tax evasion as crime that is mostly performed by this group and this is due to the improvement of the tax policy (tax cuts) and the increasing of the efficiency of tax controls and inspections. With the reducing of these criminal behaviors, it increases the supply of financial assets in the budget by paying the tax.
- The other economic crimes are less common, but it does not mean that they were not committed. Research results show that in most law enforcement agencies working on research of traditional economic crimes, the introduction of new crimes presents a difficulty, as they need a period of adjustment, and professional training focusing on identification of new crimes in their overall economic performance and in other areas where these works are performed.

REFERENCES

1. Арнаудовски Љ. , *Методолошки проблеми на статистичкото евидентирање и следење на економскиот криминалитет*, МРКПК, бр. 2 - 3, Скопје, 2008.
2. Арнаудовски Љ. , Нанев Л. и Николоска С., *„Економскиот криминалитет во РМ“,* Македонска ревија за кривично право и криминологија, бр. 1, Скопје, 2009.
3. Бановиќ Б., *Обезбеѓене доказа у криминалистичкој обради кривичних дела привредног криминалитета*, Београд – Земун, 2002.
4. Димитров Д., „ Економски деликти“, Скопје, 1998.
5. Камбовски В. , *Кривична одговорност на правните лица,* МРКПК, бр. 2-3, Скопје, 2008.
6. Кралев Т. , *Криминалистика – лексиконски курс*, Селектор, 2007.
7. Кривичен законик на РМ, Сл. весник на РМ, бр. 17/04.
8. Кривичен законик на РМ, Сл.весник на РМ бр. 114/09.
9. Николоска С., *Кривични дела против службената должност*, Графотранс, Скопје, 2008.
10. Цуклески Г. и Николоска С., Економска криминалистика, График Мак Принт, Скопје, 2008.

UDC: 343.9.02
316.624

SOCIOECONOMIC AND POLITICAL ASPECTS OF ORGANISED CRIME

Mile Petrovski[1]
Military Academy "General Mihailo Apostolski", Skopje
Radica Mitreva[2]
Barracks Goce Delchev "Centre for Electronic Reconnaissance", Skopje

Abstract: Organized crime today primarily for its obvious forms, the universal presence in almost all spheres of social life (social, economy, policy sphere, etc.) exceeds the boundaries of already known forms of national organized crime and it is commonly considered in connection with the international organized crime.

The basic requirements associated with international organized crime are: permanent association of more persons as joint profit-oriented community; organized structure which on the one hand, is characterized with the rigidity in the management, discipline of its members and care for their safety, and on the other hand, a network of delinquency with a loose style of management; linking of the legal with illegal activities in compliance with the particular needs of the population and criminal use of business and personal relationships; flexible crime technology and a wide variety of criminal methods (from exploitation, threats, blackmail, violence, forced protection, terror to active bribery and so on.), when the violence towards persons deviates in favour of pressure of any kind; conscious use of infrastructure (radio-telephone communications, communications and international transport) as well as internationality and mobility.

Today we are witnessing a change in the nature of transnational organized crime as a result primarily of the revolutionary changes in the field of technology, especially communication technology, globalization, increased intensity of exchange of goods internationally, the emergence of global terrorism and its affiliates which are closely linked to organized crime and sponsorship of some Islamic countries and the loss of national government control, in some of the countries of the world community, especially in the structure of the so-called " failed states". Certainly, the international organized crime is linked to drug trafficking and opiates originating from specific regions and local areas, with the transit of drugs to the end users which invariably includes a drug networks of customers, resellers, people who provide transportation of drugs and of course corruption of government officials (police, customs services, government representatives and others).

The power in non-state actors internationally, as a consequence of globalization, allows certain entities to convey the monopoly of power over the nation-state at the international level, while the area of free exchange of goods and services, globally, the latest discourse in developing organized international structures lies in the connection of these non-state actors with government representatives and other national leaders. Certainly, this also involves other types of international crime which implies an act of committing crime which has international repercussions on people, countries and the general state of peace in some national countries, region and the world peace involving crimes such as apartheid, crimes against humanity, against the peace, acts of aggression, genocide, kidnapping, hostage taking, piracy, slavery, torture, transnational crime and armed crimes. Such crimes are sanctioned by the UN Declaration on Human Rights in 1948, the Geneva Convention 1949 and other declarations and conventions.

The entire ranges of socially harmful activities which are defined as organized crime have an extreme devastating impact over the state of the democratization of societies. The inability of the state institutions to combat organized forms of organized crime that ultimately may have effect of compromising the viability of certain national communities and at the same time all this affect the situation of regional and global security as a whole should also be considered.

Building a proper competitive and viable strategy of the states to deal with all forms of organized crime often goes beyond the "sufficiency", or "rationality" in the use of institutional power thus exceeding the threshold of the use of deadly power of the conventional arms when combating the actors and protagonists in international organized crime.

Keywords: organized crime, state and non-state organized crime, national, regional and global security.

1 mile.petrovski@yahoo.com
2 mitreva_radica@yahoo.com

CONTEMPORARY THREATS AND ORGANIZED CRIME IN THE WORLD TODAY

Contemporary security threats in the world today are associated with threats and contradictions which threaten primarily the national security of the states' national communities, but also those threats which threaten regional security and world security and the overall security. These are the threats arising primarily from internal contradictions of states and national communities (class, economic, political, religious, etc.), but also threats such as globalization, asymmetric threats, global terrorism, global rebellion and pan rebellion, dangers arising from the spread of nuclear weapons and proliferation of dangerous radioactive materials, biological and chemical agents and of course international organized crime.

One of the most famous authors in the definition of organized crime Gunter Kaiser sets the basic conditions for the existence of the organized crime, including (Гинтер, 1996) [3]:

– Permanent association of more persons as joint profit-oriented community;
– Organizational structure which on the one hand, is characterized by rigidity in the management, discipline members, and concern for their safety, or on the other hand, a network of delinquency with loose style of management;
– Linking legal with illegal activities in compliance with the particular needs of the population and criminal use of business and personal relationships;
– Flexible crime technology and a wide variety of criminal methods (from exploitation, threats, blackmail, violence, forced protection, terror to active bribery and so on), with violence towards individuals which differs in favour of pressure of any kind;
– Conscious use of infrastructure (radio-telephone communications, communications and international transport) and
– Internationality and mobility.

Some analysts of organized crime, such as for example the Italian sociologist Letizia Paoli, reckon that the modern trends of organized crime are in contradiction with the organization of large hierarchical structures such as the Sicilian Mafia, the Japanese Yakuza and Chinese Triads (Letizia, 2002).[4] She believes that these organizations rely on social relations rather than on market dynamics and are no longer efficient structures upon which organized crime is based.

Among many characteristics of organized crime can be found in the reports of U.S. government and European task forces, committees, commissions, and variety of organizations. These attributes include the following:

– It has non-ideological motives;
– It exhibits continuity over long periods of time, is perpetual in nature;
– It uses tactical and strategic or long-term planning to reach the goals of organized crime;
– It is governed by rules and codes of secrecy;
– It seeks to monopolize products and services;
– It has an organized hierarchy;
– It uses force and intimidation;
– It restricts membership;
– It provides illegal goods and services as demanded by the public;
– It obtains enormous profits by criminal means;
– It employs corruption for immunity and control;
– It creates a division of labour with job specialization;
– It engages in money laundering;
– It invests profits in legal enterprises and seeks these businesses;
– It exhibits an ability to adapt to changes in supply and demand, law enforcement, and competition;
– It operates internationally;
– It engages in more than one illicit activity (diversity in business), and
– It uses legal businesses as fronts for illegal activity.

3 Кајзер Гинтер, (1996), *Криминологија*, Александрија, Скопје стр. 193
4 Paoli Letizia ,*The Paradoxes of Organized Crime*, (2002), Vol.37, No-1,p.g..51,

The term 'organized crime' today is not precisely defined, primarily because of its forms, universal presence in almost all spheres of social life (politics, economy, social sphere, etc.), and of course, crossing the national borders, i.e. the situation in which the national organized crime mostly is related to the international organized crime.

CHANGED NATURE OF ORGANIZED CRIME

Today we are witnessing that a change in the nature of transnational organized crime is the result primarily of revolutionary changes in the field of technology, especially communication technology, globalization, increased intensity of exchange of goods internationally, the emergence of global terrorism and its affiliates that are closely linked to organized crime and sponsorship of some Islamic countries and the loss of national government control in one of the countries of the world community, especially in the so-called structure of "failed states". Sure international organized crime is linked to drug trafficking and opiates originating from specific regions and local areas, transit of drugs to end users which invariably includes a drug networks of customers, resellers, people who provide transportation of drugs and of course corruption of government officials (police, customs services, government representatives and others).

It is important to point out that the change in power in non-state actors at the international level has been a result of globalization which allows certain entities to transfer the monopoly power of the nation-state at the international level, while the part of free exchange of goods and services globally is in the connection of these non-state actors with government and other officials in the nation states (in the evasion of goods and services, non-payment of taxes, transit of goods that are not branded and cleared, etc.).

In terms of the types of international organized crime, these include the crimes such as apartheid, crimes against humanity, against peace, acts of aggression, genocide, kidnapping, hostage taking, piracy, slavery, torture, transnational crime and armed crimes. Such crimes are sanctioned by the UN Declaration on Human Rights in 1948, the Geneva Convention 1949 and other declarations and conventions.[5]

In this, it is important to pull relationship that today means the presence of links between organized crime and international terrorist organizations, whose embodiment is Al Qaeda as a global terrorist network. In particular, this terrorist organization broke the classic terrorist network and its activities are recognizable. This terrorist organization acts out of the national-state framework, has set global agenda of engagement and has developed transnational ideology based on radical Islam (holy Jihad).

Key nodes where there is suitable opportunity for interaction between organized crime and terrorist organizations today are located in regions, areas or countries that are faced with endemic corruption, conflict or post-conflict zones and areas where the rule of law has yet to be established, further border regions, free trade zones and urban and slum areas where there are violence, crime and lawlessness. Particularly suitable transmitter of these links today occurs in the exploitation of cyberspace, and the open social networks.

The whole range of socially harmful activities which are defined as organized crime have extremely devastating impact on the condition of the democratization of societies, organized state institutions where "in such a situation the realm of fear tactics, vice, poverty is a serious danger to the freedom of citizens and human rights and all negative phenomena of that society lead to hazardous invisible abyss" (Котовчевски, 2009).[6] This is all the more important to know considering the ultimate ability of organized crime to adapt to new social and political developments in the country, with serious threats to its national security and stability.

International organized crime had especially negative impact on the post-communist societies, which came to the so-called privatization of state or socially owned capital. This process, although there was a legal basis and all institutional procedures were implemented, was associated with dirty money laundering, corruption, extortion, preparation (for financial compensation) of unreal, very low estimates of the facilities targeted for privatization. In fact, almost all post-communist countries have played identical privatization scenario which happened in a shameful process of conquest (robbery) of the national wealth with seemingly legitimate means of the structures of organized crime to ruthlessly destitute the state, citizens and criminalized the society. In these conditions the economic and political stability in the country is endangered by extremely dangerous condition of the rule of organized criminal structures that rule the society as a whole.

The most important link in organized crime is a criminal group, which according to the UN Convention consists of three or more members organized for a period before and after the action, which take coordinated measures to perform serious crime in order to achieve financial or other benefit. When it comes to Mafia, its specific forms of criminal groups that sell private property are sometimes associated with govern-

5 http://www.boredofstudies.org/wiki/index.php?title=Types_of_International_Crime_%26_Sources_of_Law_for_International_Crimes&printable=yes,датум на пристапување,06.03.2012

6 Митко Котовчевски, *„Војникот носител на мирот"*,Годишен зборник,УКИМ 2009, УДК: 349.9.02(100), стр. 409

ment representatives and agencies and often take quasi government role in the society. Examples are the US mafia, Cosa Nostra Sicilian Mafia and the Japanese Jacuzzi. Certain criminal groups are engaged in international business, operating with one or more cross-border areas with the purpose of making a higher profit.

The biggest and also the most extreme engagement of organized crime and criminal groups are accomplished in the area of so-called illegal political economy, the Big Three of drug trafficking and weapons in money laundering and corruption and illegal activities in the sequence in which the engagement shown by organized criminal groups which are related to the dark side of globalization.

Illegal political economy is actually associated with international organized criminal activities beyond the borders of one state. It is estimated that such criminal activities participate from 0.5 to 20% of the gross domestic product of some countries annually, making this illegal political economy an important source of global revenue. Such activities are still connected with money laundering and spread of political corruption.

Drug trafficking, weapons and people are the most dominant and appear in the network diagram of organized crime, in the longer term This situation gained momentum especially after the collapse of the former socialist countries, communities and the end of the Cold War. Besides market drugs from natural sources and plants (heroin, cannabis, opium and cocaine), the world's today is growing consumption of synthetic drugs. Assessing the market for synthetic drugs UN in its report of 2004 determined that this year were produced 480 tons of synthetic drugs. The trafficking with drugs, weapons and people is concentrated in three regional markets, with a significant correlation between them, creating significant diffusion between them. In East Asia synthetic drugs from China, Taiwan, Myanmar and the Philippines carry the markets of Thailand, Japan, Australia, New Zealand, Europe and North America. In North America, the United States produces large amounts of synthetic drugs for domestic consumers and supplement market in Mexico. The main manufacturing centres in the Netherlands, Poland, Belgium, Lithuania, Bulgaria, Germany are supplying the European market.

In a sea of goods with entrepreneurial spirit there is often part of international organized crime. As can be seen from the diagram below (Figure 1) the first place in this huge diagram of goods is still taken by clothing, then electronic equipment, computer equipment and tools and equipment for the consumer. In the last 10 years the significant place belongs to the smuggling of cars from Western European countries to Eastern Europe and the Balkans. Europol estimates that over 700,000 vehicles are part of smuggling, theft, illegal sales and other schemes of organized crime.

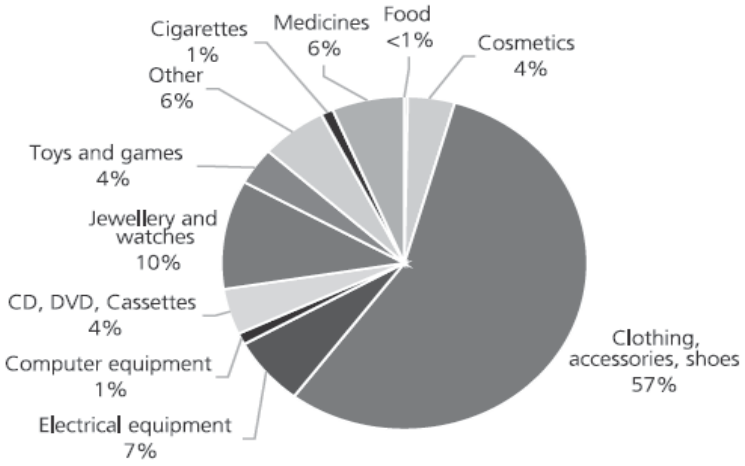


Figure 1 *Counterfeit seizures made at the European borders by product type (number of incidents) 2008 (UNODC, 2010)*

An important type of organized crime from the position of abuse of power, conventional and especially nuclear weapons is the arms trade and trade (smuggling) of nuclear materials. This criminal activity is one of the most profitable businesses in the international organized crime, with extreme danger to international stability. These weapons and radioactive material originate from uncontrolled landfill of decomposing states and communities (as for example the former Soviet Union or the Republic of Albania) or are part of international organized crime, global terrorist networks such as al-Qaeda.

As a current phenomenon that is associated with global terrorism and international organized crime is the proliferation of dangerous nuclear materials (hazardous depleted uranium which remains as waste material in reactors producing electricity). This depleted uranium through a technological process is the main raw material for the production of nuclear weapons, which according to the capacity are sufficient to

destroy the entire city neighbourhoods, important and critical infrastructure and other facilities. There are also incidents of these dangerous radioactive materials, but also frequent accidents in nuclear reactors of older generation (see the hext table).

It is necessary also to emphasize the danger of the possibility of terrorists' threats and attacks by means of transportation of toxic industrial chemicals, which are necessary for the maintenance of the modern lifestyle.

Particularly significant are the efforts of some countries to supply enriched uranium that could produce nuclear weapons (Iran) or substantially increase the operational capabilities of their armed forces (Korea and other countries).

Countries involved in incidents with proliferation of nuclear materials and organized crime suspects in the period from 2001 to 2010 year (Zaitseva, 2007)[7]

State Number of Number of included	Incidents	Countries
Ukraine	9	33
Russian Federation	7	38
Georgia	5	15
Belarus	3	27
Kazakhstan	2	2
India	2	4
Tajikistan	2	6
Bulgaria	1	3
Congo	1	1
France	1	1
Kenya	1	3
Namibia	1	3
Portugal	1	4
South Africa	1	5
Tanzania	1	4
Thailand	1	7
Turkey	1	2
Uzbekistan	-	3
Cameroon	-	2
Armenia	-	1
Ethiopia	-	1
Moldova	-	1

The smuggling of migrants is a truly global concern, with a large number of countries affected by it as origin, transit or destination points. Profit-seeking criminals smuggle migrants across borders and between continents. Assessing the real size of this crime is a complex matter, owing to its underground nature and the difficulty of identifying when irregular migration is being facilitated by smugglers. Smugglers take advantage of the large number of migrants willing to take risks in search of a better life when they cannot access legal channels.

It is estimated that just under one third of all immigrants in the United States of America are there illegally, with about 80 % of the illegal immigrant population in the country originating in South America (as well as Mexico). Of all illegal immigrants in the United States, an estimated 25-40 % entered the country on a legal visa and then overstayed, and the remainder entered the country clandestinely. Of the latter group, 97 % entered the United States clandestinely through that country's border with Mexico; coastal areas comprised less than 1 % of the total. While not all illegal immigrants are smuggled, these figures do provide an indication of the extent of the situation.

7 Organized Crime, Terrorism and Nuclear Trafficking Strategic Insights, Volume VI, Issue 5 (August 2007) by Lyudmila Zaitseva,pg 4

Each year, some 55,000 migrants are thought to be smuggled from East, North and West Africa into Europe, generating about $150 million in revenue for criminals. While the number of migrants smuggled from Africa into Europe is far lower than the number smuggled from South America and Central America into North America, the conditions are no better: long desert routes and treacherous sea crossings. While figures on fatalities can be difficult to ascertain, media reports indicate that between 1996 and 2011, at least 1,691 people died while attempting to cross the Sahara and that in 2008 alone, 1,000 deaths occurred during sea crossing of migration.

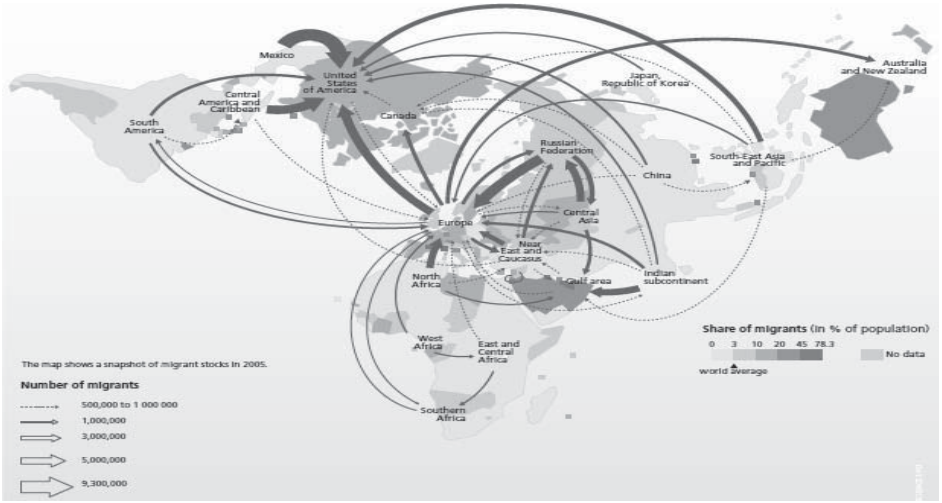


Figure 2 *Main migration flows 2005*

(Sources: Marie-Françoise Durand, Philippe Copinschi, Benoît Martin, Delphine Placidi, Atlas de la mondialisation, Paris, Presses de Sciences Po, 2009 Development Research Centre on Migration, Globalisation and Poverty, Global Migrant Origin Database Updated March 2007, Washington (D. C.),Banque mondiale et Brighton, Université du Sussex) www.migrationdrc.org

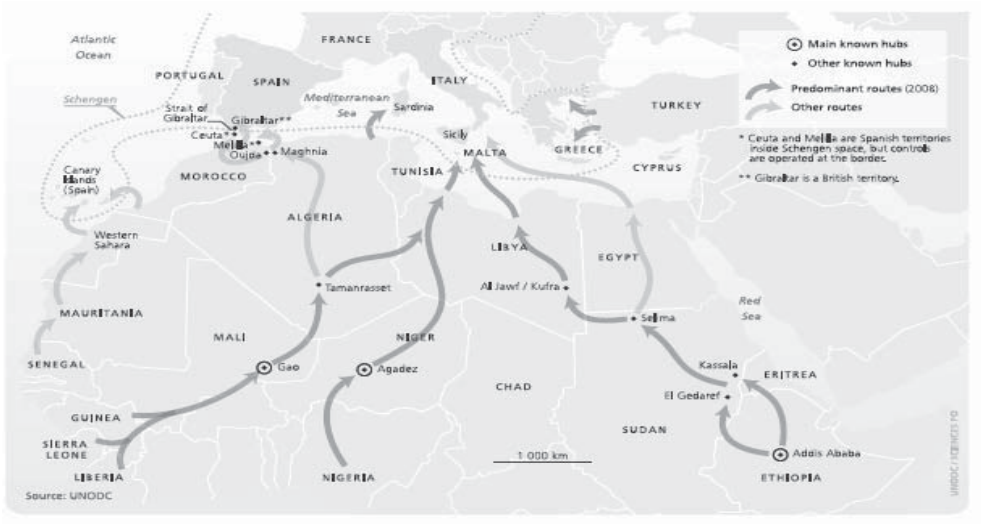
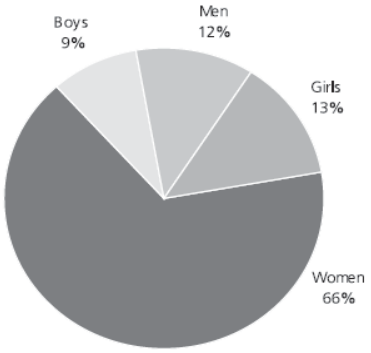


Figure 3 *Main routes for African irregular migrants to Europe, 1999-2008*

The exploitation of human beings can be highly lucrative for organized criminal groups. Although figures vary, an estimate from the International Labour Organization (ILO) in 2005 indicated that about 2.4 million people are victims of trafficking at any given time, and that profits from trafficking are about $32 billion per year. Human trafficking is one of the most lucrative illicit businesses in Europe, with criminal groups making about $3 billion from it per year, making it a considerable criminal business that preys on

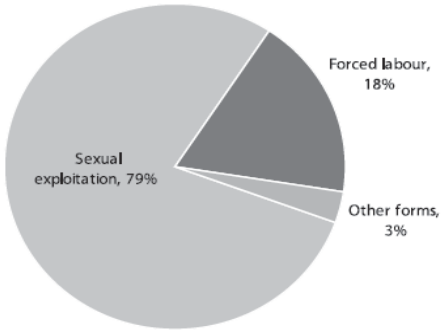
the world's most marginalized persons. Human traffickers regard people as commodities; items that can be exploited and traded for profit (Figure 4). In Europe, most convicted traffickers are male, though female offenders are overrepresented when compared to other crimes, as some gangs consider women to be more effective in entrapping victims by gaining their trust (Crime, 2009).



Source: UNODC/UN.GIFT

Figure 4 *Profile of victims identified by State authorities in 61 countries, 2006 (UNODC, The Globalization of Crime, 2010)*

In 2005, ILO estimated that globally there are around 2.4 million victims of human trafficking at any given time. Recent research on overall forced labour trends however would suggest that the scope of the problem is much bigger. In Europe, over 140,000 victims are trapped in a situation of violence and degradation for sexual exploitation and up to one in seven sex workers in the region may have been enslaved into prostitution through trafficking (Figure 5). Victims are generally misled or forced by organized criminal networks into a situation of abuse from which it is difficult to escape; they might be beaten or raped or their families might be threatened if they try to get away. Victims' passports are often seized by the traffickers, leaving them with no form of identification. In cases where they have been trafficked between countries, victims often have little or no knowledge of the local language. Nearly every country in the world is affected by human trafficking, as a point of origin, transit or destination, and victims from at least 127 countries have been reported to have been exploited in 137 States. Human trafficking is a regional as well as a domestic crime, with victims trafficked within their own country, to neighbouring countries and between continents (Organization, 2012).



Source: UNODC/UN.GIFT

Figure 5 *Distribution of victims identified by State authorities according to the form of exploitation, 2006 (UNODC, The Globalization of Crime, 2010)*

The strategy of the use of military force to combat the activities of organized crime into their bases usually sets in a joint performance that includes asymmetric and unconventional threats, particularly global terrorism, and other security threats.

The global, military forces, especially those of the leading political-military alliances (as NATO), have the focus in the fight against international organized crime, put the control of the corridors of arms trafficking and trade (smuggling) with dangerous radioactive materials (for example today it is the area of the Middle East and the Korean Peninsula).

In this, it is always the question of the legitimacy of the use of an armed force, further the level of use of force that is the danger of exceeding the threshold of the use of deadly power of conventional weapons in conflict with holders and promoters of international organized crime.

CONCLUSION

Organised crime, especially transnational organized crime affects the safety in three ways and therefore needs multilayered approach to its explanation. Internationally, organized crime undermines norms and institutions, which are crucial for maintaining the international system. Nationwide international organized crime can destabilize internal cohesion, to derogate from internal economy and disrupt the social climate in the country. This condition is associated with the so called human security.

International organized crime undermines the safety of man as an individual in society. Criminal ventures affect the health. For example, the regions along the path of drug smuggling have seen unprecedented growth of drug addicts among the population. Sex tourism increases the rate of drug addiction and HIV infections. Arms smuggling deepens and prolongs the conflict in certain crises. Revenge with bloody consequences among certain groups, families and tribal communities has been growing. But the biggest problem is the so-called chain diagram of criminal activity mutual support or derived from one another. For example, smuggling cars from Western Europe increased the rate of theft, money laundering and other criminal activities related to the exchange of goods and goods.

REFERENCES

1. *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (United Nations publication, Sales No. E.10.IV.6). Available from www.unodc.org/documents/data-and-analysis/tocta/TOCTA_ Report_2010_low_res.pdf.
2. International Labour Organization, *A Global Alliance against ForcedLabour: Global Report under the Follow-up to the ILO Declarationon Fundamental Principles and Rights at Work* (Geneva, ILO, 2005). Available from www.ilo.org/wcmsp5/groups/public/@ed_norm/@ declaration/documents/publication/wcms_081882.pdf.
3. International Labour Organization, *Global Estimate of Forced Labour 2012: Results and Methodology* (Geneva, ILO, 2012). Available from http://www.ilo.org/sapfl/Informationresources/ILOPublications/WCMS_182004/lang--en/index.htm
4. United Nations Office on Drugs and Crime, *Global Report on Traffickingin Persons* (February 2009). Available from www.unodc.org/unodc/en/ human-trafficking/global-report-on-trafficking-in-persons.html.
5. *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. 11 *Global Report on Trafficking in Persons.*
6. *UNODC: The Globalization of Crime: A Transnational Organized Crime Threat Assessment (2010),*
7. Report of the Secretary-General on the work of the Organization, Official Record of the fifty-fifth session of the General Ammembly, Supplement No.1 (A/55/1) of 30, August 2000
8. SIPRI (Stocholm Internacional Peace Reaserch Institute), Yearbook 2012, Armament, Disarmanents and international security.
9. Security Stdies for the 21 th Century, by Sylttz H. Richard, Godson Roy, Quester H. George Dulles.
10. Митко Котовчевски, „Војникот носител на мирот“,Годишен зборник,УКИМ 2009, УДК: 349.9.02(100),
11. Lyudmila Zaitseva, Organized Crime, Terrorism and Nuclear Trafficking Strategic Insights, Volume VI, Issue 5 (August 2007),

UDC: 343.352:351.74/.75

CORRUPTION IN THE BODIES OF INTERNAL AFFAIRS AS THE SOCIAL LEGAL PHENOMENON

Roman Kisil
Lviv State University of Internal Affairs, Department of Administrative-Legal Sciences

Abstract: An attempt to analyze concrete problems and formulate some suggestions which are directed at providing a new level of warning of corruption and bribery among the personnel of organs of internal affairs is done in the article.

Keywords: a crime, bribery, corruption, counteraction, militia, organs of internal affairs, law enforcement authorities, subsections of internal safety, latent crimes.

BASIS OF THE PROBLEM

According to statistics from the Ukrainian Ministry of Internal Affair's Security Service in recent years, the level of crime among police officers remains at the high level. The prevention and detection of crimes and corruption acts among personnel still do not meet modern needs.

Consequently, one of the functional priorities of the competent state bodies and state generally is improving the system of effective measures to prevent corruption and bribery among law-enforcement personnel.

REVIEW OF RECENT RESEARCHES AND PUBLICATIONS

Specific issues of prevention of crimes of corruption and bribery, including those, that may possibly be committed in law-enforcement agencies, reported in the researches of following domestic and foreign scientists: B. Averyanov, L. Arkusha, L. Bagriy-Shakhmatov, O. Bandurka, B. Volzhenkin, O. Dzhuzha, O. Dulskuj, A. Dolgova, A. Gapon, A. Gida, V. Zakharov, M. Kamlyk, P. Heha, A. Kelman, Y. Kondratiev, M. Kornienko, A. Kurakin, O. Negodchenko, Y. Orlov, V. Ortynsky, A. Prokhorenko, A. Selivanov, L. Skalozub, V. Sushchenko, A. Tereshchuk, S. Shalhunova, V. Yusupov and other scientists.

Goals and objectives of the research - development of the effective anticorruption system in the bodies of internal affairs to minimize the problem of corruption and bribery among its officers.

THE PRESENTATION OF THE ARTICLE'S ESSENTIALS

In the recent years quite a lot was done in the realm of anti-corruption and bribery procedures in the internal affairs. However, we must confess that it gave no real positive results.

Improving the effectiveness of anti-corruption and bribery measures requires solving a number of political, legal and institutional problems. One should bear in mind that there are number of conditions that neutralize their integration as well as following realization. These conditions include: the absence of an effective corruption-prevention system, the complexity of exposing these acts and the high latency of such law-offenses.

A necessary condition of a successful fight against corruption and bribery among the officers of the Internal affairs is the complex research of the possible directions of the police staff activity where the offenses with signs of corruption may occur combined with the permanent creation of appropriate conditions of service, career prospects, improvement of the prestige of service as well as guarantees their social security basics [1, p. 6].

According to specialists, who are researching this problem, at the actual level of social evolution, total elimination of corruption and bribery is compared with the "so-called Utopia", because of that this task cannot be accomplished to the end, due to the high latency and material expenses of this process. After all, for their complete elimination society has to spend a great effort in the spheres of economic, politic and organ-

izational restructuration. Therefore, our task at least consists of minimization of the named phenomenon [4, p. 115], making corruption and bribery in the future economically viable.

Considering the facts given above, it is obvious that without the implementation of the science-based reforms in the system of law enforcement agencies functioning we cannot speak about tangible results in combating corruption and bribery as the integrative problems of modern society.

Thus, the fight against corruption should be based on a combination of preventive and legal repressive measures. But, nevertheless, priority should be given to preventive measures of general social and special criminological directions. Therefore, the main goal of public policy in the sphere of struggling against corruption and bribery should be a creation of an appropriate system of prevention and response, identify and overcome social preconditions and effects of those phenomena [2].

During quite a long time in many scientific publications it was suggested that certain social phenomena such as the level of criminal activity and the number of law offenses (felonies, misdemeanors and non-criminal acts of illegal behavior), the fact of corruption in the state apparatus are primarily determined by economic problems. However, foreign studies represented absolutely different tendency: the more economically developed country is (such as USA, Germany, United Kingdom etc.), the higher level of corruption is registered within the law-enforcing institutes of that country (the so called "corruption paradox"). To reduce the level of corruption in these states a set of typical identification and preventive measures are used.

For example, in the UK autonomous anti-corruption units were formed within which specialized appropriate services were established, combined with simultaneous practical measures and anticorruption procedures of their functioning development. These procedures include covert electronic surveillance, usage of "informant's institute", encouraging informants from among the criminals into giving hits against corrupted police officers, as well as special operations and inspections of the staff in susceptibility to corruption.

It is noteworthy that the London Metropolitan Police was able to modernize the "archaic strategy of a simple investigation to modern, highly-effective prevention measures in the realm of resolving corruption problem." This strategy includes three following major components. Firstly it consists of testing the candidates for police. Considering that the requirements to the potential officer are really high, necessity of the special preliminary-qualification service emergence was notified and practically realized because it is one of the decisive factors that reduce corruption. Secondly, it is mechanisms, used to ensure information security. Strategy of limited access to information in general and division of levels of such access is seen as a very important component of security that should also be applied to the civilian police. Thirdly, it is a system of methods that are related with the ethical dimension. British experts believe that the need of permanent monitoring of both each staff member and police unit as a whole ethics status is also a fundamental way of preventing bribery in the police service. In this purpose it is necessary to organize regular trainings to enforce employees with strong ethical postulates [3, p. 143].

The recent experience of Georgia and Russia represents the importance of multidimensional reformation processes that are held in the systems of internal affairs of named countries. Thus, combining the positive aspects of international experience in combating corruption offenses is the optimal way of designing and implementation of efficient measures aimed at eliminating the causes which impel local law-enforcement institutions to abuse the legal regulations and delinquency.

In this direction, it is necessary to review the system that is used for officers to a police service professional selection; to pay greater attention for official duties realization, discipline and legality in the police system, as well as to the process of practical realization of statutes regulations; promptly and professionally respond to complaints and other signals about the cases of illegal actions of law-enforcement personnel; to coherent the mechanism of legal response of those officers who commit law-offences.

Also, it is necessary to mention that there are three main practical approaches to the problem of reducing corruption in Ukraine resolving. Firstly, we can strengthen the laws and their implementation simultaneously increasing the risk of punishment. Secondly, we can create economic mechanisms that allow officers to increase their income without breaking rules and regulations. Thirdly, we can enhance the role of markets and fair competition which will reduce the size of the potential profit from corruption. The last but not least way is also connected with legal competition enforcement in the context of provision of the public services provided by duplication of jurisdiction among government agencies.

Yet the main obstacle of bribery and other sordid offenses prevention among officers of internal affairs should be an appropriate level of social protection of young professionals and their families, first-rate medical insurance, free state loans to buy estate property, higher pensions – every factor that is tantamount to raise of wages and thus increases loss of employee in case he's being caught on corruption activity [8].

Also, the importance of public control over the activities of anti-corruption bodies whose main duty is to combat corruption and bribery is rising, gaining its rightful place in the system of resistance to this destructive social phenomenon. Political parties and public associations, the media and freedom of speech, representative bodies and individuals should play a special role in this process. Forms and methods of such

activities, as well as imperative response of relevant state authorities in investigating reports of corruption and bribery should be clearly defined in the law [5, p. 170-171].

However, the modern fundamental key issue in law-enforcement is the outflow of highly-experienced personnel into the private sphere. This situation is characterized, above all, by the fact that a significant number of young professionals who came to work at the police after graduation from the higher specialized educational institutions discharge from the internal affairs system under certain circumstances, and having a law degree (specialty - "Law ") can work both in public and in private legal enterprises, institutions and organizations. We believe that providing an education for the state police officers in the specialty of "Law" is inappropriate. In this case, it would be more rational to focus on specialized education in higher educational institutions to prepare professionals to work strictly in law enforcement system under specialty - "Law enforcement".

Those measures are also explained by that fact that knowledge, for example in the field of specialized investigation activities that students have gained in institutes of internal affairs system can be used for example to provide legal consulting of criminal contingent. Also, according to the court statistics information, persons who are discharged from the police, mostly citizens of 35 years, most likely commit crimes, because of practical skills, gained during professional activity and different opportunities help to circumvent the law and to avoid legal responsibility.

Among the organizational and management preventive measures priority is still preserved by the functions concerning recruitment, training and placement, improvement of personnel education methods. As part of the value-oriented approach in the selection of personnel, the departmental instructions provide an illustrative list of ethical, business and personal qualities which are necessary for each employee and are based on medical and psychological criteria that prevent the penetration of the persons who are unable to work in the police.

In our opinion, another important aspect of legitimacy improvement is the service in law enforcement agencies on a contract basis. This possibility is provided by the Law of Ukraine "On Police" (art. 17), norms of which, unfortunately is not always rationally used. It is commonly known that the contract is a special form of employment deal concluded by the parties in written form for a specified period or at the time of specified task accomplishment [6, p. 114].

Main feature of the contract (unlike regular employment deal) is it a mandatory written form. According to the law, this contract is concluded in two examples with the same legal force that is stored by each party. Only after signing a contract is the order about employment produced. This order is the basis for writing in the data about the employment fact into the workbook.

The second feature of the contract - is its periodical characteristic that is the contract is concluded for a definite term or for a specified task accomplishment legal fixation of which is the basic imperative obstacle of its validity.

The period of contract is not limited by the law and depends on the mutual consent of the parties. In practice, most contracts are concluded for a period of 3 to 5 years [9, p. 132].

So, for more effective and productive functioning, it is necessary for the law enforcement officers to settle a contract with the structural subdivision of internal affairs where the very service will be held. This need arises from several reasons. Firstly, an employee who graduated from special higher educational institution of the Ministry of Internal Affairs of Ukraine and already concluded the contract, must comply with the requirements that are provided by this act, because in the case of violation of named regulations or premature termination person will suffer legal responsibility, including financial. This feature also applies to the other party of the contract, whose task is to provide law enforcement officers with everything necessary for the proper performance of their duties. Secondly, if the employee does not perform their duties in the right, appropriate way, after the expiration of the contract period a structural unit of internal affairs represented by the chief officer that personalizes the employer according to the contract, has the right not to prolong the period of contract with that officer. In this case, the employee may be dismissed from the service. Because of the previously-named facts this form of service in law enforcement agencies will ensure proper selection of personnel to carry out their tasks and fulfill their law-enforcement duties.

Developing of ethical principles in the functioning of the bodies of internal affairs is no less important than solving logistical, human and social issues of their operation, as the quality of the tasks accomplished by those structures, is primarily indicated by the mental features of law-enforcement service staff.

Active cooperation of the Internal Affairs of Ukraine with the public institutions and non-governmental organizations, on the one hand, produce the social perception of police image as an open organization that enhances the credibility, and also prevents the process of professional deformation of law enforcement officers, reducing the level of commercialism and cynicism [7].

Thus, to counter corruption, bribery and other offenses in the system of Internal Affairs it is highly important to develop a new and to improve already existing methods and techniques that have become the fundamental in the realm of law-enforcement activity legitimation.

CONCLUSIONS

In summary it can be suggested that in order to combat corruption and bribery among police officers it is strictly needed to relevant legislation to reform the police. First of all, it concerns the proper recruitment and training of future specialists and introduction of the contract service in the system of internal affairs that should be the driving force for the procedure of selection of such personnel, whose credo is fighting against crimes.

Yet, without adequate social protection, decent wages and providing structural units with everything necessary for a proper accomplishment of their heavy duties, it is impossible to reorganize the law enforcement bodies into the effective, non-corrupted social institution.

REFERENCES

1. Стеценко С. Г. Корупція в органах внутрішніх справ: проблеми протидії : монографія / С. Г. Стеценко, О. В. Ткаченко. - К. : Алерта, КНТ, Центр учбової літератури, 2008. - 168 с.
2. Концепція боротьби з корупцією на 1998-2005 роки / затв. Указом Президента України : від 24.04.1998 р., № 367/ 98.
3. Куліш А. М. Досвід боротьби з корупцією в поліції Великої Британії /
4. М. Куліш // Право України. - 2005. - № 12. - С. 141-145.
5. Кісіль З. Р. Корупція в органах внутрішніх справ: проблеми протидії / З. Р. Кісіль // Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична : зб. наук. праць / головний ред. В. Л. Ортинський. - Львів : ЛьвДУВС, 2009. - Вип.2. - С. 109-117.
6. Борисов В. Громадське суспільство та питання подолання корупції /
7. Борисов, О. Кальман // Вісник Академії правових наук. - № 2. - 2005. - 168-173.
8. Науково-практичний коментар до Закону України «Про міліцію». - К. : Укр. акад. внутр. справ. 1996. - 144 с.
9. Мартиненко О. А. Злочини серед працівників ОВС України:їх
10. детермінація та попередження: дис. ... доктора юрид. наук : 12.00.08 / О. А. Мартиненко ; Харків. нац. ун-т внутр. справ. - Х., 2007. - 434 с.
11. Васильев В. Л. Юридическая психология / Васильев В. Л. – [3-е изд.]. – СПб. : Питер, 2000. – 624 с.
12. Науково-практичний коментар до законодавства України про працю / В. Г. Ротань, І. В. Зуб, О. Є. Сонін, - 10-те вид., допов. і переробл. - К. : Юрид. книга ; Севастополь : Ін-т юрид. дослідж., 2009. - 944 с.

UDC: 343.71:621.316

CRIMINAL ANALYSIS OF ELECTRICITY THEFT AND ITS SOCIAL CONSEQUENCES[1]

Sasa Markovic[2]
Valjevo Police Department

Abstract: Electricity theft by individuals and legal entities (corporations) is becoming more frequent phenomenon, because of inefficient public system and unclearly defined legal system, in which electricity is protected object. Electricity in our country is produced and transmitted to the end users by public state-owned corporations. The system for controlling electricity sale and delivery is extremely inefficient. Laws and bylaws which regulate this area are outdated and, as such, give plenty of opportunity to the end users and to employees in the public corporations, involved in this process, to make different kinds of abuse and criminal acts. These criminal activities are difficult to prove in court proceedings, and the financial damage for the state is substantial. In the last few years, Electricity Distribution Company of Serbia has started installing, the so-called, 'smart' electricity meter, and particularly on large, typically commercial, consumers. The meters are protected with verification mark, performed by authorized control bodies, and the electricity distribution company mark. Consumption of electricity and registered events, such as opening the cover of the meter which is sealed with an appropriate mark, are read by computers. Although electricity theft is estimated in millions of RSD each year, for every commercial user in particular, proving this criminal act, in a legal court process, is very difficult, practically impossible.

The paper presents the ways this criminal act of electricity theft is performed, by the commercial users - large consumers, on the territory of the police department of Valjevo. Additionally, the paper also deals with the treatment of public prosecutors and police during the clarification of criminal acts and success in proving them in the juridical processes. The author especially puts en emphasis on a legal and sublegal act, which regulate this area in the criminal justice matter.

Keywords: electricity theft, fraud, legal subjects, police force, public prosecution, criminal proceedings.

INTRODUCTION

Serbia produces near 31 billion kWh yearly, but at the same time, loses up to 19.5% from the whole amount of produced electric energy.[3] In regular business activities, The Public Corporation for Electric Power of Serbia (in the text below EPS) has made significant technical and non-technical losses of electrical energy. Technical losses appear in transmission, distribution and transformation of electricity. Non-technical losses represent the amount of electricity consumed by consumers that EPS is not able to identify and charge.[4]

The mentioned non-technical losses include: consumption of electricity by illegally connected consumers; manipulation in the electricity meter enclosure; measuring errors in meter itself, mostly because different kinds of abuse (inhibitions, various bridging, 'management' balances).[5]

The EPS management total losses are estimated at around 100 million Euros of which more than 60 million Euros have been caused by theft.[6]

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.
2 sasamarkovic975@gmail.com
3 "Procena Elektroprivrede Srbije"- the study done for the Serbian Government by Deloitte&Touche in the autumn of 2001
4 Banović, B.; Lajić, O.; Milošević, M.; "Krađa električne energije, kao pojavni oblik krivičnog dela krađe", Bezbednost 1-2/2008, p. 130
5 Ibid: str. 132
6 Energetika rs.com ,08.04.2010

CRIMINAL AND SOCIAL ASPECT OF THE PHENOMENON OF THEFT OF ELECTRICITY

Electricity theft is one of the most common criminal offenses committed on the territory of our state.[7] In this paper the term "electricity theft" refers to a basic criminal act of theft and also to all criminal acts from the field of offenses against property, if they are aimed at obtaining electricity illegally. That will be done regardless the fact that the Criminal Law of the Republic of Serbia[8], in the part of offenses against property, defines several legal clauses, which in a specific way define various forms of theft of other moveable properties, or obtaining illegal material benefit, depending on the values and ways of execution, number of offenders, use of force, threat, bringing and maintaining others in fallacy, etc.[9] The part of the Criminal Law dealing with moveable property defines it as any energy produced or collected to provide light, heat or movement, a telephone impulse, as well as computer data or computer program. If the measuring instrument – electricity meter has been modified in a way to lower the meter reading, the question is whether that is a criminal act of theft or of fraud. Before removing the cover of the meter for making modifications inside it (criminal act "The destruction and damage of public devices"), the damage has to be done to the verification and / or distribution mark or seal (criminal act "Removing or violation of the official seal or mark"). Therefore, we can conclude that a criminal act of fraud is committed together with several other criminal offenses. Without going into the details of the criminal law and criminal procedural aspects of every criminal act of illegally obtaining electricity, the author uses the term electricity theft in the paper.

But if we consider the most modern 'smart' digital multifunctional meters- meters are equipped with computer systems, and that the theft of electricity is done with modifications inside the meter, in order to make the meter processor measure lower electricity consumption, these acts can be referred to as the criminal offenses with elements of cyber crime.

The criminal offenses of cyber crime, with the exception of the crimes charged in the group against the security of computer data, in terms of the Law of the competence and organization of the state authorities to fight against cyber crime, include: • offenses against intellectual property, assets, economy business and legal transactions in which computers, computer networks, computer data are objects or instruments of execution, as well as their products in a material or electronic form if more than 2,000 copies (with copyrights) are involved or if the material damage exceeds 1,000,000 RSD; • offenses against freedom and rights of citizens, sexual freedom, public order and the Constitution of the Republic of Serbia in which cases, due to the method of execution or instruments used for execution, we can conclude that those are acts of cyber crime.[10]

Both individuals and legal entities can be prosecuted and convicted of electricity theft. In fact, legal proceedings can be conducted against an individual on the basis of reasonable doubt that he has committed a criminal act of electricity theft according to the Criminal Proceedings Law[11] and for offenses defined in the Criminal Law. For legal entities "Zakon o odgovornosti pravnih lica za krivična dela"[12](Law on liability of legal persons for offenses) defines conditions of responsibility of legal entities for criminal offenses, criminal sanctions that may be imposed on legal entities and rules of procedure for deciding on the liability of legal entities, imposing criminal sanctions, decisions on rehabilitation, termination of security measures or legal consequences of the conviction and execution of court decisions.[13] Passing the Law on liability of legal persons for offenses (Zakon o odgovornosti pravnih lica za krivična dela) in 2008, the National Assembly of Serbia adopted the viewpoint expressed in our legal theory of the necessity of introducing the responsibility of legal entities for criminal offenses in the criminal legal system of Serbia. Additionally, the view presented in legal theory that the establishment of such responsibility can be and should be, primarily for criminal and political reasons accepted. Thirdly, this solution is necessary to comply with legal standards contained in the numerous relevant international documents, as well as to ensure consistency of the existing criminal legislation in the Member States of the European Union, which already regulates the issue of liability of legal entities for criminal offenses. The legislator, therefore, accepted the indisputable fact that the liability of legal entities for offenses unstoppably leads to the European legislation and its legal standards and also international documents to majority of countries around the world.[14] That is why the text of the Law on liability of legal entities for offenses is harmonized with positive experiences in the implementation of the

7 In 2014., out of the 102 715 recorded criminal acts in the Republic of Serbia, 51 320 were thefts and major thefts, which makes 50% of the overall number. Source: Zvanična statistika MUP-a R. Srbije..

8 Krivicnom zakoniku RS "Sl. glasnik RS", no.85/2005, 88/2005, 10772005, 72/2009, 111/2009 и 121/2012

9 Krivični zakonik, art. 203., 204., 208., 210, etc.

10 Bodrožić, I.; Krivična dela sa elementima visokotehnološkog kriminala, Bezbednost, no. 3/2013, Beograd, p.144

11 Zakonik o krivicnom postupku, Sl. glasnik RS, no. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 and 55/2014

12 Zakon o odgovornosti pravnih lica za krivična dela, Sl. glasnik RS, no.97/2008

13 Since the law regulating the responsibility of legal entities for criminal acts (Zakon o odgovornosti pravnih lica za krivična dela) came to power, there has not been a single court case based on this law in the Valjevo court.

14 Vrhovšek, M.; Pravno lice kao izvršilac krivičnog dela prema Zakonu o odgovornosti pravnih lica za krivična dela, NBP, KPA, 2010, p.41-42

Law on Economic Offences. Generally accepted opinion is that the Law has shown good results in reducing economic offenses, during its fifty years of application. Offenses of legal entities threaten the economic and financial system of the country.

The countries of former Yugoslavia, usually relate the liability of legal entities to the behaviour of the responsible person, which means that only a criminal offense committed by a responsible person can be treated for the liability of a legal person. If any other employee, who is not the responsible person, commits a criminal offense, the legal entity cannot be accused of this crime. Furthermore, it is important that the offense has been committed in the name, for the account or benefit of that legal entity, or that committing it the person violates some of the duties of a legal entity, or using this, legal entity has realized or should have realized unlawful material benefit for itself or other entity.[15]

However, even though the law has been in force for more than six years in the Republic of Serbia, the police department of Valjevo has not filed any criminal charges in the district of its responsibility, nor has there been any legal procedures or convictions for the criminal acts under that law, we can conclude that the law is not applied.[16]

As with other offenses against property in the area, the main reason for the electricity theft is gaining illegal material profit. The method of committing the criminal act has changed over time, from the consumption of electricity without measuring at all, illegal connection to someone else's electricity meter, directly connecting to someone else's electricity meter, placing magnets on electricity meter that interfere with its operation, to the illegal modifications of the meter so it measures lower consumption of electricity. However, companies for electricity distribution put a lot of effort to get technically improved meters for measuring, which at the same time make offenders of these crimes try to find new, modern ways of electricity theft. A huge problem with electricity is that its owner is the state over public companies, which in the name of state distribute electricity to the end user and representatives of these public companies, which most frequently show almost no interest in the theft (they act in a manner "It is not me who is damaged, the state is"). In many cases, the employees of public companies 'in their spare time', for a certain amount of money, help the end user in electricity theft, in a way that is difficult to detect. Those employees are usually professionals in this area (electricians, fitters, etc.), whose regular job is that the end user – the buyer of electricity is connected to the electricity system and to make the measuring equipment work correctly. In this way, they become accomplices in committing the crime, and also make it difficult for the police and other competent authorities to detect, solve and prove the commission of a crime in the court.

Since electricity theft is wide spread, the state budget has less money to invest in improving the technical system of Electric Power Company. Legal entities - companies which commit the theft have lower costs and can offer their products at much lower price than other manufacturers. The social consequence of inadequate suppression of this kind of theft is that it happens more frequently than before, more consumers are involved in this crime and the number of undetected thefts is rapidly increasing. Some experts estimate that in the Electric Power Industry of Serbia only a fifth of electricity theft is discovered by the competent authorities, and just a small percentage of discovered go to the court, and only a few of offenders are sentenced.

There are more and more newspaper headlines warning the public of this phenomenon: "Believe it or not: Serbs can steal electricity in 52 Ways"[17], "In Serbia electricity theft is estimated at the amount of 80 million Euros"[18], etc.

The text below presents some new forms of electricity theft committed by large consumers, usually commercial ones (legal entities). The following passages are concerned with the particularities that have been discovered on the territory under the jurisdiction of the police department of Valjevo in the last two years, where the damage to the state are millions in cash amounts at a year level by a single perpetrator.

CHARACTERISTIC METHODS OF ELECTRICITY THEFT IN 2014 ON THE TERRITORY OF VALJEVO POLICE DEPARTMENT

In order to give you more information about modern ways of electricity theft, we should consider some prior knowledge in the field of energy first.

Supplying the end users - consumers with electricity is regulated by the Zakon o energetici[19] and the Government of RS has passed the Uredbu o uslovima isporuke i snabdevanja električnom energijom[20] which regulate this area. Although nowadays the end-users can choose from which entity to buy electricity,

15 Kolarić, D.; Korupcija i odgovornost pravnih lica za krivična dela, NBP, KPA, 2006, p. 110
16 Source: Javno tužilaštvo Valjevo.
17 Vesti online.com,25.01.2014
18 Beta B92, 03.05.2014
19 Zakon o energetici, Sl. glasnik RS, no.57/2011, 80/2011- ispr. 93/2012 и 124/2012
20 Uredbu o uslovima isporuke i snabdevanja električnom energijom, Sl. glasnik RS, no.63/2013

the largest number of them continues to be supplied by the Elektrosrbija D.O.O. which is a public company established by the Republic of Serbia and perform activities of general interest. On the territory of Valjevo, the distribution to end users is done by the Electricity Distribution Company of Valjevo, which is an organizational unit – the branch of Electroserbia D.O.O. Kraljevo.

New forms of criminal activity and electricity theft were observed on the territory of Valjevo Police Department during 2014. The thefts were discovered by professionals employed in the Electricity Distribution Company in Valjevo (ED Valjevo, in the text below). It is interesting that the theft was in progress continuously for 2-3 years and the value of illegal benefit for consumers of electricity s several millions of RSD, because large consumers were involved.

To illustrate the problems in solving the cases of electricity theft, we will analyze five of these cases committed by legal entities, which are still under investigation and have not yet received the court epilogue. [21] In all the cases, digital, multifunctional meters for commercial use were used for measuring electricity (neither had residential meter installed) and some of them were 'smart' meters. The specificity of 'smart' meters is that they can be read remotely and can register some 'fraudulent acts' done on the meter. The meters are delivered from the manufacturer with two state verification marks (seals) on the top cover of the meter. Any damage on the state verification marks/seals is unauthorized and removing the seal is legally regulated and only allowed to be done by the Directorate of Measures and Precious Metals and some other bodies (usually the manufacturers) who are authorized for the verification of the meters. The state verification marks/seals contain a number which presents the year when the calibration expires (has to be done again) and the number which presents what body has done the verification. Some of these meters register every opening of the upper and lower cover of the meter (the date and time of every opening) and some do not. It depends on the type of the meter. The lower cover of the measuring meter is protected with one or two marks/seals of the Electricity Distribution Company. Marks in a form of label in a plastic case or lead seals can be found on the both covers of the meter.

- Case number one: In January 2014, a fire was reported in the meter enclosure of a commercial user-A, in Valjevo. During the fire, the electricity meter was significantly damaged. The fire was reported to ED Valjevo by one of its employees who was already on-site, not officially sent by ED Valjevo (he was not even employed in the Department of measurement in ED). That person was on-site only because he was in personal relations with the commercial user-A. After the fire was put down, that person connected the user-A to the electric distribution network without metering the consumed electricity (every action he performed was not legal). The Department of measurement of ED analyzed the electricity consumption of the user-A after receiving the report on the incident, and found out that in the period from 01.12. 2012 until the destruction of the meter (in fire), the electricity consumption was significantly lower compared to the previous period. Additionally, it was found that after installing a new meter, the consumption of electricity was the same as it used to be back to the period before 01.12. 2012. Because of these suspicious circumstances, the damaged meter was sent to its manufacturer to be analyzed, at the end of January 2014. The manufacturer noted unusual damages not seen in the previous practice. The damages on the meter were not caused by increased voltage or current. The meter was exposed to an external open flame, which caused its damage. Someone wanted to burn (completely damage) the meter to hide the following unauthorized modification- adding new resistors, in parallel, to existing ones in the secondary circuit of current transformer, in the meter, so it registers less consumed electricity. In this case there is a serious doubt that the fire was set to hide the committed crime (the modification in the meter and damaging of the state verification mark). The manufacturer concluded that in the period from 10.10. 2012 until the fire, about 40% of consumed electricity was not measured (because of the performed unauthorized modifications). It was found that before the unauthorized modifications maximum measured current values, monthly, were 6 or 7 amps and after modifications, 3 to 4 amps.

All the documents related to the case were officially sent to the Public Prosecutor's Office, by ED Valjevo, in March 2014. The prosecutor, who is in charge of the case, did not send a request for any further information and actions to the Police Department of Valjevo, yet. A year from the event, the police were not been officially notified of the event, and no legal measures and actions were taken in solving this case (crime).

- Case number two: In June 2014, the Department of measurement ED Valjevo, read and analyzed electric characteristics from the 'smart' meter installed to measure the consumed electricity of a commercial user-B in Valjevo. The 'smart' meter for commercial use was produced in 2011 and was calibrated to 2023. It had a switching module (enables the function of consumption management) and GPRS module (for remote communication) so it could be read or switched off remotely. During the remote reading of electric characteristics from the meter it was noticed that current in one phase was zero and so was the power in that phase (that means there was no measuring of the consumption of electricity in that phase). The following step was to read the data from the 'fraud event log' registry of the meter,

21 Source: Documents of ED Valjevo.

where all events that could indicate potential abuse are recorded. It was found out that in March 2014, both the upper and lower covers of the meter were opened. Therefore, it was suspected that the damage to the both verification marks/seal of the authorized body and mark/seal of the ED Valjevo were made. In July, the expertise of verification marks/seals was requested from the only authorized body for metrological supervision, the Directorate of measures and precious metals. The authorized representatives of the Directorate of measures went to the commercial user-B's object in Valjevo, performed the requested supervision of the meter verification marks and made an official report that no damage to the verification marks was done.

However, the employees of the Department of measurement ED Valjevo, when installing a 'smart' electricity meter on 28.12.2012, made a photo documentation of the meter and all its marks/seals verifications sent to the ED Valjevo. They compared the looks of marks/seals when the meter was installed (photos made on 28.12.2012) with the looks of marks/seals in July 2014. the mark/seal on the cover of the meter of the ED Valjevo was not in the same position and wires were coming out to the 'front part' of the seal (when the meter was installed) and in July 2014 they were found coming out to the 'back side'. The length of the wire passing through the seal was even not the same. In order to determine what really happened to the meter, after the metrological supervision by the Directorate of measures was done, the meter was sent to the manufacturer (and the new one was installed). The manufacturer did the detailed examination of the meter and sent an official report to the ED Valjevo. In its report the manufacturer claimed that both the verification marks/seals were forged and modification was done within the meter to stop measuring of consumed electricity in one phase.

In October 2014, the employees of the Department of measurement ED Valjevo read and analyzed electric characteristic from the new meter installed to a commercial user-B, and again found out that current in one phase was zero, and noticed a decrease in electricity consumption. Afterwards they read the data from the 'fraud event log' registry of the meter and found that only 20 days after installing the meter, someone opened the upper and lower covers of the meter. A new photo documentation of the meter was done and compared with the photo documentation done during the installation of the meter. Again the appearance and position of seals were not the same as at the time of installing the meter.

The commercial user-B was disconnected from the electric distribution network and all the documents related to the case were sent to the Public Prosecutor's Office. The police were not included in the investigation in order to help solving and proving apparently committed criminal offenses.

What is very important to note in the case of the commercial user-B is that we have two completely deferent opinions about the verification marks/seals in the meter. The Directorate of measurements and precious metals did not find that marks/seals were damaged or forged, but the manufacturer found out the opposite-that the marks/seals were forged! The manufacturer in its report gave a detailed explanation proving the marks were forged. The Directorate of measurement in its report claimed the opposite, that marks were original and undamaged, without giving any explanation or proof. The Directorate of measurements and precious metals is the only authorized institution in the state for supervision of the verification of marks/seals in electricity meters, controlling the correctness of the same, according to the Zakon o metrologiji [22] and Uredbe o nacinu vrsenja metroloskog nadzora[23]. The Directorate for measurements was founded to protect the general interests of the state and of all citizens and it must not allow any intentional or unintentional mistakes or lack of professionalism of its employees.

- Case number three: In September 2014, the Department of measurement of ED Valjevo read and analyzed electric characteristic from the 'smart' meter installed to measure the consumed electricity of a commercial user-C in Mionica. The meter had GPRS module for communication so it could be read remotely. During the remote reading of electric characteristics from the meter it was noticed that current in two phases was zero and so was the power (that means there was no measuring of the consumption of electricity in those two phases). The 'smart' electricity meter was installed at the user-C in January 2012, and photo documentation was made. The meter was produced in 2011 and calibrated to 2023. After the employees of the Department of measurement noticed current in two phases is zero, they went on-site to check the meter. They noticed that the plastic verification mark/seal was in a different shape than the one when the meter was installed (because they had photo documentation). What they found on the meter was the 'strawberry-shaped' plastic verification mark while the photo documentation in which they could see the meter was installed with a 'square- shaped' plastic verification mark. They also checked the class of accuracy of the meter and found out that the meter measured only 20% of the consumed electricity. Since they suspected illegal modification on the meter was done, the meter was sent to the manufacturer. Soon, the ED Valjevo received a report from the manufacturer that seals on the meter were forgeries. The manufacturer also claimed that, at the time when that particular meter was produced, they did not have and did not use the mark/seal in a 'strawberry-shape' at all. At the time, they used a prismatic 'square- shaped' verification mark/seal,

22 Zakon o metrologiji, Sl. glasnik RS, br.30/2010

23 Uredbe o nacinu vrsenja metroloskog nadzora, Sl. glasnik RS, br.88/2010

while the 'strawberry' ones have been in use since 2013. It was also noted in the report that meter did not register consumed electricity in two phases.

In this case the time when the modifications inside the meter were done could not be determined, because the processor of the particular meter did not register the opening of the covers of the meter. This case shows us how important is that 'smart' meters have the option of registering opening of the covers so we can determine the exact time when the theft occurred and how long it lasted. A 'smart' meter helps us estimate the value of unmeasured but consumed electricity.

All the documents related to the case of the commercial user-C were sent to the Public Prosecutor's Office. The police have not been officially informed of the case yet.

Case number four: At the end of October 2014, the employees of the Department of measurement ED Valjevo read and analyzed electric characteristic from the 'smart' meter installed to measure the consumed electricity of a commercial user-D in a village near Valjevo. The 'smart' electricity meter for commercial use was produced in 2010. The meter was calibrated to 2024 and the verification lead seals had number 24 engraved (photo no.1). The meter was installed at the user-D in July 2013, and the photo documentation was made. It had GPRS module for communication so it could be read remotely. During remote reading of electric characteristics from the meter it was noticed that current in one phase was zero and so was the power in that phase (that means there was no measuring of consumption of electricity in that phase). The following step was to read events the meter registered and saved in its memory. The meter registered opening of its upper cover (cover protected from the opening by the verification seals) on June 23rd 2014. From July 1st 2014 onwards maximum monthly current value in one of the phases was zero (that means there was no measuring of consumption of electricity in that phase). After the employees of the Department of measurement remotely read entire electrical characteristics they went on-site to check the meter. The verification lead seals found on the meter had the number 25 engraved (photo no.2) instead of number 24 (the meter was installed calibrated until 2024) proving that lead seals were forgeries, the originals were replaced. Even the wires which passed through the seals were not the same length (comparison was done with photos taken when the meter was installed) and the position of the seals in relation to the wires was not the same (the position of the seal, length of wires and location where wires 'go in' and 'go out' from the seal cannot be changed once the seal is squashed with pliers). Checking of class of accuracy of the meter was done. The meter did not measure about a third of consumed electricity

The commercial user-D was disconnected from the distribution electric network. The police have not yet been informed about this case, although there is a reasonable suspicion that a criminal offense of electricity theft with removing verification seals was committed.

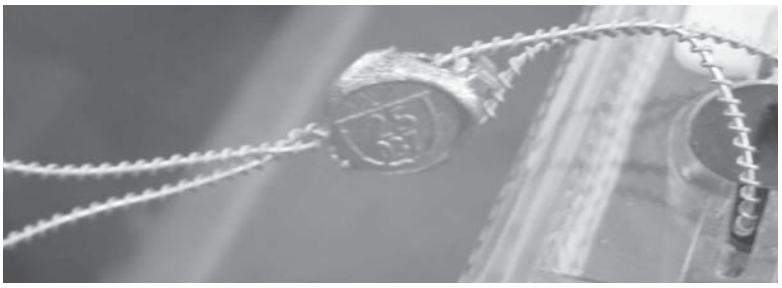


Photo 1 *Magnified part of the photo of the meter made on 25.07.2013. Lead seal has number 24 engraved.*

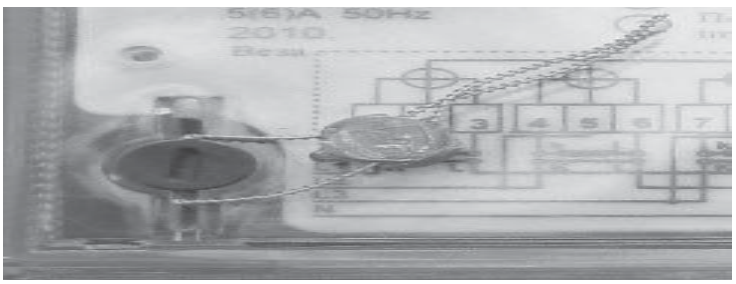


Photo 2 *Magnified part of photo of the same meter made on 24.10.2014. Lead seal has number 25 engraved.*

- Case number five: In late October 2014, the Department of measurement of ED Valjevo suspected there was an electricity theft going on at a commercial user-E in Valjevo. When on-site checking class of accuracy with measuring instrument "Zera MT 30" was performed, it was found out the meter registered about 10% less electricity than actually consumed. The employee of ED Valjevo who installed the meter did not make photo documentation. The on-site check proved that all marks/seals including lead seal of ED Valjevo and both verification marks-lead and plastic were partially damaged. The commercial user-E was disconnected from the distribution electric network. The Directorate for measuring and precious metals were informed of the event and requested to do the supervision of the verification marks. Supervision was done and the Directorate for measuring made a report claiming that both seals were original and undamaged. ED Valjevo appealed to the report and asked the Directorate to perform the supervision again. The procedure is still on-going.

The public prosecutor's office was not informed and the police were given the authority to carry out an investigation. The investigation report was made.

If we analyze these cases, which all involve suspected criminal offense of electricity theft, we can bring out next conclusions:

1) There are laws that regulate the field of energy supply and metrological supervision, however, imperfection of legal regulation of this area leaves many opportunities for abuse. That way the public company for supplying end-users with electricity is directly damaged, and the state indirectly;
2) There are doubts in the quality of work of the Directorate for measuring and precious metals as the only institution authorized for metrological supervision and for expertise of electricity meters.
3) The public company did not immediately inform the criminal prosecution authorities on suspected criminal offences performed on electricity meters. They pressed criminal charges to the public prosecutor's office after all internal checking was done. That is why no investigation of crime scene was done, nor taken urgent operational-tactical and investigative actions to complete clarification of the offence.
4) The Department of measurement ED Valjevo, although not obliged, makes the photo documentation of the look of the meter with its verification and distribution marks/seals, so they can compare the current situation to the situation when the meter was installed and easily notice if there was an abuse on the meter.
5) At the request of ED Valjevo, the manufacturers of electricity meters performed a detail analysis of unauthorized modifications done inside the meter and even the inspection of marks/seals correctness with every fact explained in detail with a multiplicity of facts in its report.
6) No case has received court epilogue, yet.
7) When we see how much the electricity meters with possibility of remote reading and with modern computer systems that detect every opening of a cover and modifications on the meter are misused, we can only assume how much the older models of meters, in which an ordinary magnet is enough to stop the measuring of consumed electric energy are misused.

CONCLUSION

In the future, it is necessary to improve the system of power supplying with changing existing law regulations and providing, a safer way of measuring consumed electricity. The possibility of abuse in this area must be kept to a minimum. We believe that all measuring meters should relocate, as soon as possible, to the public areas and that all legal entities, in general all large consumers of electricity, should have 'smart' digital, multifunction meters with remote reading of power consumption. The practice of some employees of ED Valjevo, which is not mandatory, is taking pictures before and after each installation of electricity meters making photographic documentation. That practice has shown to be very helpful in proving the abuse done by removing and damaging the state verification mark and/or distribution mark-seals from the meters, in order to modify them. Our proposal is that making photo documentation of a meter and other measuring equipment should be the obligation of the EPS.

In cases with a suspicion of committing an offense the police and the public prosecutor must be informed immediately, in order to take all necessary measures predicted by "Zakonik o krivicnom postupku", to clarify the crime and to identify the offender. In clarifying the crimes committed by the modification of 'smart' electricity meters, which have modern computer systems, should include public prosecutor's office and the police who are fighting against and trying to stop cyber crime.

It is necessary to introduce a new criminal offense in a legal system, which would refer to the criminal responsibility for electricity theft for an individual or legal entity having financial benefit from that criminal

activity. Thus, a consumer (person or entity) who has been given the use of a meter for measuring the consumed electricity should be criminally responsible if the modifications are done to the meter (stop metering on one or more phases), regardless of whether that consumer has personally done the repairs or engaged someone else to it. Therefore, it would not be necessary to prove and establish the identity of the person who performed the modifications on the electricity meter. The perpetrator of the unauthorized modifications would be responsible for committing an offense according to the current legislation, for example for taking off the official seal or mark and destruction or damage to public devices.

In the current legislative system it is very difficult, and in most cases impossible, to completely clear up the offense of electricity theft, and even harder to prove it in court, because it is necessary to collect evidence of all the circumstances: the time and place of execution, determine the value of the illegally confiscated goods (electricity in this case) and who the direct perpetrator of a crime is. The perpetrator of the theft is not only the person who has the benefit of that crime, but also a person who performs modifications on the meter. Hence, mainly electricity theft is committed in complicity of two or more persons, one who has skills for crime execution (electrician, etc.) and the other one who has the benefit of a reduced measuring of consumed electrical energy.

And finally, it is necessary to bring in the Law about responsibility of legal entities for criminal offenses they committed, that can be easily executed.

REFERENCES

1. Banović, B.; Lajić, O.; Milošević, M.: "Krađa električne energije, kao pojavni oblik krivičnog dela krađe", Bezbednost 1-2/2008, p. 130-146
2. Bodrožić, I,; Krivična dela sa elementima visokotehnološkog kriminala, Bezbednost, br. 3/2013, Beograd, p. 142-158.
3. Kolarić, D.; "Korupcija i odgovornost pravnih lica za krivična dela", NBP, KPA, Beograd, 2006, p. 101-114
4. Krivični zakonik RS,"Službeni glasnik RS" br.85/2005,88/2005-ispr.,107/2005-ispr.,72/2009, 111/2009, 121/2012 i 104/2013
5. Uredba o uslovima isporuke i snabdevanja električnom energijom,"Službeni glasnik RS" no.63/2013
6. Uredbe o načinu vršenja metrološkog nadzora,"Službeni glasnik RS" no. 88/2010
7. Vrhovšek, M.; "Pravno lice kao izvršilac krivičnog dela prema Zakonu o odgovornosti pravnih lica za krivična dela", NBP, KPA, Beograd, 2010, p. 17-42
8. Zakonik o krivičnom postupku, "Sl. Glasnik RS", br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014
9. Zakon o nadležnosti i organizaciji državnih organa za borbu protiv visokotehnološkog kriminala,"Službeni glasnik RS" no. 61/2005, i 104/2009
10. 10. Zakon o odgovornosti pravnih lica za krivična dela"Službeni glasnik RS" no. 97/2008
11. Zakon o energetici,"Službeni glasnik RS" no. 145/2014
12. Zakon o metrologiji,"Službeni glasnik RS" no. 30/2010

UDC: 343.352
343.971

CORRUPTION, TRUST AND INTEGRITY[1]

Gyöngyi Major[2]
Institute for Strategic Research, Budapest
Aleksandar Cudan[3]
The Academy of Criminalistic and Police Studies, Belgrade

Abstract: Emphasizing the significance of recognizing the motivation behind conscious and rational decisions of the participants in corruption, as well as accentuating those possibilities that are created within the functioning of institutions, this paper focuses on the concept of corruption within the context of the New Institutional Economics perspective, on the one hand, and on the other within the context of New Public Management. Starting from new approaches, the attntion focuses on the possibility of detection and study of corruption risk, which is increasingly interpreted as one of the most significant points of anti-corruption strategic programmes. It is pointed out in literature that the important characteristics of participation in the corruption process are the reciprocity of relations and the power of cooperation, due to which the study of social norms and trusts which might lead to the growth of interdependence becomes even more necessary.

Discussing the possibilities of risk reduction, the study bases on Coleman model, which within the context of game theory shows the possibility of risk reduction, aspiring to highligh the roles on the principles of integrity based on preventive measures.

Keywords: risk, cooperation, integrity, strategy, corruption.

INTRODUCTION

In its broadest sense, the very definition of corruption would suggest that corrupt acts are deviations from implicit or explicit behavioural norms, done to maximise private gains. However, the widespread nature of corruption in some societies indicates that corrupt behaviour is the norm itself – despite the fact that it is inefficient and generally condemned.[4]

In this study, we first of all wish to emphasise that corruption is a phenomenon that is far too complex to be simply considered a deviant behaviour in economic relations and, in this interpretation context, efforts made to decrease its degree are unrealistic.[5] Corruption is a consequence of complex social processes, in which – besides political and economic factors – "deep-rooted cultural reasons also play a key role: social traditions to a great extent determine the existence and pervasiveness of corruption."[6] Those fighting against corruption must understand the nature of corruption if they are to be efficient in their mission.[7]

1 This paper is the result of the research on project: "Crime in Serbia and instruments of state responce", which is financed and carried out by the Academy of Criminalistic and Police Studies, Belgrade - the cycle of scientific projects 2015-2019.
2 major.gyongyi@gmail.com
3 aleksandar.cudan@kpa.edu.rs
4 Mishra, 2005
5 Literature about corruption has recently increased explosion-like in volume (Reinikka – Svensson, 2005) and focuses primarily on analyses that compare countries and ones about corruption perception indices. Studies examine corruption in the light of and as dependent on countries' politics and institutional structures. Macro-level statements, however, stop at the phenomenon level and fail to investigate the deeper context of the problem. Besides social impacts, the examination of individual ambitions is also very important (Dovidio et al. 2006). Though literature on corruption is growing in volume, no empirical research has so far been carried out to examine the interrelations between personality traits – like extroversion, conscientiousness, risk taking, emotional stability – and corruption related processes. Co-authors Bereczkei and Tóth emphasise that exactly because "different tests indicate that people's personality characters show major differences in how they participate in social interactions, this diversity is to be expected also in the case of corruption. Corruption related research projects tend to take a one-sided approach: they mainly examine the phenomenon's social components and effect mechanisms and have so far paid little attention to individual abilities, attitudes and inclinations. And that is connected not only to personality psychology but also the genetics science." In other words, though there is no direct relationship between corruption and genes, there appears to be an indirect connection in any case. In their study, Bouchard and Loehlin (2001) proved that genetics related factors are 40-60% responsible for differences between individuals in their personality traits, attitudes and social orientations. For this reason, research in this area is desirable.
6 Takács–Csapodi-Takács-György, 2011
7 Blackburn – Forgues-Puccio, 2009

While traditional societies are transparent and the breaking of norms easily gets unveiled,[8] modernity is characterised by an increasing complexity of relations, as a result of which transparency decreases and exchange transactions are realised more and more along self-interest. In the game theory context, corruption is a behavioural system that carries the elements of competition and cooperation at the same time.[9] According to co-authors Bereczkei-Tóth, this is exactly where one of the problem's roots is found. "In a society where publicity does not work sufficiently enough and society's macro-processes are not sufficiently transparent, corruption forms a rather closed and autonomous system, which is more or less independent of the institutions of society. "Internally", cooperation fortifies and legitimises it, together with all its materialistic and psychological advantages (profit, satisfaction, trust, etc.). "Externally", however, it is closed and is not covered by the social checking processes that would point out its unlawfulness and immorality. As time goes by, the system of services and counter-services may become arranged into a stabile structure in which the parties tend to care much more about day-to-day challenges than society's value judgments, as the latter are often hardly perceivable by them." [10]

If the players in corruption interaction manage to overcome the cognitive dissonance that though corruption brings gains but it also breaks norms, they can think of the interaction as something legal. As a result, corruption may reach a level where it comprises a stabile subsystem within society. If social control is not strong enough, becoming a participant may far more become a merit than staying outside the compulsion triggered by circumstances. [11]

To successfully fight against corruption, therefore, publicity and transparency are a must – but, on the other hand, to keep control over corruption, it is indispensable to prevent the establishment of corruption structures.[12] Participation in corruption is greatly dependent upon the power of collusion between players and the reciprocity of their relations – which are dependent on the effects of norms and the level of trust.

CORRUPTION AND TRUST IN INSTITUTIONS

In the broadest sense, corruption can be considered as a contract failure: an interaction in which one party does not observe its contract undertakings, which, in general, is the consequence of a system of interconnections comprising three components: information asymmetry, a conflict of interests of the parties to the interaction and the asymmetric distribution of decision risks.

For a long time, corruption behaviour – the breaching of "laws" – had been considered a deviant form of behaviour. New institutional economics, however, has provided a new interpretation of the problem, in which "the breaching of laws is not some special case but the field for economic rationality and, for this reason, corruption is a natural subject of economic research."[13]

In the framework of new institutional economics, whether someone participates in corruption primarily depends on the cold-blooded deliberation of the benefits, risks and long-term return. Becker's analysis,[14] which is now a classic, and the model developed from it by Ehrlicht, presents crime as a decision making problem and carries out the analysis on the level of individuals, using the traditional tools of microeconomics. The central assumption in this theory is that in case two acts are mutually exclusive in a given period of time, one will associate an expected gain to each of them and will decide about one or the other based on this gain.[15] And though the decision is influenced by what norms (institutions) make headway in the given

8 By contrast, there are references to (and interpretations of) certain forms of corruption also in, for example, tribal societies. Levi Strauss's works are often quoted to state that in South American societies leaders often maintain their power through the system of gifting and counter-gifting. According to Blackburn et al. (2009), corruption exists everywhere in the world, in all political and economic systems, to a lesser or greater extent.

9 For its participants, corruption is a cooperative "game", in which unselfishness between players carries a major role – but on the level of the entire society, it is an expressly selfish strategy.

10 Bereczkei-Tóth http://mek.oszk.hu/07900/07999/pdf/bereczkei-toth_p.pdf

11 Tóth, 2003

12 The connective tissue of the structure of corruption is trust and, in general, personal networking. (This is the cooperative aspect of corruption.) It is for this very reason that Abbink (2004) emphasises the importance of the 'rotation' of persons in institutions.

13 Hámori, 1998 146. See the basic concept of Hirschman, according to which the individual chooses from action alternatives freely and rationally, after making his/her own cost/profit analysis, i.e. after having laid the veil of ignorance on the costs and profits for other and the entire society (Hirschman, 2000).

14 According to Becker (1968), economists, walking in the footsteps of Marshall, had long looked at illegal activities as being too immoral to deserve the attention of systematic science. We should remind the reader, though, that the economics of crime is traditionally traced back to Chadwick's work of 1829.

15 Ehrlich, 197. In the framework of new institutional economics, whether someone participates in corruption primarily depends on the rational deliberation of the benefits, risks and long-term return.

social medium, these norms are not exclusive[16] and do not determine everything. Even the most deeply rooted moral rules may be ignored in the process of people's rational attempt to maximise private gains.[17]

From the point of view of economic development, an ever more unavoidable – central – subject[18] is the establishment and operation of institutions which are suitable to make the fair observation of contracts[19] "rewarding", in which a breach of the contract costs more than the potential gains from its breach. The fundamental economic truth that people will breach contracts as long as it is worth to them is irrefutable. As it is becoming ever more obvious that the problem cannot be managed at the level of the decision making scope of the individual, the establishment of a system of institutions in which the observation of contracts brings positive gains is getting key importance.[20]

A fundamental precondition of the operation of institutions is the cooperation between the parties, i.e. the respect for the limits set by the institution in their decisions. Institutions can fulfil their function – inspiring the observation of fair game rules, which, at the same time, also decreases the unpredictability of the future – if a critical mass of players obeys the rules. If that is not achieved, they, by definition, can even increase the unpredictability of the future as they form a further unknown factor in the decision making process. For this reason, it is indispensable to identify and operate the motivational factors which institutions can use to motivate players to follow rules.

Several studies have recently been published about this topic. With reference to Hurd,[21] we would like to mention the three motivations to follow rules: force, self-interest and the feeling of obligation arising from the legitimation of norms. Agreeing with Hurd's argumentation, we consider the third factor as the best solution from the point of view of the long-term efficiency of rules as, in this scenario, decisions are triggered by an internal urge to respect fairness. The voluntary observation of rules is the only possible scenario to eliminate corrupt behaviour from the system.

The fight against corruption often fails because it tries to manage the effects rather than eliminate the institutional causes – and it is temptation that should be decreased.

In summary, we can say that institutional economics looks at institutions as the carriers of the game rules and, logically, identifies good institutions with good sets of game rules.[22]

Using a simile from the world of sports, the question that institutional economics asks with regard to corruption is how rules that produce fair play and an enjoyable game can be defined.[23] In recent times, not even mainstream economics has been able to work with complete ignorance of the role of institutions.[24] We would, first and foremost, like to refer to the work of Rodrik[25] and Acemoglu,[26] which discusses the differences in the level of economic development in the light of the quality of institutions. Based on their findings, we can say that the question to economics is no longer whether or not institutions play a role but which particular institutions do and how good institutions can be created.[27]

16 Especially not if and when the cost of sanctions is low. However, attention ought to be paid to the argumentation of Malik (1990), according to which the strictness of the sanction is not directly proportionate to its deterrent effect. Moore stringent sanctions inspire those who breach contracts to spend more on minimising the risk of getting caught. Lott (1992) emphasises that more stringent sanctions do not necessarily lead to refraining from crime – much more to criminals spending more money on defence counsels.

17 Hámori, 1998, 147.

18 See the World Bank's (2002) report on institutions and development, which defines three dimensions of the relationship between institutions and development: the supply of information to the players of the economy, the enforcement of ownership rights and contracts and the support of the survival of market competition.

19 Today, international organisations call countries to account for the operation of institutions.

20 It is also worthwhile to remember the argumentations that tie the role of institutions to decreasing the level of uncertainty. The cornerstones of North's institutional theory, for example, are the untenableness of the assumption of rationality and the existence of fundamental uncertainty (North, 2005, pp 16–17). According to North, institutions structure interpersonal relations and determine decision alternatives in a stabile though not necessarily efficient way (North, 1990, 6). At the same time, we should also consider that, as the primary reason for economic backwardness, North identifies the fact that the societies in this category could not create rules that were efficient, not expensive to enforce and suitable to ensure the observation of contracts. (North, 1990, 54)

21 Hurd, 1999

22 Reference is made here to the works of some Nobel laureates like Ronald Coase, Oliver Williamson or Elinor Ostrom. According to them, institutions can be analysed like game rules and vice versa: they must be analysed like game rules.

23 We will not necessarily get a realistic picture about the quality of the game based merely on the number of fouls or goals.

24 Though institutional economics became part of mainstream economics only in the 1990s, its elements had developed along mainstream economics for a longer period. The development of institutional economics is described in summary by Chavance, 2009 and Hodgson, 2004.

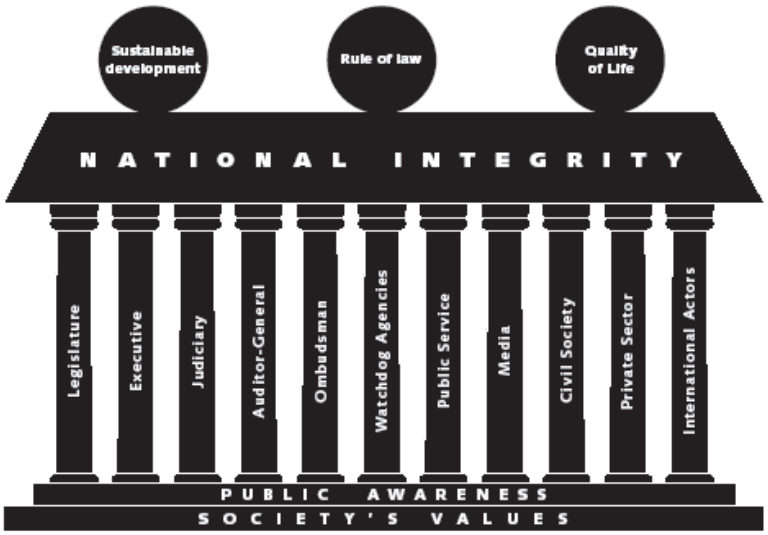
25 Rodrik et al, 2004

26 Acemoglu et al, 2005

27 Győrffy, 2012

INTEGRITY DEVELOPMENT AS AN ANTICORRUPTION GUIDING PRINCIPLE

The general recognition of the importance of institutions has led to a change in the fight against corruption. This change of direction can be interpreted as a paradigm shift, which shifted attention from the former reactive approach – crime investigation – to prevention and the strengthening of the power of resistance against corruption.[28] The idea of integrity development has become a key concept, as a means of creating the game rules for the healthy operation of institutions. The foundation of this new concept, which focuses on institutional immunity, is the strengthening of value consciousness,[29] which means and leads to complex and consistently value-based operation: with institutions functioning on the value base of society, roofs that cover them, with the "national integrity" logo shown in the frieze and the substantive aims that rest on them – namely sustainability, lawfulness and life quality.[30]



Transparency International's NIS Greek Temple (Pope, 1996)

An institution that operates in a healthy way decreases the room for corruption by making integrity[31] a fundamental logic and requirement in the behaviour of players and in organisational operation – which is capable of controlling practices in an understandable and transparent system. For the system, consistency and transparency play a key role in making corruption accurately perceivable, i.e., shed light on all activities that deviate from the service of the "public". If integrity is interpreted not only from a procedural (process-related) but also a substantive (content-related) aspect, it also integrates – besides basically ethical issues like commitment to the public interest and the attitude of incorruptibility (or, rather, integrity) –

28 The practice of using "soft means" for the containment of corruption, i.e. the application of integrity management systems operated with a preventive approach, has just begun – but in the countries where it is already applied, it is bringing far more success than state interventions that focus exclusively on criminal law and regulatory means.

29 Rules, value consciousness and commitment are parts of the organisation's power of resistance and form an antibody that quickly senses attacks by parasites and can react to them. Pallai uses this expressive metaphor to describe the practice of corruption: using Richard Dawkins's meme concept, he points out that certain corruption practices work as successful memes. "A person inclined towards corruption will quickly receive the memes carrying corruption ideas appearing in society (cultural "gondola packages"), which give them ideas and help those considering corruption to reduce their feeling of guilt through some sort of rationalisation. In a social medium tolerant towards corruption and in a weak organisation, these memes spread quickly and operate excellently. If necessary, they are also adaptive: the spreaders are often individuals and groups that possess strong interest enforcement capabilities, intelligence and a broad network of acquaintances, who/which quickly learn from one another and collect information about the changes in the receiving medium and can thus accurately and quickly reshape and adapt adopted practices with an eye to gaining benefits. If we consider corruption practices as memes we can look at their carriers as parasites that carry the corruption gene, who will attack the public administration organisation to gain benefits. I am using the term "parasite" because both parasites and corrupt persons need a host organism/organisation: they cannot create their conditions of life alone… Parasites cause severe damages to a weak organism. At is at this point that illnesses must be treated: the fight against the parasite must be launched and other illnesses that cause the weakening should also be treated."

30 The national integrity system, which ensures the good governance of institutions, is depicted by Jeremy Pope (1996) as an antique temple. See Figure 1.

31 "Integrity is a concept of consistency of actions, values, methods, measures, principles, expectations, and outcomes. Full definition of integrity: 1. firm adherence to a code of especially moral or artistic values: incorruptibility; 2.: an unimpaired condition: soundness; 3. the quality or state of being complete or undivided: completeness" http://www.merriam-webster.com/dictionary/integrity

further values like professional competence, organisational intelligence and management culture: it is with the entirety of all these that the organisation can create a cooperative system of its activities and members.[32]

It is important to emphasise that integrity development is not merely a set of tools and means but a management and control approach, a state-of-the-art strategy which is characterised by the incorporation of tools for the coordination, motivation and mobilisation of staff in the management's toolset. What makes these important is the fact that value and rule awareness makes the institution's staff partners for and in the fight against corruption. "The integrity approach raises awareness of the responsibility of the organisation and its staff in the fight against corruption."[33]

Institutions' integrity development can actually be interpreted as a culture change in management. The essence of this change is that integrity becomes a guiding principle of the good governance of the institution, which can permeate the institute's entire operation. In this respect, professional literature distinguishes primary – direct – and secondary means and tools of integrity construction: the latter, once infiltrated into the organisation's planning and management system, can make the quality of integrity a guiding principle that truly permeates the organisation's entire operation. For the distinction of tools and means, see the table.

Integrity management framework: Three pillars and two layers. (OECD, 2009)

	Instruments	Processes	Structures
Core measures	Codes, rules, guidance, integrity training and advice, disclosure of conflict of interest, etc.	Overall continuous integrity development process, continuous development processes for individual instruments, one-off projects to introduce or change instruments, etc.	Integrity actor, management
Complementary measures	Integrity as criterion in personnel selection and promotion, integrity aspects of procurement procedures and contract management, including integrity in the quality assessment tool, etc	Processes in personnel management, procurement and contract management, financial management, etc.	Personnel management, contract management, financial management, etc.

The integrity model and the related "Good Governance"[34] aim at ensuring the healthy operation of institutions, in which preference is given to the observation of rules and, moreover, institutions are operated as a system suitable for the implementation of values and goals.[35] Integrity-building as a new anticorruption principle thus requires systematic development, which not only provides a cyclic, self-perfecting logic at the organisation level but – in connection with the development of personal integrity – also gives rise to a desire to develop individual integrity competences.[36] In recent times, the interpretation of competence has incorporated new meanings, which – in the context of "meta-abilities" – enable self-controlled acting and development.[37]

Competence-based integrity development is also important as it is a learning process. Joint participation, direct experiencing and empirical learning can together lead to a decrease in integrity related risks.

CONCLUSION

Though the new anticorruption paradigm is only in its infancy, we are already witnessing the continuous confirmation of the rightfulness of the integrity development concept defined with a preventive approach. As, according to international experience, prevention-focused practice is slowly but surely getting adopted, this study focuses on the strengthening of the culture of integrity. Integrity as a guiding principle

32 Pallai, 2014
33 Pallai, 2014
34 Please note that "good governance" is not a new concept. As early as in 1338, Ambrogio Lorenzeti, for instance, painted the allegoric pictures of "good" and "bad" governance on the four walls of the council room of the Town Hall of Siena, Italy.
35 It was during the era of the neoliberal economic policy, which became known through Margaret Thatcher, that the New Public Management concept was born, which tried to use the economy-effectiveness-efficiency trinity to adapt professional enterprise management mechanisms into public administration – which, as emphasis shifted towards private interests, led to corruption scandals. It was in reaction to this phenomenon that value-centred public administration trends began to take shape. And these started to give preference to the Good Governance and the related Integrity models (Sántha-Klotz, 2013).
36 Integrity as a complex personal competence is also measured by the performance appraisal system of the public sector (professionals, government officials, etc.) (Sántha-Klotz, 2013). See: "Towards a Sound Integrity Framework: Instruments, Processes, Structures and Conditions for Implementation" Global OECD Forum on Public Governance, Paris, 4-5 May, 2009.
37 Zaugg, 2006

for organisation management may support the operation of society on the foundation of ethics and, by applying a complex competence approach, can potentially become the cornerstone for the achievement of society's substantive goals – the synthesis of sustainability, lawfulness and life quality.

Corruption as it is deceives in human's mind, and before it becomes materialized, it integrates into practice and customs, affects our moral values and finally evolves into a criminal act. The aim of this work is to introduce this topic and to highlight its relevance both to the professionals who encounter it during their professional careers, and to the ordinary people who may come across it in their everyday life.

REFERENCES

1. Abbink, K. (2004) Staff rotation as an experimental policy: An experimental study. European Journal of Policy Economy 20, 887-906.
2. Acemoglu, D.–Johnson, S.–Robinson, J. A. (2005): Institutions as The Fundamental Cause of Long-Run Growth. (Ed:Aghion, P.–Durlauf, S. N.) In: Handbook of Economic Growth. Vol.1A. Elsevier B. V. 385–472
3. Bereczkei ,T .- Tóth, P : A korrupció kialakulása és fennmaradása: evolúciós-etológiai szempontok http://mek.oszk.hu/07900/07999/pdf/bereczkei-toth_p.pdf
4. Becker, G. S. (1968): Crime and Punishment – An Economic Approach; Journal of Political Economy, Vol. 76., No. 2., 169–217.
5. Blackburn , K. – Forguse –Puccio , G. F. (2009): Why is corruption less harmful in some countries than in others. Journal of Economic Behavior & Organization. 72. 797–810
6. Bouchard, T. J. and Loehlin, J. C. (2001) Genes, evolution, and personality. Behavior Genetics 31. 243-273.
7. Chadwick, E. (1829): Preventive police. London Review, Vol. 1. 252–308.
8. Chavance, B. (2009): Institutional Economics. New York: Routledge
9. Győrffy, D. (2012): Intézményi bizalom és a döntések időhorizontja. Közgazdasági Szemle, 59(4) 412–425
10. Dovidio, J. F., Piliavin, J. A., Schroeder, D. A. and Penner, L. A. (2006): The Social Psychology of Prosocial Behavior. Lawrence Erlbaum Ass., London.
11. Ehrlich, I. (1973): Participation in Illegitimate Activities. A theoretical and Empirical Investigation; Journal of Political Economy, 81. 521–575.
12. Hámori B. (1998): Érzelemgazdaságtan – A közgazdasági elemzés kiterjesztése; Kossuth Kiadó, Budapest
13. Hirschman, A. O. (2000): Versengı nézetek a piaci társadalomról – és egyéb újkeletű írások; Jószöveg Mőhely Kiadó, Budapest
14. Hodgston, G. M. (2004): The Evolution of Institutional Economics: Agency, Structure and Darwinism in American Institutionalism. London: Routledge
15. Hurd, I. (1999): Legitimacy and Authority in International Politics. International Organization. 53. (2) 379–408
16. Lott, J.R. (1992): Do We Punish High Income Criminas Too Heavily? Economic Inquiry, 4(4) 583-608
17. Malik, A (1990): Avoidance, Screening and Optimum Enforcement. RandJournal of Economics. 21(3)
18. Mishra, A. (2005): Persistence of corruption: Some theoretical perspectives. World Development. 34 (2) 349–358
19. North, D. C. (1990): Institutions, Institutional Change and Economic Performance. Cambridge University Press, Cambridge.
20. North, D. C. (2005): Understanding the Process of Economic Change. Princeton University Press, Princeton, N. J.
21. OECD: (2009): Global Forum on Public Governance Towards a Sound Integrity Framework: Instruments, Processes, Structures and Conditions for Implementation
22. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=GOV/PGC/GF(2009)1&-doclanguage=en
23. Pope, J.: National Integrity Systems: The TI Sourcebook. Berlin: Transparency International. 1996.
24. Pallai, K: Bevezető gondolatok a közigazgatási integritás és integritásmenedzsment témájához.
25. http://uni-nke.hu/uploads/media_items/bevezeto-gondolatok-a-kozigazgatasi-integritas-es-integritas-menedzsment-temajahoz.original.pdf

26. Reinikka, R. – Svensson, J. (2005): Using microsurveys to measure and explain corruption. World Development. 34 (2) 359–370

27. Rodrik, D.–Subramanian, A.–Trebbi, F. (2004): Institutions Rule: The Primacy of Institutions over Geography and Integration in Economic Development. Journal of Economic Growth, 9. 131–165.

28. Sántha, Gy. – Klotz, P.(2013): Integritásmenedzsment. Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet.

29. Takács, I. – Csapodi, P. – Takács-György, K. (2011): A korrupció, mint deviáns társadalmi attitűd. Pénzügyi Szemle, 56(1), 26-42

30. Tóth P. (2003). A korrupció mint adaptív stratégia. Egy magatartásbiológiai megközelítés lehetősége. (Ed:Berki, Z)In: Korrupció Magyarországon II. Budapest, Transparency International Magyar Tagozata Egyesület. 11-41

31. World Bank (2002): World Development Report 2002. Building Institutions for Markets. World Bank, Washington

32. Zaugg, R. J. (2006): Handbuch Kompetenzmanagement. In: Durch Kompetenz nachhaltig Werte schaffen. Fertschrift für Prof Norbert Thom zum 60. Geburtstag. (Ed:Zaugg) Bern-Stuttgart-Wien, Haupt Verlag.

UDC: 343.59-057.874
316.624-057.874

PEER INFLUENCE AND THEIR REACTION ON SCHOOL VIOLENCE

Natasa Jovanova[1]
University "St. Kliment Ohridski", Bitola, Faculty of Security, Skopje

Abstract: The subject of this paper is an analysis of peer influences on the children and their reaction to violence in schools. When we analyzing the violence between children particularly in schools, among the important factors that are analyzed is peer pressure on the behaviour of children and their reaction as bystanders/observers of it. In this direction, the paper provides an analysis of the theories that explain the impact of peers on children violent behaviour, such as attraction theory, homophile and theory of domination. Another question or aspect in the area of prevention of school violence is peer reaction or manner of response in case they occur as bystanders/observers of school violence. This category of children is often forgotten in the studies, but has an important role in the prevention of school violence. Researches show that there are several categories of bystanders/observers: "assistants" that assist in the violence directly, "supporters" come around and see or laugh until other children perform violence, "defenders" who are trying to stop the violence and "outsiders" that are not aware of the violence or not interested about it. According to the important role of peers, prevention programs should also be directed to peers and their transformation into active bystanders/observers, trough rising of their awareness that from their way of reaction, depends how much will be present violence among children in schools.

Keywords: peers, violence, children, reaction.

INTRODUCTION

The issue of school violence is a current topic worldwide. The fact that we cannot deny the existence of school violence in any society imposes an obligation in the scientific and professional community for its study in order to prevent it. But, to get the answer why violence occurs, and even more why children perform violence, especially in schools, is a very difficult. In the literature, there are many theories that give explanation about the children violent behaviour, ranging from biological, psychological, sociological and new sociological theories. Most comprehensive theory that can give a more comprehensive picture of children violent behaviour is system theory that does not squeeze out the impact of certain factors, but is considering their mutual connection and influence on children violent behaviour. On the children behaviour can impact many intertwined factors, some more and some less visible, more or less intense or act as mediators, and it would be difficult or unrealistic to expect that we can enlighten the whole network of factors. But despite this fact, the need for determination of the factors that are connected with children violent behaviour is necessary as data source for direction in creation of prevention programs.

Within the overall network of factors, can be found number of individual factors (such as gender, temperament, depression, socialization), group of micro social factors (family, school, peers and the media) and macro social factors in which violence occurs (the impact of politics, culture and war).

Hence within the literature very little attention is paid to the influence of peers on the children violent behaviour and their reaction to violence, taking into account that the peers play a critical role in the creation of the external behaviour of children. Therefore children behaviour is dependent from their personal characteristics, as well as from the characteristics and behaviour of certain peer. (Hanish, Kochenderfer-Ladd, Fabes, Martin, & Denning, 2004)

During childhood and adolescence peers are playing a huge role in the life of children. While in the childhood the relationship with the peers is superficial and their connection is related with participating in joint activities, in the period of adolescence contact with peer gets characteristics of community, loyalty and affection. In that period, adolescents are increasingly leaning towards peers and relations with them are more intense than the relationship with parents. In that sense, the groups of peers simultaneously represent a medium for learning and practicing social skills and roles for adolescents. By comparison with the peer group, the adolescents are getting information about their value, how others see them, which contribute for building their self-image. (Batic, 2010) In the peer group, adolescent learn certain patterns of behav-

1 natasa.akademija@yahoo.com

iour based on theory of socialization which is theoretical basis for clarifying the role of friendly relations in adolescence. When this interpretation will be applied to the adolescent, the question that arises from here is how another person who is at same age as adolescent, who is also insufficient mature, can influence on the socialization of the first person, whether the adolescent may suffer negative consequences of such socialization!

PEER INFLUENCE ON CHILDREN VIOLENT BEHAVIOR

In the literature about school violence, the thesis that peers are an integral part in supporting and maintaining the violent behaviour of children is present more often. Related to this, in the literature can be found some theoretical explanations that make an attempt to explain the causes of peer influence on children violent behaviour. There are few dominant theories that give explanation and suggest that children learn to commit violence by their peers.

The first theory is called homophile (Espelage, Holt, & Henkel, 2003). The concept of this theory is very simple. You can take for example the phrase "birds of a feather flock together." Pupils from higher grades in elementary schools and high schools tend to associate or befriends with peers who are similar to them in terms of behaviours, attitudes and interests (Espelage, Holt, & Henkel, 2003). It is true that some pupils select each other on the basis of similarities in these characteristics, but also is true that peers socialize each other through into acting and behaving a certain way of internalizing the norms of the group. Support for the homophile hypothesis is documented in the literature for violence, which has found that individuals within the same friendship group tend to show a similar level of involvement in violent behaviour (Espelage, Green, & Wasserman, 2007). Simplified, violent children hang out with violent children. But not all peer groups are made up of members who perform violence. Children that have high position in the peer group socialize their friends to engage in violent behaviour. Correspondingly the level of violence within the peer group, is a predictor of adolescent violent behaviour that belonging to that group. (Swearer, Espelage, & Napolitano, 2009). Other theories offer explanations why this effect occurs. The theory of domination is one of them. Developmental psychologists have shown that establishing a higher status in the group provides an opportunity for greater control or influence over other peers (Pellegrini & Long, 2002). Dominant status can be achieved either by affiliative methods (for example, leadership) or antagonistic methods (for example, violence). The need for dominance, raises the question why the presence of violence is changed during the school years, or why typically increases during periods of transition, such as the transition from primary to secondary school. (Pellegrini & Long, 2002) Aggression or violence were long recognized as an important way for establishing dominance in the group and it is often used in these time points in order to establish control over other children. Children who want to establish dominance in the group often choose violence in order to reign in the peer group.

The attraction theory is also particularly relevant for understanding how peers influence on children violent behaviour. This theory assumed that adolescents are attracted to other adolescents who possess characteristics that reflect independence (delinquency, aggression, disobedience) (Bukowski, Sippola, & Newcomb, 2000; Moffitt, 1993) cited in (Swearer, Espelage, & Napolitano, 2009). Admiration for possessing such characteristics, some adolescents makes them to accept their form of behaviour including violence. These authors (Bukowski, Sippola, & Newcomb, 2000) argue that adolescents manage the transition from primary to secondary schools through their attractions to peers who are aggressive. In a study of 217 boys and girls during this transition, Bukowski and colleagues found that girls' and boys' attraction to aggressive peers increased on entry to secondary school. This increase was larger for girls, which is consistent with Pellegrini and Bartini's (2001) finding that, girls nominated "dominant boys" as dates to a hypothetical party. (Swearer, Espelage, & Napolitano, 2009)

Besides these theories which generally explain the negative influence of peers, most of the research suggests that the emphasis of the pressure from the peer group is excessive and that the influence of peers should not be considered always as negative. There is a need to focus also on the positive impact of peers who have normal behaviour, as a mechanism for regulation of the child behaviour. It is certain that there is a high level of conforming to group norms in adolescence, but that conformism refers primarily to the adoption of the principle of friendly relations, as well as the principles of loyalty, trust and support as core values that support social cohesion (Batic 2010). However, how much will be intense the peer influences depend on other factors related to the personal characteristics of the child, which can sometimes create resilience from this influence from peers. Sometimes peers may have compensatory or protective function if children grow up in adverse family circumstances, and in the company of the peers realized the need for belonging, security and acceptance. (Beljanski, 2009)

PEER REACTION ON VIOLENCE

When we considering the question of violence, it is observed from the perspective of those who perform violent behaviour and those who experience violence. But there is one key element that is missing and that are bystanders. What is distinctive about them? Most of the violence in the school generally takes place in front of witnesses, so, for most of the pupils, the scenes of a school violence is something that have been already seen and they consider it an inevitable part of everyday school life. Rigby and Johnson (Rigby and Johnson, 2005) found that practically all pupils in elementary and secondary school have witnessed verbal violence, many of them have witnessed physical violence, and a significant part sexual violence. In a situation when peers found themselves as bystanders/observers, they choose different ways of responding to violence, through inclusion, passive observation or by helping (Rigby & Slee, 1993). According to the different role of peers, they may appear in the role of "assistants" that assist in the violence directly, "supporters" come around and see or laugh until other children perform violence, "defenders" who are trying to stop the violence, and "outsiders" that are not aware of the violence or not interested about it. Having many defenders in the peer group prevents violence, while assistants and supporters can increase its presence. (Doll, Song, & Siemers, 2004) Thus peers can encourage, discourage or tight violence in the class. Based on that, bystanders or observers often indirectly are involved in the process of victimization.

The role of the bystander/observer depends from his/her interaction with the victim or the child that perform violent behaviour (Twemlow & Sacco, 2008). Usually, bystanders/observers have passive role, in terms of the absence of reaction to violence that is happening in front of them, and they often see guilt of those who perform violence and of the victim who allow the violence to continue. But often can be noticed and active role of bystanders/observers by inclination or approval for those who commit violence, because in their eyes, "it is better to lean towards stronger rather than weaker". Sometimes bystanders/observers simply distance themselves from the incident without any reaction, just observe. There are many reasons for this reaction, starting with the fact that some incidents they do not perceive as violence, some observers do not agree with violence, but because of powerlessness or from other reasons avoid to prevent violence or to report the event to an adult in school or family. However, it cannot be underestimated and category of children that often gives help to those who are victims. Most studies that are based on self evaluation of pupils (Whitney & Smith, 1993), on the question what they do when they witnessed peer violence, 54% of pupils in primary schools said that they try to prevent the violence, 27% that they do not do anything, but they thought that they should do something, 19% said that they do not do anything because it does not affect them, and 16% of them said that they join to the attacker. In the survey in primary schools in Greece, the readiness of children for helping was much smaller: when children were asked what they do when they witness bullying/teasing: 28% of children said that they did not join, but enjoy watching, 33, 5% said they were forced to join, and 25, 2% that often accompany the bully, 4, 3% that are trying not to be drawn into the event. Only 4.5% of pupils had told the bully to stop, and 4, 2% called for help from an adult. (Pateraki & Houndoumadi, 2001) Research conducted for doctoral thesis "Violence among children in schools- with special focus on prevention" in 2012 (Jovanova, 2014), indicates that only 35% of pupils from elementary schools (included in the survey) are trying to help those who have been victims of violence, 13 2% said they "do nothing but think that should help", about 2% incline towards those who commit violence, "just watch" around 6% and 2% call an adult from the school (teacher, educator, psychologist). These data are confirmed also in a research in the Republic of Serbia, where it was established that protective behaviour showed 35% (physical protection) to 65% of pupils (verbal protection) when peer is physically assaulted and 23% (physical protection) and 69% (verbal protection) when peer is verbally attacked. Very serious results gathered by the researchers from this study, is that half of the pupils choose the answer "I do nothing even think that I should," and every fourth that "they are not worry about peers troubles." This suggests that children generally have a passive role in the reaction, if it is noticed that only 35% of them are giving help to those who are victims (Plut & Popadić, 2007). This type of reaction, enable violence. Some bystanders/observers accept this type of reaction because of lack of interest, but some have a fear that they can suffer if they try to help (and often tutoring by their parents that it is better to stay away from such events in order not to suffer). Almost all data in this area are based on self evaluation of pupils given in a questionnaire. A try for a different approach is made by group of Canadian researchers, who trough observation examined the situations about school violence with recording the interaction of children from first to sixth grade in natural conditions, in classrooms and in the school yard. In a situation of violence, peers were present and had some role in 85% of cases. Inside the school yard, intervened in 13% of cases when they were present, double frequently happened that they observe what is happening or to join the child who performed violence (Craig & Pepler, 1997). In the classroom, peer intervened in 14% of cases when they were aware of the violence, while teachers intervened in 73% of cases when they saw violence (Atlas & Pepler, 1998). In a study that was conducted with the same methodological approach (Hawkins, Pepler, & Craig, 2001) pupils in the school yard intervened in 19% of cases, and 57% of these interventions were successful.

But it must be emphasized that there is a difference between how peers react and what they feel about violence. According to a study by Rigby and Slee (Rigby & Slee, 1993), 80- 85% of pupils do not support the violence. Moreover, 80% of pupils showed admiration of peers that intervened (Hawkins, Pepler, & Craig, 2001). Charach et al, in the survey from 1995 found that 86% of children felt uncomfortable while watching violence, but that 43% of children said that they will try to help a pupil who is victimized and the other 33% that felt the need to help, but not helped (Manarina, 2003). This suggests that peers do not justify violence, but do not intervene because of various reasons. The role of peers and their way of response can be influenced by various factors (including: the form of violence, the situation, the age of those who are involved in the violence, etc.). How will react the bystander/observer depend largely from the social context, circumstances and conditions in which violence occurs. If there are significant differences in power between pupils, is it expected bystanders/observers to withdraw and not to react whether they think that violence is wrong! In situations of passive observation of individual, bystanders/observers may see themselves as the audience who see and reacts to the game. If there is no audience, there will be no game. From this perspective, often those who do violence and victims will perform what bystanders/observers will permit (Twemlow & Sacco, 2008).

Based on these findings, one of the most important factors in the creation of prevention of school violence should be peers and their proper reaction as witnesses of violence. The difference between how peers act in violent situations and their views of the violence may be the key to establishing a positive intervention strategies based on peers proper reaction. With educating of peers for understanding of what means violence, what consequences produce it, to develop empathy in relation to the victim and to take action against violence, the difference between the actions of peers and their attitudes towards violence can be reduced. Consequently, successful interventions in schools must focus on the transformation of bystanders/observers into active witnessed. Whatever program we use, there is a need for identifying those bystanders/observers that can be used as part of a reduction of school violence, with which the chances for program to be effective will increase.

THE PEER ROLE IN PREVENTION OF SCHOOL VIOLENCE IN THE REPUBLIC OF MACEDONIA

One of the most important principles of all preventive policies is the active participation of pupils in the whole process of creating programs and their implementation and modification. In the whole process of creating and implementing of prevention programs, can be emphasize that without appropriate, active participation of children, all efforts would be futile. This principle is defined in the Strategy for reducing violence in schools, in which is noted that should be respected "the active participation and cooperation of all stakeholders in the educational process in the development and maintenance of a safe school environment that respects differences from any kind", adding that the pupils will be involved in the creation of school programs to reduce violence (Strategy for reducing violence in schools 2012-2015). Related to this, the Strategy proposes a number of activities for encouraging and emphasis of active approach of pupils, because it is about their rights, responsibilities, needs, feelings and welfare. Based on this, Strategy provides:

- Pupils must be familiar with their rights and the rights of their peers, teachers, family members and members of their community (UNICEF, Bureau for Development of Education, Algorithm, p. 13). These activities should be carried out through various modalities, such as role play, discussion, in order to understand the true meaning of human rights.
- Pupils must be actively involved in setting the rules of the game in the school, in terms of what behaviours are good and which are wrong, what are the rules and responsibilities in order to establish harmony in the school and a positive school climate. They should participate in the creation of a Code of Conduct that would put a clear position of pupils and rights and responsibilities of all. (UNICEF, Bureau for Development of Education, Algorithm, p.13)

When it comes to activities in the Action Plan, proposed in the Strategy (in the section "Reduction of school violence") is stated that the during the process of creation of the Action Plan for reduction of school violence, pupils are underline as one of the key partners in this activity (besides school employees, Bureau for development of Education, parents and representatives of local government). Especially is emphasized their role in the "Developing of school program for reducing of violence, promotion of a culture of coexistence and increasing the school safety", in process of "Creating a school protocol for intervention" and in the "Implementation of the school program and the protocol".

The principle of active involvement of pupils in each phase of the implementation of certain activities is significant and is especially noticeable in the Strategy for the reducing violence in school. The question is how much of these activities will be carried out and whether pupils will be really are equal partners with

other partners in the implementation of the activities! Moreover when we talk about active role of pupils we speak about true and real participation and contribution, not only fulfilling the formal point of presence of pupils in their realization.

Special emphasis and responsibility is given to pupils as subjects that should actively contribute in the reduction of violence through appropriate response. But to have active pupils and their appropriate response to possible violence in schools, it is necessary to fulfil some conditions. Within the schools in the Republic of Macedonia, except those included within the project "Prevention of violence in schools" funded by UNICEF Office in Skopje, in others, workshops and lectures for violence is left to the will of professional personnel in school. According to the findings, without effective implementation of workshops and lectures for rising of awareness of children about violence, understanding the impact of violence, the need for their reaction to it, children/pupils will not be able to recognize their role and place in the prevention of violence in schools.

CONCLUSION

The peer influences on the children behaviour is an issue of special interest. If in the theory is confirmed the thesis that peers are a medium for learning in the process of socialization of adolescents, then their influence on children violent behaviour is especially important. The influence of peers can be negative or positive, depending of the peer group and its accepted norms of behaviour. Peers can have a positive impact on the behaviour of children, but only if they have positive characteristics, attitudes, behaviours and an appropriate response to violence in school. The rejection of the child by the peers, rebuke or putting on the side of the victim of violence, can be a factor that can influence on prevention of performing violence by child in and outside of school. Encouraging active role of peers in order that they can be promoters of good behaviour of their peers, is a priority in any preventive policies and programs related to school violence. This foundation for active participation and reaction of peers against children violent behaviour, should be promoted not only in schools, but also supported and practiced by parents because education of their children to appropriate reaction when he finds himself in the role of bystander/observer of violence, may be a step towards ensuring the proper conduct and protection of their one child possible future violent behaviour.

REFERENCES

1. Beljanski, M. (2009). Predlog programa prevencije u oblasti nasilja među vršnjacima. (R. Grandić, Ур.) Pedagoška stvarnost, 55 (7-8), 713-734.
2. Doll, B., Song, S., & Siemers, E. (2004). Classroom Ecologies That Support or Discourage Bullying. Bo S. M. Swearer, & D. L. Espelage (Ур.), Bullying in American schools: a social-ecological perspective on prevention and intervention (стр. 161-184). New Jersy: Lawrence Erlbaum Associates, Inc., Publishers.
3. Espelage, D. L., Green, H. J., & Wasserman, S. (2007). Statistical analysis of friendship patterns and bullying behaviours among youth. Bo L. Hanish, & P. Rodkin (Ур.), Peer social networks New directions for child and adolescent development (стр. 61-75). San Francisco: Jossey-Bass.
4. Espelage, D. L., Holt, M. K., & Henkel, R. R. (2003). Examination of peer-group contextual effects on aggression during early adolescence. Child Development (74), 205-220.
5. Hanish, L. D., Kochenderfer-Ladd, B., Fabes, R. A., Martin, C. L., & Denning, D. (2004). Bullying Among Young Children: The Influence of Peers and Teachers. Bo D. L. Espelage, & S. M. Swearer (Ур.), Bullying in American schools: a social-ecological perspective on prevention and intervention (стр. 141-160). New Jersey: Lawrence Erlbaum Associates, Inc., Publishers.
6. Pateraki, L., & Houndoumadi, A. (2001). Bullying among primary school children in Athens, Greece. Educational Psychology (21), 167-175.
7. Pellegrini, A. D., & Long, J. (2002). A longitudinal study of bullying, dominance, and victimization during the transition from primary to secondary school. l. British Journal of Developmental Psychology (20), 259–280.
8. Plut, D., & Popadić, D. (2007). Reagovanje dece i odraslih na školsko nasilje. (S. Ševkušić, Ур.) Zbornik Instituta za pedagoška istraživanja , 39 (2), 347-366.
9. Rigby, K., & Slee, P. (1993). Dimensions of interpersonal relation among Australian children and implications for psychological well-being. Journal of School Psychology (133), 33-42.

10. Swearer, S. M., Espelage, D. L., & Napolitano, S. A. (2009). Bullying prevention and intervention: realistic strategies for schools. New York: The Guilford Press.
11. Twemlow, S. W., & Sacco, F. C. (2008). Why school antibullying programs don't work. Plymouth: Jason Aronson.
12. Whitney, I., & Smith, P. K. (1993). "A survey of the nature and extent of bullying in primary and secondary schools. Educational Research (35), 34-39.
13. Батиќ, Д. (2010). Фактори на ризик и фактори на заштита на малолетничкото престапништво (индивидуални и семејни фактори). Годишник на Факултет за безбедност-Скопје, стр. 263-272.
14. Јованова, Н. (2014). Насилство меѓу децата во училиштата- со посебен осврт на превенцијата. докторска дисертација, Факултет за безбедност-Скопје

UDC: 343.971:177.82(497.7)
343.97:316.647.8(497.7)

THE CIRCULUS VITIOSUS OF HATE AND CRIME: HATE CRIMES AND THE CASE OF THE REPUBLIC OF MACEDONIA

Angelina Stanojoska[1]
University St.Climent Ohridski, Bitola, Faculty of Law, Kicevo

Abstract: Always connected to the dark side of humans, hate has been reason for many mistakes during human existence. It has been known as a trigger for wars, but also as a starting point for individual activities. On the other hand, human nature and choices through life are predictors of how many and how different characteristics a human being will "wear" through his/her existence. And although every day we proclaim equality among people, every day people are discriminated because of something. Their colour of skin, their ethnical origin, gender, sexual orientation, religious views… These and other "differences" very often are used as reasons for justifying criminal acts. Killers justify their brutality with someone's different colour of skin or something else.

The deaths of Matthew Shepard and James Bird are not the only ones, but were the ones that awoke American society and opened the question of existence of hate crimes. Today, although societies are becoming more modern with every moment that passes, humans become more brutal. Hate crimes and discrimination happen more often, with a goal to deliver a message to the "different" and tell them they are not accepted and welcomed.

The paper includes short historical review of hate crimes, their beginning, legal solutions, and criminological characteristics. It also gives an overview of Macedonian situation through numbers given by the Helsinki Committee of human rights.

Keywords: characteristics, difference, discrimination, hate crime, incrimination, Macedonia.

INTRODUCTION THE CONCEPT OF HATE CRIMES

Hate crimes are a concept which is known to society for a long time, although as such until lately did not have the place and interest it deserved. Explaining the meaning of hate crimes, we could state that it is mainly a criminological concept; because of the acts it can be realized in.

The term hate crimes analyzed from logical and terminological side explains something the starting point of which is hate, but also the existence of such a term brings on the other hand (maybe) the need of having something opposite, such as crimes of love (something like this could be euthanasia).[2]

Hate crimes are criminal acts committed with a bias motive. It is this motive that makes hate crimes different from other crimes. A hate crime is not one particular offence. It could be an act of intimidation, threat, property damage, assault, murder or any other criminal offence.[3] Written like this, as we mentioned previously, hate crimes are rather a concept, than a group of crimes for which we can give a legal definition.

Prejudice or bias can be broadly defined as preconceived negative opinions, intolerance or hatred directed at a particular group. The group must share a common characteristic that is immutable or fundamental, such as "race", ethnicity, language, religion, nationality, sexual orientation, or other characteristic.[4]

A criminal act is a hate crime if it is motivated by bias or prejudice. The use of the word "hate" can mislead people into thinking that the defendant must hate the victim or the victim's group for a criminal act to be considered a hate crime. This is not the case. The factor that turns an ordinary crime into a hate crime is the perpetrator's selection of a victim based on a bias or prejudice about the group to which the victim belongs. The term "bias-motivated crimes" is, therefore, used in this guide interchangeably with "hate crimes". The term "discriminatory crimes" can also be used to emphasize that hate crimes are an extreme form of discrimination. Hate crime laws use different terms to establish bias motives, and do not always use

1 angiest22@gmail.com
2 Ciric, Jovan. "Zlocini mrznje - americko i balkansko iskustvo" *TEMIDA 4 (2011): 21-22*
3 OSCE (ODIHR). *Hate Crimes Laws: A Practical Guide.* (2009): 16
4 OSCE (ODIHR). *Preventing and responding to hate crimes: A resource guide for NGO's in the OSCE region. (2009): 15*

the word "hate". Some laws refer to "motives of hostility"; others do not refer to any emotional state of the defendant, but simply penalize crimes where the victim is *selected* due to their group characteristic.[5]

Using the word *hate* before *crime* does not mean that the offender hated the victim. It is used to connect the crime with some characteristic of the victim or the group he/she belongs to; and as such give a severe characteristics to the crimes. This is one of the differences between hate and ordinary crimes. The other one is because of their symbolism. Namely, the impact it makes to the victims is connected with his or her membership to a given groups.

Unlike victims of many other criminal acts, hate crime victims are selected on the basis of *what* they represent rather than *who* they are. The message that is conveyed is intended to reach not just the immediate victim but also the larger community of which that victim is a member.[6]

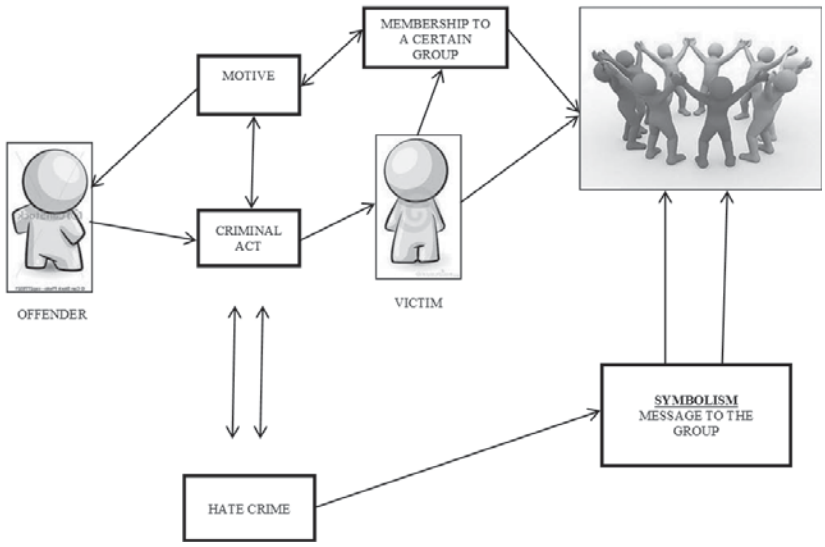


Figure 1 *The Circulus Vitiosus of hate and crime*

These crimes are always committed with one goal, which is intimidation of the victim (if he/she survives) and intimidation of the group or the community where the victim belongs (based on his/her characteristics). It is fuelled by motives based on hate which comes from those characteristics and ends as a symbolic act that delivers a message.

Group characteristics are often apparent or noticeable to others, such as language, gender or ethnicity, and are often immutable; they cannot be changed by a decision of the bearer. Therefore, if an offender targets wealthy people for theft, such cases would not be recognized as hate crimes. This is because wealth is not a characteristic that creates a shared group identity, nor is it a deep and fundamental part of a person's identity in the same way as race or religion. By contrast, crimes that target victims because of their national origin, for example, would be hate crimes.[7]

Hate crimes can be committed for one of a number of different reasons:

– The perpetrator may act for reasons such as resentment, jealousy or a desire for peer approval;
– The perpetrator may have no feelings about the individual target of the crime but have hostile thoughts or feelings about the group to which the target belongs;
– The perpetrator may feel hostility to all persons who are outside the group in which the perpetrator identifies himself or herself; or
– At an even more abstract level, the target may simply represent an idea, such as immigration, to which the perpetrator is hostile.[8]

Race and racism, ethnicity, national origin and nationality, xenophobia, homophobia, transphobia, religion and belief, sex and gender, are some of the most found reasons of hate crimes. All of them in most countries are defined as grounds of discrimination and possible victims of hate crimes are protected by actual laws of those countries.

5 OSCE (ODIHR). *Prosecuting Hate Crimes: A Practical Guide (2014): 20*
6 OSCE (ODIHR). *Hate Crimes Laws: A Practical Guide.* (2009): 17
7 OSCE (ODIHR). *Prosecuting Hate Crimes: A Practical Guide (2014): 21*
8 OSCE (ODIHR). *Hate Crimes Laws: A Practical Guide.* (2009): 18

THE TRANSFORMATION OF AMERICAN LAWS: BEING WHO YOU ARE IS THE REASON

In the pre-dawn hours of June 7, 1998, Byrd was walking home in Jasper, Texas, when he was stopped by three white men who offered him a ride home. Byrd got in the bed of their pick-up truck, but the men did not take him home. Instead, they drove him to a desolate, wooded road east of town, beat him severely, chained him to the back of the truck by his ankles and dragged him for more than three miles. The murderers drove on for another mile before dumping his torso in front of an African-American cemetery in Jasper. Byrd's lynching-by-dragging gave impetus to passage of a Texas hate crimes law.[9]

Four months later, horrific events that took place shortly after midnight on October 7, 1998 would become one of the most notorious anti-gay hate crimes in American history and spawned an activist movement that, more than a decade later, would result in passage of the Matthew Shepard and James Byrd Jr. Hate Crimes Prevention Act, a federal law against bias crimes directed at lesbian, gay, bisexual or transgendered people. Two men, Aaron McKinney and Russell Henderson, abducted Matt and drove him to a remote area east of Laramie, Wyoming. He was tied to a split-rail fence where the two men severely assaulted him with the butt of a pistol. He was beaten and left to die in the cold of the night. Almost 18 hours later, he was found by a bicyclist who initially mistook him for a scarecrow.[10]

Matt died on October 12 at 12:53 a.m. at Poudre Valley Hospital in Fort Collins, Colorado with his family by his side. His memorial service was attended by friends and family from around the world and garnered immense media attention that brought Matt's story to the forefront of the fight against bigotry and hate.[11]

Renamed the Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act upon its passage by the House in 2009, the piece of legislation took eleven years of softening-up, and ultimately passed by being an amendment to the National Defense Authorization Act of 2009. But the Matthew Shepard Act's fate was sealed independent of the horrific focusing event. Intrinsic in the law binding the previous policy subcommittee together[12] was dynamic democratization, a tendency toward inclusiveness pervasive in the mores of the political culture. The ideas within the solution stream needed nothing other than time to formulate themselves into the noetic vocabulary of the age, making policy propagation characteristically different than legislation in a field requiring technicality and expertise; essentially, these ideas were available pieces of politics. All that remained missing was the self-evident problem, a symbol that could carry the accompaniment of the national tide. The Matthew Shepard Act had a popular policy image shaped by a captivating causal story: Americans owe the LGBT community, or Shepard himself, a step toward protection from hate crimes.[13]

"You understood that we must stand against crimes that are meant not only to break bones, but to break spirits - not only to inflict harm, but to instill fear. You understand that the rights afforded every citizen under our Constitution mean nothing if we do not protect those rights - both from unjust laws and violent acts. And you understand how necessary this law continues to be.[14]And that's why, through this law, we will strengthen the protections against crimes based on the colour of your skin, the faith in your heart, or the place of your birth. We will finally add federal protections against crimes based on gender, disability, gender identity, or sexual orientation. And prosecutors will have new tools to work with states in order to prosecute to the fullest those who would perpetrate such crimes. Because no one in America should ever be afraid to walk down the street holding the hands of the person they love. No one in America should be forced to look over their shoulder because of who they are or because they live with a disability."[15]

The Act creates a new federal criminal law which criminalizes wilfully causing bodily injury (or attempting to do so with fire, firearm, or other dangerous weapon) when:

(1) the crime was committed because of the actual or perceived race, colour, religion, national origin of any person, or (2) the crime was committed because of the actual or perceived religion, national origin, gender, sexual orientation, gender identity, or disability of any person and the crime affected interstate or foreign commerce or occurred within federal special maritime and territorial jurisdiction.[16]

9 http://www.adl.org/imagine/james-byrd-jr.html [07.12.2014]
10 http://www.matthewshepard.org/our-story/matthews-story [07.12.2014]
11 Ibid
12 18 USC § 245 of the 1968 Civil Rights Act, which permits federal prosecution for hate crimes motivated by race, color, religion, or national origin against a victim participating in a federally protected "state or local activity" (Jacobs and Potter 1998, 38).
13 Daniel Semelsberger. The Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act:Irresistible Movement of a Social Construct. p.2; available at https://www.academia.edu/7563692/The_Matthew_Shepard_and_James_Byrd_Jr._Hate_Crimes_Prevention_Act_Irresistible_Movement_of_a_Social_Construct [06.12.2014]
14 http://www.whitehouse.gov/the-press-office/remarks-president-reception-commemorating-enactment-matthew-shepard-and-james-byrd- [04.12.2014]
15 Ibid
16 http://www.justice.gov/crt/about/crm/matthewshepard.php [06.12.2014]

The newly enacted § 249 has three significant subsections. Subsection (a) (1) criminalizes violent acts (and attempts to commit violent acts undertaken with a dangerous weapon) when those acts occur because of the actual or perceived race, colour, religion, or national origin of any person. This section of the statute has a broader reach than existing hate crime statutes. (18 U.S.C. § 245, for example, requires that government prove not only that the crime was motivated by animus but also because of the victim's participation in one of six enumerated federally protected activities). Section 249(a) (1) was passed pursuant to Congress's Thirteenth Amendment authority to eradicate badges and incidents of slavery. **The government need prove no other "jurisdictional" element to obtain a conviction.** Subsection (a) (2) of § 249 protects a wider class of victims. Subsection (a) (2) criminalizes acts of violence (and attempts to commit violent acts undertaken with a dangerous weapon) when motivated by the actual or perceived gender, disability, sexual orientation, or gender identity of any person. It will also apply to violent acts motivated by animus against those religions and national origins which were not considered to be "races" at the time the Thirteenth Amendment was passed. This portion of the statute was passed pursuant to Congress's Commerce Clause authority. **Thus, to obtain a conviction, the government must prove that the crime was in or affected interstate or foreign commerce.** Subsection (a) (2) (B) of the statute contains a detailed description of the ways the commerce clause element may be fulfilled. Subsection (a)(3) of § 249 provides for prosecution of crimes committed because of any of the characteristics defined in (a)(1) or (a)(2), whenever such crimes occur within the Special Maritime and Territorial Jurisdiction (SMTJ) of the United States.[17]

The statute criminalizes only violent acts resulting in bodily injury or attempts to inflict bodily injury, through the use of fire, firearms, explosive and incendiary devices, or other dangerous weapons. The statute does not criminalize threats of violence. Threats to inflict physical injury may be prosecutable under other hate crimes statutes, such as 42 U.S.C. § 3631 or 18 U.S.C. § 245. **Such threats may also be prosecutable under generally applicable federal laws preventing interstate communication of threats.[18]**

"At root, this isn't just about our laws; this is about who we are as a people. This is about whether we value one another - whether we embrace our differences, rather than allowing them to become a source of animus. It's hard for any of us to imagine the mind-set of someone who would kidnap a young man and beat him to within an inch of his life, tie him to a fence, and leave him for dead. It's hard for any of us to imagine the twisted mentality of those who'd offer a neighbour a ride home, attack him, chain him to the back of a truck, and drag him for miles until he finally died. But we sense where such cruelty begins: the moment we fail to see in another our common humanity -- the very moment when we fail to recognize in a person the same fears and hopes, the same passions and imperfections, the same dreams that we all share."[19]

Incidents, Offenses, Victims, and Known Offenders

by Bias Motivation, 2012[1]

Bias motivation	Incidents	Offenses	Victims	Known offenders
Total	5.796	6.718	7.164	5.331
Single-Bias Incidents	5.790	6.705	7.151	5.322
Race:	2.797	3.297	3.467	2.822
Anti-White	657	739	763	756
Anti-Black	1.805	2.180	2.295	1.771
Anti-American Indian/Alaskan Native	101	109	115	92
Anti-Asian/Pacific Islander	121	134	143	119
Anti-Multiple Races, Group	113	135	151	84
Religion:	1.099	1.166	1.340	484
Anti-Jewish	674	696	836	232
Anti-Catholic	70	79	86	27
Anti-Protestant	33	34	35	24
Anti-Islamic	130	149	155	110

17 Ibid
18 Ibid
19 http://www.whitehouse.gov/the-press-office/remarks-president-reception-commemorating-enactment-matthew-shepard-and-james-byrd- [04.12.2014]

Anti-Other Religion	92	107	115	36
Anti-Multiple Religions, Group	88	89	101	44
Anti-Atheism/Agnosticism/etc.	12	12	12	11
Sexual Orientation:	1.135	1.318	1.376	1.281
Anti-Male Homosexual	605	720	741	754
Anti-Female Homosexual	146	162	175	116
Anti-Homosexual	321	369	393	358
Anti-Heterosexual	24	26	26	20
Anti-Bisexual	39	41	41	33
Ethnicity/National Origin:	667	822	866	639
Anti-Hispanic	384	488	514	393
Anti-Other Ethnicity/National Origin	283	334	352	246
Disability:	92	102	102	96
Anti-Physical	18	20	20	16
Anti-Mental	74	82	82	80
Multiple-Bias Incidents	6	13	13	9

Incidents, Offenses, Victims, and Known Offenders

by Offense Type, 2012[2]

Offense type	*Incidents*	*Offenses*	*Victims*	*Known offenders*
Total	**5.796**	**6.718**	**7.164**	**5.331**
Crimes against persons:	**3.258**	**3.968**	**3.968**	**3.948**
Murder and no negligent manslaughter	5	10	10	5
Forcible rape	15	15	15	18
Aggravated assault	644	854	854	1.011
Simple assault	1.336	1.570	1.570	1.697
Intimidation	1.230	1.489	1.489	1.182
Other	28	30	30	35
Crimes against property:	**2.547**	**2.547**	**2.993**	**1.413**
Robbery	126	126	149	251
Burglary	142	142	174	145
Larceny-theft	258	258	281	166
Motor vehicle theft	23	23	24	8
Arson	38	38	46	37
Destruction/damage/vandalism	1.906	1.906	2.263	757
Other	54	54	56	49
Crimes against society	**203**	**203**	**203**	**243**

Analyzing the US statistics for 2012, regarding hate crimes, we may conclude that this crime is mostly connected to crimes against person and crimes against property, attacking either the person who is part of the group either their property; and of course through those attacks sending a message.

HATE CRIMES AND INSTITUTION'S REACTION: THE CASE OF THE REPUBLIC OF MACEDONIA

On the territory of Europe, hate crimes are part of the interest of the OSCE, which publishes reports yearly. Reports contain information regarding hate crimes and hate speech in the member countries. Using those statistics, the OSCE through the ODIHR tackles various levels of state framework and assists participating states in their efforts to prevent and suppress hate crimes. The ODIHR organizes police training, supports law makers and also organizes trainings for judges and prosecutors. Also the part of those efforts are intergovernmental organizations and NGO's and other parts of civil society as most important part of the chain, because they play an important role in monitoring and reporting incidents, support victims and work on raising awareness in society.

Beings participating country of the OSCE, the Republic of Macedonia has committed it to pass legislation that provides for penalties that take into account the gravity of hate crime, to take action to address under-reporting, and to introduce or further develop capacity-building activities for law enforcement, prosecution and judicial officials to prevent, investigate and prosecute hate crimes. Specifically, Macedonia has repeatedly committed itself to collect, maintain and make public the reliable data on hate crimes, across the criminal justice system from the police to the courts. In recent years, participating states and also Macedonia have consolidated their commitments on hate crime in recognition of the importance of a comprehensive approach in addressing the many facets of the problem.[20]

In the Criminal Code of our country, still there is no article which directly incriminates the hate crime acts. Instead of it, hate crimes can be:

- Aggravating circumstances - Article 39(5) of the Criminal Code of the Republic of Macedonia: (5) When determining the sentence, the court shall especially consider whether the crime has been committed against a person or group of persons or property, directly or indirectly, because of his/hers sex, race, colour of skin, gender, belonging to a marginalized group, ethnic origin, language, citizenship, social origin, religion or religious belief, other beliefs, education, political adherence, private or social status, mental or physical disability, age, family and marital status, property status, health condition, or any other ground provided in law or ratified international agreement.[21]

- Endangering security - Article 144 (4) of the Criminal Code of the Republic of Macedonia:

(4) Whosoever, by means of information system threatens to commit a crime, being subject to prescribed imprisonment of five years or more serious sentence, against a person because of their belonging to specific sex, race, colour of skin, gender, belonging to a marginalized group, ethnicity, language, citizenship, social background, religion or religious belief, other beliefs, education, political affiliation, personal or societal status, mental or physical disability, age, family or marital status, property status, health condition, or on any other ground established with law or ratified international agreement, shall be sentenced to imprisonment from one to five years.[22]

- Causing of hate, discord or intolerance on national, racial, religious and other discriminatory ground – Article 319 of the Criminal Code of the Republic of Macedonia:

(1) Whosoever by force, maltreatment, endangering the security, mocking of the national, ethnic, religious and other symbols, by burning, destroying or in any other manner damaging the flag of the Republic of Macedonia or flags of other states, by damaging other people's objects, by desecration of monuments, graves, or in any other discriminatory manner, directly or indirectly, causes or excites hatred, discord or intolerance on grounds of gender, race, colour of the skin, membership in marginalized group, ethnic membership, language, nationality, social background, religious belief, other beliefs, education, political affiliation, personal or social status, mental or physical impairment, age, family or marital status, property status, health condition, or in any other ground foreseen by law on ratified international agreement, shall be sentenced to imprisonment of one to five years.[23]

20 http://hatecrime.osce.org/what-do-we-know [22.12.2014]
21 Article 39 (5) of the Criminal Code of the Republic of Macedonia, Official Gazette of the Republic of Macedonia, N.37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7 /08 , 139/08 , 114/09, 51/11, 135/11, 185/2011, 142/2012, 166/2012, 55/2013
22 Article 144 (4) of the Criminal Code of the Republic of Macedonia, Official Gazette of the Republic of Macedonia, N.37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7 /08 , 139/08 , 114/09, 51/11, 135/11, 185/2011, 142/2012, 166/2012, 55/2013
23 Article 319 of the Criminal Code of the Republic of Macedonia, Official Gazette of the Republic of Macedonia, N.37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7 /08 , 139/08 , 114/09, 51/11, 135/11, 185/2011, 142/2012, 166/2012, 55/2013

The official state statistics does not contain data about crimes which at the end can be characterized as hate crimes. The same situation can be seen at the official site of the ODIHR[24] (Hate Crime Reporting).

The only source for the time being is the Internet site of the Helsinki Committee for Human Rights of the Republic of Macedonia. It is an Internet site[25] where everyone can learn basic information for hate crimes, find information of the situation in Macedonia; also everyone can report a hate crime or an incident based on bias.

This site contains statistical data for every incident and hate crimes which happened between February 2013 and December 2014.

Figure 2 *Hate crimes and incidents in the Republic of Macedonia (February 2013 - December 2014)*
Source: http://www.zlostorstvaodomraza.mk/main?l=en_US [22.12.2014]

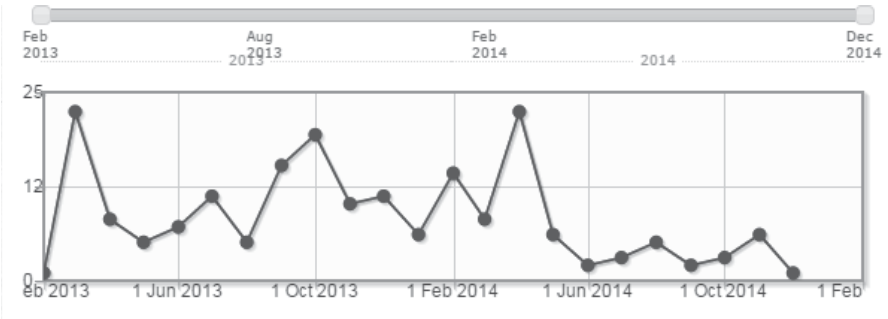


Figure 3 *Dynamics of hate crimes and incidents in the Republic of Macedonia (February 2013 - December 2014)*
Source: http://www.zlostorstvaodomraza.mk/main?l=en_US [22.12.2014]

The above statistics shows that between the beginning of 2013 and the end of 2014, 192 incidents happened. Most of the them are incidents due to ethnical belonging, citizenship or language 143, then 22 incidents are connected to causing national, racial or religious hate, discord or intolerance; 21 were incidents due to political affiliation or political belief; 18 due to religious affiliation or religious belief; 9 due so sexual orientation or gender identity; 8 were incidents on a sport match; 6 were injuries of the right of equality and 1 incident was due to racial or other discrimination.

We also should mention that this is not an official statistics and not all of those 192 incidents are verified as incidents of hate or hate crimes. But it is a good starting point for some future collecting of data regarding this crime.

Also to the ODIHR, for 2013, the Macedonian Helsinki Committee reported ten physical assaults by groups of attackers causing serious injuries and often involving weapons, including knives and sticks, as well as 46 physical assaults, five of which caused serious injuries. Victims of the assaults were either eth-

24 http://hatecrime.osce.org/former-yugoslav-republic-macedonia [22.12.2014]
25 http://www.zlostorstvaodomraza.mk/main [22.12.2014]

nic Albanians or ethnic Macedonians. In addition, the Committee reported 20 incidents of damage to property, including 13 incidents in which stones were thrown at buses or trains, several of which resulted in injuries, and an unspecified number of additional incidents targeting objects affiliated with ethnic groups. The Committee also reported two incidents of racist graffiti, one each on an Orthodox church and a mosque. ILGA-Europe and the LGBT Support Centre reported five incidents of damage to property, including against community centres and personal property; one incident of threats by a group against a group of LGBT activists; and two physical assaults resulting in serious injuries against transgender people, including one carried out by a group. The organizations also reported an arson attack against an LGBT support centre.[26]

The OSCE Mission to Skopje and the Macedonian Helsinki Committee reported a series of incidents of damage to property against the LGBT Support Centre in Skopje, including damage to the door and windows, one attack against the centre that put at risk the staff present at the time, and a separate arson attack. The Macedonian Helsinki Committee reported further three incidents of damage to property, including one additional attack against the LGBT Support Centre during gay pride week; a series of physical assaults against LGBT activists by a group, and a further physical assault against a gay man by a group; and one incident where a group of people threw stones at the house of a well-known LGBT rights activist.[27]

From the intergovernmental organizations, the OSCE Mission to Skopje reported one physical assault against an ethnic Macedonian boy and several additional assaults against ethnic Albanians; several incidents of vandalism; one attempted arson attack against an ethnic Albanian settlement; one incident of vandalism against the statue of a historical Serbian leader; one incident of damage to property against agriculture facilities owned by ethnic Albanians; and several incidents of vandalism to cars owned by ethnic Albanians. The Mission did not provide specific numbers in some cases. The International Organization for Migration (IOM) reported that swastikas and fascist graffiti were drawn on the buildings in the town of Bitola on the anniversary of the deportation of Macedonian Jews to the Nazi extermination camp at Treblinka. The OSCE Mission to Skopje reported a series of incidents of damage to property against the LGBT support centre in Skopje, including damage to the door and windows, an attack against the centre that put at risk the staff present at the time and one arson attack. These incidents were also reported by the Macedonian Helsinki Committee.[28]

CONCLUSION

"Of all crimes, hate crimes are most likely to create or exacerbate wider tensions, and these in turn, can trigger larger, community-wide conflict, civil disturbances and acts of violence." - Ambassador Janez Lenarčič, former ODIHR Director

1) Hate crimes are a concept which deeply widens the phenomenon of crime, making crime to be used as *instrumentum operandi* for real action based on bias;
2) The Republic of Macedonia does not have criminal incriminations which directly incriminate actions of hate crime and hate speech. The criminal acts are either aggravating circumstances or are parts of other crimes (as their qualified parts). Having a legal concept and criminal framework for suppressing these crimes is an important step in their prevention;
3) Not having national statistical data on the problem causes a gap and darkness of the real situation. Only using the data given by NGOs or IGOs is the first step, but not enough for building preventive strategies;
4) Not knowing the characteristics of perpetrators and only making guesses which are mostly target groups and what kinds of crimes are based on bias also does not help in promoting campaigns for suppressing intolerance in every way;
5) As a domino effect to conclusions 4 and 5 comes out the one that is about informational campaigns and work on suppressing intolerance and proclaiming of coexistence;
6) Not cooperating with the ODIHR regarding yearly reports is not good for the image of the state and its position in Europe;
7) The fact that the situation with hate crimes can only be seen by usage of NGOs statistics makes other see Macedonia as weak and non-serious partner in action against this crime.

26 Hate Crime Report for 2013, http://hatecrime.osce.org/infocus/2013-hate-crime-reporting-now-available [22.12.2014]
27 Ibid
28 Ibid

REFERENCES

1. Ciric, Jovan. "Zlocini mrznje - americko i balkansko iskustvo" TEMIDA 4 (2011): 21 - 36;
2. Criminal Code of the Republic of Macedonia, Official Gazette of the Republic of Macedonia, N.37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7 /08 , 139/08 , 114/09, 51/11, 135/11, 185/2011, 142/2012, 166/2012, 55/2013;
3. Hate Crime Report for 2013, available at http://hatecrime.osce.org/infocus/2013-hate-crime-reporting-now-available;
4. Ignjatovic. Djordje. "Pojam i etiologija nasilnickog kriminaliteta". *CRIMEN 2(2011):* 179 - 211;
5. Kovacevic. Milica. "Zlocini mrznje i normativno regulisanje" TEMIDA 4 (2011): 55 - 66;
6. Nikolic - Ristanovic. Vesna. Slobodanka Konstantinovic - Vilic. Miomira Kostic. *Kriminologija.* Beograd, 2010;
7. OSCE (ODIHR). *Hate Crimes Laws: A Practical Guide.* 2009;
8. OSCE (ODIHR). *Preventing and responding to hate crimes: A resource guide for NGO's in the OSCE region. (2009);*
9. OSCE (ODIHR). *Prosecuting Hate Crimes: A Practical Guide.* 2014*;*
10. Semelsberger. Daniel. The Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act:Irresistible Movement of a Social Construct.
11. https://www.academia.edu/7563692/The_Matthew_Shepard_and_James_Byrd_Jr._Hate_Crimes_Prevention_Act_Irresistible_Movement_of_a_Social_Construct;
12. Tripkovic. Milena. "Ekspanzija mrznje: Osnovnih obelezja masovnih zlocina mrznje" TEMIDA 4 (2011): 37 - 54.

Internet sources

1. http://www.zlostorstvaodomraza.mk/main
2. http://hatecrime.osce.org/former-yugoslav-republic-macedonia
3. http://www.whitehouse.gov/the-press-office/remarks-president-reception-commemorating-enactment-matthew-shepard-and-james-byrd-
4. http://www.justice.gov/crt/about/crm/matthewshepard.php
5. http://www.matthewshepard.org/our-story/matthews-story
6. http://www.adl.org/imagine/james-byrd-jr.html

UDC: 338.124.4
343.9.02

LEADING INDUSTRY OF ECONOMICAL CRISES: ORGANIZED CRIME? – INTERWEAVING OF MARKET ECONOMY AND ORGANIZED CRIME THROUGH THE CASE OF JÓZSEF STADLER -

Tamas Bezsenyi[1]

National University of Public Service, Faculty of Law Enforcement, Department of Management Science

Abstract: The following research based on a tight cooperation with Pest County Police Headquarters, the National Bureau of Investigation where I analyzed criminal files about organized crime gangs after the regime change. The main question of the research was: what sociological and economical factors contributed to the strengthening of organized crime in Hungary? Where can we discover the responsibility of the state? How state regulation affected organized crime?

The present days' organized crime roots from illegal criminal groups which existed in the socialist period. Thanks to the liberal economic reforms in 1981 the second economy had a great economic potential during the socialist period. Organized criminal groups often invested in private sector, thus corporate crime became linked to organized crime. Due to their better economic conditions the criminal networks could establish a different kind of private ventures, like restaurants, pubs or tobacco shops.

After the declaration of democracy many organized crime networks took advantage of regulatory gaps. They preserved their status and informal capital from the second economy. Due to the economical change the new entrepreneurs were informally forced to borrow capital from organized crime groups, or they used these groups' money to recover their debts. They could not turn to court because of their illegal transactions. Other organized crime networks misused government subsidies and created semi-firms, which could operate successfully due to the problems of state control.

The case of József Stadler – an entrepreneur from Akasztó – became one of the most iconic cases of the 1990s, calling the attention of the wider public to the deficiencies of the newly emerging market economy in Hungary. The following analysis aims to showcase that the entrepreneur from Akasztó was capable of becoming a successful businessman during the 1990s. Owing to a weak culture of investigative journalism and a lack of knowledge about economic crimes, Mr. Stadler was and still is often portrayed as a simple tax evader by the media, although he is much more than that. Based on the case study about Stadler, I would like to describe the connection among the actors of market economy and organized crime gangs.

My research seeks to show that during the third Hungarian Republic from the 1990s' organized crime groups have worked with the help of entrepreneurs. Due to the economic crisis of 2008 and the emergence of political extremism, the organized crime groups became number one public enemies, who are again using the same methods which were successful during early 1990s. A kind of semi-legal market and entrepreneurship has developed since 2008.

Keywords: informal relations, economical crises, entrepreneurship, regime change.

"People hope that at least the police know how to order the world - I can imagine no more pathetic hope - but unfortunately in all these detective stories there is another quite different swindle going on - I don't even mean the fact that your criminals will be brought to justice. This delightful fairy tale is no doubt morally necessary. It is one of the lies that keep the state going, as does the pious saying, crime doesn't pay - whereas in fact you only have to look at human society to see the truth on that score."[2]

"*The chaotic transition of the Soviet Union to the market economy created the conditions for the widespread penetration business activities in Russia (…) by organized crime.*"[3] According to sociologist Manuel Castells, this process helps intensify legal and illegal trading activities with the post-Soviet area. In a report from 1994, the Centre for Social and Economic Analysis – a background institution of the Office of the President of Russia – estimated that around 10% of economic actors in Russia were involved in illegal economic activities, with illegal transactions equalling to 20% of the capital worth of the regular economy.[4]

1 bezsenyi.tamas@uni-nke.hu

2 Dürrenmatt, Friedrich: *The Pledge. Requiem for the Detective Novel.* University of Chicago Press, Chicago, 2000. 8–9.

3 Manuel Castells: *Az évezred vége. Az információ kora. Gazdaság, társadalom és kultúra III. kötet*. Gondolat Kiadó, Budapest, 2007, 206. o. [Az információs társadalom klasszikusai]

4 Rossiiskaya maffia sobiraet dos'ye na krupnykh chinovnikov i politikov. *Izvestiya*. 26th of January. pp1-2.

PENETRATION OF ORGANIZED CRIME INTO ECONOMY

The case of József Stadler – an entrepreneur from Akasztó – became one of the most iconic cases of the 1990s, calling the attention of the wider public to the deficiencies of the newly emerging market economy in Hungary. Due to the intensification of vendettas, infamous contract killings and other high profile economic crimes (Globex, Postabank-case) during the second half of the decade, the public forgot the significance of the Stadler case. Journalists and other experts tended to focus on latter crimes in their books[5] or articles.[6]

Through a series of interviews conducted with police detectives, it quickly became apparent that for the reasons mentioned above,[7] the case of the entrepreneur from Akasztó – along with his motivations, and the criminal techniques applied – quickly faded from the agendas of criminal justice conferences and symposiums as well. In the meantime, the case file grew so thick, that involving new detectives in the investigation became increasingly difficult, and eventually impossible. Just bringing new officers up to speed through a detailed overview of the files would have taken several weeks at first and would have later taken several months at least. According to one of the detectives, one of the house-searches alone yielded several hundred kilogram bags of documents, occupying 40m^2 of storage space.[8] Undoubtedly, one of the most ironic elements of the case is the fact, that the case documents – totalling several tons – are nowhere to be found. They are not in the police archives, and according to my inquiries, they are not in the Hungarian historic archives either. By all accounts, it seems that they have been scrapped.[9]

DIFFICULTIES OF INVESTIGATING ORGANIZED AND ECONOMIC CRIMES

In the following, I will review the effects that the political system change of 1989 had on the police force's relation to investigating economic crimes. By doing so, I hope to shed light on the true nature and extent of the influence of Mr. Stadler in this process. The following analysis aims to showcase that the entrepreneur from Akasztó was capable of becoming a successful businessman during the 1990s and during the economic crisis of 2008 alike. Owing to a weak culture of investigative journalism and a lack of knowledge about economic crimes, Mr. Stadler was and still is often portrayed as a simple tax evader by the media, although he is much more than that.

Another issue compounded the lack of understanding surrounding the nefarious activities of Mr. Stadler. On the 5th of January 1990, prominent politicians from SZDSZ and FIDESZ brought charges against the Homeland Security Service of the Ministry of the Interior, for illegally spying on opposition parties and civil society initiatives.[10]

As a result of all public attention the case was getting, high-ranking police officials felt compelled to indiscriminately disband informant networks, including assets working in the field of criminal justice.[11] This decision proved to be detrimental in the fieldwork of investigation. Without assets, carrying out operative investigations proved to be nearly impossible. Investigations regarding economic crimes took a particularly heavy blow. During the transition period many of these crimes were committed against the state itself.[12] In many cases, the damages caused were less apparent and thus went unnoticed. Counter to the pre-1989 mentality, the Criminal Code of that day (1978. IV. Law) did make it possible (in Chapter XVII) for economic crimes to be committed against private entities, not just the state and its companies. Informally, however, the state remained at the centre of the authorities' perception of economic crimes.

At the time, the National Police Department[13] (*ORFK*) did not have a separate property damage department. The Budapest Police Department's (*BRFK*)[14] property damage department functioned as an operative entity only with concrete investigations being conducted by a general *investigative* department. County police departments had property damage departments, which conducted both operative and investigative work. However, without informants, conducting meaningful operative work became impossible.

5 Mong Attila – Vajda Éva: *Az ártatlanok kora*. Elektromédia, Budapest, 2009.
6 Diós Erzsébet: *Bankcsődök és bankárperek: bankbukások története tanulságokkal*. OKRI Szemle (szerk.: Virág György) 2009. pp. 81-100.
7 Interview with "B. M." police colonel 2013. 02. 24.
8 Interview with "B.I." retired police colonel, 2013.03.31.
9 Interview with "B. M." police colonel 2013. 02. 24.
10 Monika Walepa: Hostages and Skeletons in Poland, Hungary and the Czech Republic. In: Monika Walepa: *Skeletons in the Closet. Transnational Justice in Post-Communist Europe*. Cambridge University Press, New York, 2010. 82–83.
11 Interview with "N.L." retired police colonel, 2013.04.17
12 Interview with "B. M." police colonel 2013. 02. 24.
13 Hierarchically the highest national body of law enforcement in Hungary
14 The main police department of Budapest.

The decision not to transform the departmental structures of the police force to better suit the changing economic realities – i.e. by not converting the communal property damage departments into property damage departments, and the decision to disband the informant networks – led to a drastic increase in economic crimes like fraud, embezzlement or malfeasance.

The realization and acknowledgement of these processes calls for the reinterpretation of the statistical data presented in Mihály Tóth's research paper: *Market Economy and Criminal Law*. Tóth's data shows, that between 1986 and 1988 the yearly number of crimes known to the authorities was 180,000 on average. This number steadily increased: to 225,393 in 1989, to 341,061 in 1990, to over 400,000 in 1991 and to 447,215 in 1992.[15] According to Tóth's data, the number of economic crimes stayed more or less stagnant at 8,000/year all throughout this period. As seen from the article, the author had difficulties explaining this stagnation, saying that two-thirds of these crimes were tariff and foreign exchange related, whose *"number was constant (or at least, the amount of money spent on uncovering these crimes was)."*[16]

The lack of restructuring the police force following the 1989 transition, as outlined above, seems like the most plausible explanation for this lack of increase in the statistics. The anachronistic language quoted by Tóth in his analysis and the outdated problem understanding behind the statistics totally disregard the fact of the system change. This gives a further indication of the ill preparedness of the police force of the day.

Furthermore, it is important to highlight the question of moral and law. Here I am referring to the lack of a strong economic or tax moral. This meant that Mr. Stadler was portrayed by some parts of the media and perceived by many as a folk hero of sorts – this is clearly illustrated by the article in *National Sport*.[17] Péter Imrédy wrote five volumes on the life of the entrepreneur, entitled "*The Stadler Story*". The language used by Mr. Stadler in the interviews in the books is simple, peasant like with an almost rustic quality – similarly to the language he used in spoken language, as illustrated by several video interviews.[18] Mihály Tóth lamented the lack of a proper societal moral compass himself, blaming the paternalistic perception of Hungarian society. According to him the extensive amount of written regulations resulted in *arbitrary reinterpretation*[19] of the "*everything is allowed that is not prohibited by law (written laws of course!)*" norm. In other words, the lag of the speed and the unclear phrasing of new regulation in the wake of the political economic system change – and the abundance of legal loopholes – facilitated the blurring between the lines of legality and illegality.

ENTREPRENEUR OF THE SYSTEM CHANGE

József Stadler started exporting various products to eastern markets from the 1990s, especially to the Soviet Union, and the newly emergent Ukraine and Russia. In police testimonies made in front of the Parliament's Oil Committee, the implications of the dissolution of the Soviet Union were discussed. According to Ernő Kiss, Police Brigadier General: "*the penetration of people from various parts of the state institutions into the spheres of economy has started there as well. We have the appropriate connections in these countries. Right from the start, we should have done the same, as the professionals and politicians from their country. We did not do anything, however have the appropriate staff to conduct information gathering operations in Ukraine or even in Russia based out of Hungary.*"[20] Besides the deficiencies caused by the disbanding of the informant networks, Homeland Security's lack of adequate connections with the services of neighbouring countries made uncovering trans-boarder criminal networks specializing in economic crimes practically impossible. It is likely that formerly high ranking state officials of the Soviet Union – and other eastern republics – moved to lucrative economic activities without greater difficulties, much like they did in Hungary.

Following the 1991 dissolution of the Soviet Union, Russian imperial system was exposed to ever-changing economic reform efforts. The Hungarian economist Laszlo Csaba mentioned the ban of barter, with which the government tried to force the members of the society to use the national currency. Stadler and other similar exporters could be successful in the Eastern European markets, because Russian economic policy forced the companies to pay 40% tax basis on the revenue from exported products.[21] László Csaba

15 Dr. Tóth Mihály: Piacgazdaság és büntetőjog In: Lévay Miklós (szerk.): *Kriminológiai Közlemények 52*. Magyar Kriminológiai Társaság, Budapest, 1995. pp. 4-5.

16 Dr. Tóth Mihály: Piacgazdaság és büntetőjog In: Lévay Miklós (szerk.): *Kriminológiai Közlemények 52*. Magyar Kriminológiai Társaság, Budapest, 1995. p. 5.

17 Sinkovics Gábor: Stadler József: Jövök! Nemzeti Sport 2007. 12. 12. (http://www.nemzetisport.hu/migralt_cikkek/20071212/stadler_jozsef_jovok)

18 Stadler válasza az armanira *Index Videó*. 2007. 11. 04. (http://index.hu/video/2007/11/04/stadler_valasza_az_armanira/?s=tag:stadler)

19 Dr. Tóth Mihály: Piacgazdaság és büntetőjog In: Lévay Miklós (szerk.): *Kriminológiai Közlemények 52*. Magyar Kriminológiai Társaság, Budapest, 1995. p. 23.

20 Minutes of the Parliamentary investigative committee created to investigate any possible links between the oil business and organized crime. 2000. 10 o'clock Monday, October the 30th, meeting held at meeting room number 61 of the Parliament, accessible online at: last download: 2013.05.15 (http://www.parlament.hu/biz36/olaj/v006-021.htm)

21 Csaba László: Tanács-talanul a keleti piacon. *Társadalmi Szemle*, 1991/6., pp. 3–16.

described the economic policies of Yeltsin as having a sort of folkloric quality based on *poetry* and *realities*. The reason being, that while the political declarations made in the media lead observers to believe that the government was pursuing a strict monetary policy, in reality they continued to pursue Soviet style planning cycles.[22]

This meant that making profit became increasingly difficult on these eastern markets. Insider information, well placed informants and the exploitation of the loopholes in the laws were absolutely vital elements of success.[23] Among other things, the financial interventions of Gerashchenko hindered the emergence of a stable market economy. Similarly to the Hungarian situation, there remained several factors that allowed József Stadler to exploit his existing contacts – and to find new ones – to maintain the profitability of his enterprises.

In 1988, József Stadler founded *Stadler LLC* with an initial capital stock of one million forints. Mr. Stadler was the chief executive of the company from the very start. At first, Stadler LLC only conducted trade within the borders of Hungary, however following the transition, the company quickly expanded to international trade. In the *Stadler Story*, Mr. Stadler says that he had started out in the 1960s by buying cheap alcohol from various agricultural collectives in Bács-Kiskun County, and selling it to neighbouring pubs and restaurants at a profit.[24]

By 1988-89 he had established such good relations with the leaders of various collectives, that he already had a good grasp on the workings of the wholesale distribution networks in the country. Similar entrepreneurs from that time also misused these informal networks for illegal purposes.[25] He started buying alcohol from the factory, and he built a large distribution network, operating with his own trucks. At the time of the system change, the manufacturers and wholesalers that Mr Stadler had been doing business with got into a tough spot. The COMECON formally ceased to exist on June 28, 1991. Several companies lost the markets that they took for granted overnight: the Nagykőrős Canning Factory, the Szobi Szörp Inc., the Kőbánya Brewery or the prosperous Budafok wine cellars. This meant that Mr. Stadler could buy up their products dirt-cheap. In 1990, the coalition Antall government was formed between MDF, KDNP and FKgP. The eastern markets were not overly important for these parties. The infamous *"Tavarisi konyec"* (it's over comrades!) poster of MDF[26] symbolized the mentality of the governing coalition.[27] In reality, the reason for this distancing had more to do with the fact that the economic supporters of the new government did not enjoy the sort of access to information and knowledge of the functioning of the state administration – as highlighted by László Csaba – on the eastern markets – as did their predecessors. In a co-authored article, Alexandr Buzgalin and Andrej Koganov highlight the immense difficulties in penetrating the Russian market of the day.[28] Miklós Kun – a historian – corroborated this in an interview he gave about Russian markets. He suggested that western companies had been supporting local traders in the newly emerging post-Soviet nations, who had good contacts with influential people in order to be well informed about the relations and situations on the ground.[29] Moreover, the imports of agricultural products increased at that time in Hungary.[30]

The Antall government's decision to deepen trade relationships with Germany made the situation of the struggling Hungarian companies even worse. They were unable to sell their products on the German market, because of their low quality. To use a metaphor: it is easier to turn small ships in a narrow straight or bay in the direction of the wind, than it is turning a three mast giant. If we identify the narrow straight as the changes caused by the system change, than it is easier to see why newly emerged small entrepreneurs like Mr. Stadler– the little ships – had an easier time navigating the waters than enormous post-socialist mammoth companies – three mast ships. The Antall government provided export subsidies to companies that were willing and capable of exporting. They provided agricultural exporters with a 30% cash-back subsidy of the prices of their exports. Entrepreneurs received 30% back on various food products.[31]

22 Csaba László: Volt-e sokkterápia Oroszországban? In: *A jelcini gazdaságpolitika alternatívái. – Szakértői jelentés*. Szovjet Füzetek VI. Magyar Russzisztikai Intézet, Budapest, 1992. p. 9.
23 Csaba László: Volt-e sokkterápia Oroszországban? In: *A jelcini gazdaságpolitika alternatívái. – Szakértői jelentés*. Szovjet Füzetek VI. Magyar Russzisztikai Intézet, Budapest, 1992. p. 22.
24 Imrédy Péter: *A Stadler story 1. kötet A kisjuhásztól a nagy felvásárlóig*. Kastély-Bor Kft., Akasztó, 2008. pp. 51-52.
25 Paládi József: *A zöldséges maffia*. Népszava, Budapest, 1988, 114–128. o.
26 Orosz István : Tovarisi konyec! Magyar Demokrata Fórum választási plakát, 1990. (http://muzeumantikvarium.hu/item/tovarisi-konyec--magyar-demokrata-forum-valasztasi-plakat,-1990---tervezte-orosz-istvan-)
27 Sárközy Tamás: *Magyarország kormányzása 1978–2012*. Park Könyvkaidó, Budapest, 2012. 192.
28 Alexandr Buzgalin – Andrej Koganov: Totális privatizáció – méreg és orvosság (Tézisek) In: *A jelcini gazdaságpolitika alternatívái. – Szakértői jelentés*. Szovjet Füzetek VI. Magyar Russzisztikai Intézet, Budapest, 1992. pp. 79-80.
29 Márton Gábor: Felértékelődnek a keleti piacok Szegedma.hu 2010. 07. 14. (http://szegedma.hu/hir/szeged/2010/07/felertekelodnek-a-keleti-piacok.html)
30 Petschnig Mária Zita: Túl az első fél éven. A pangó piac nem ígér változást. In: Kéri László – Petschnig Mária Zita: *24 évszak*. Intera Rt., Budapest, 1995, 332–333. o.
31 Juhász Pál - Mohácsi Kálmán: Az agrárágazat támogatásának néhány összefüggése. *Közgazdasági Szemle*, XLII. évf., 1995. 5. sz. pp. 471-484.

Comparing police interviews and the article of journalist József Ballai, it seems that Ballai's account of Mr. Stadler's initial success is very accurate.[32] Stadler LLC started off with a small fleet of trucks, however by 1993-94 the company *"owned 42 – mostly Mercedes-Benz – bobtail trucks."*[33] At the time, the company made an export profit of 125 million dollars. Owing to Mr. Stadler's good contacts, his partners paid him in USD. In comparison to his profits from abroad, his one billion forint profit from the domestic Hungarian market seemed only like peanuts. At the exchange rate of the day, the 125 million profit made from exports equalled several tens of billions of forints. On the books, however Stadler LLC only showed a modest profit of 600 million forints. This meant that the company only had to pay corporate and other taxes after this amount.

At first, APEH – the Hungarian tax authority – only asked him the questions about his company's inventory register, since he could never give an exact answer when asked how large his inventories were. When asked about his fruit concentrates and beer inventories, he always said, that he had X number of pallets, however he could not say how many bottles that meant in total.[34] József Lovas, a detective of the Kecskemét Police Department's property protection department conducted several covert investigations against Mr. Stadler, however there was never enough evidence to start conducting an overt investigation against the entrepreneur. In the Imrédy autobiography of Mr. Stadler, the entrepreneur makes mention of Detective Lovas, remembering how he would always call him into his office, and ask how he was able to make such immense profits.[35] It should be noted, that there is no proof as to the truth of this claim by Mr. Stadler, based on the interviews conducted with police detectives.

As the above cited figures show, Mr. Stadler's profits would have easily allowed him to pay the larger tax burdens, however he wanted a larger empire and he wanted it fast.[36] In order to achieve his goal, he used a double invoicing system. The lot numbers, dates, company information were exactly the same. Only the unit and final prices differed. He provided invoices with the larger prices to the tax authority, in order to receive larger export subsidies. In other words, he received the subsidies after much larger – fictive – sales. This, and not the VAT fraud he committed, was the real source of his immense profits.[37] If we look at Stadler LLC's books, we can easily see, that the non-fraudulent export subsidies that would have been due to the company after the actual sales prices, would have covered Mr. Stadler's costs and left him with a significant profit – approximately a third of what he made by his cooking of the books.[38]

THE MACROECONOMICAL EFFECTS OF MODUS OPERANDI

The only issue Mr. Stadler had to deal with because of his double invoicing scheme was that of the fictional profits his company was generating on paper – and thus the surplus taxes that he would have had to pay after these. In order to avoid paying these taxes, the accountant of the company, Gyula Hrubi, recommended generating surplus overhead costs and fictional losses, in order to eat-up the "*balloon profits*".[39]

This is how other organized crime syndicates appeared around Mr. Stadler. Nándor Pergel, a well tailored criminal, who spoke good French, and was involved in a horde of economic crimes, specialized in creating phantom companies in order to commit massive VAT fraud operations.[40] His air-conditioned car at the beginning of the 1990s gave a strong indication as to his financial situation for the police investigators. László Zsíros was one of Pergel's affiliates, in charge of accounting and phony invoicing. Ferenc Domák – or "Cinóber" as he was known among the criminal underworld - came from the world of prostitution and drug trafficking. He was shot dead on Üllői road in 1996.[41]

This ring of criminals mainly specialized in "*transiting*" products with sham contracts through Hungary. One company would import 155,288 pieces of cosmetic items for 971 thousand forints, which it sold on to a second company for 41 million forints. This company then resold the items for 20 million forints. The third company then sold the items for 147.5 million to the fourth, which sold the items to Mr. Stadler's company for a few million more. Of course, the tax authority refunded the VAT to Mr. Stadler's company in Akasztó. However, József Balla's – the journalist chronicling Mr. Stadlers activities – claim that the VAT refund was the centrepiece of the illicit activities, is largely false. The above mentioned cosmetic items consisted of cheap French perfumes, and artificial leather shoes from Syria, manufactured for the dead – thus

32 Interview with "B. M." police colonel 2013. 02. 24.
33 Ballai József: A Stadler-dosszié - I. rész: A búsuló juhász. *Magyar Narancs* 2001. 02. 01. (http://magyarnarancs.hu/belpol/a_stadler-dosszie_-_i_resz_a_busulo_juhasz-62501)
34 Interview with "K.F." retired police major, 2013.03.12
35 Imrédy Péter: *A Stadler story 1. kötet A kisjuhásztól a nagy felvásárlóig.*Kastély-Bor Kft., Akasztó, 2008. pp. 148-149.
36 Interview with "B. M." police colonel 2013. 02. 24.
37 Interview with "B. I." retired police colonel 2013. 03. 31.
38 Interview with "B. M." police colonel 2013. 02. 24.
39 Interview with "B. M." police colonel 2013. 02. 24.
40 Interview with "B. M." police colonel 2013. 02. 24.
41 Interview with "N. L." retired police colonel, 2013. 04. 17.

they were not of very high quality.[42] The above described process of "*transiting*" happened through non-existent companies – that were unknown to the business registry court.[43] Physically the imported items went right to Mr. Stadler's warehouse in Akasztó, for less than one million forints. After the *"transiting"* had taken place, Stadler LLC resold the stock to Ukrainian and Romanian companies for a little more than the purchase price. This meant, that he had his initial investment returned, and he could show a huge loss towards the APEH, which meant that the company's yearly profits would fall accordingly, and thus Mr. Stadler would have to pay less tax.[44]

In order to unravel the process of "*transitioning*" the authorities had to prove that the companies involved did not exist. The investigators succeeded in doing so. They also managed to prove that all the invoices were written with Nándor Pergel's typewriter.[45]

Another activity conducted by Mr. Stadler in order to increase his company's overhead costs shows just how easy it was for those involved in exporting to deceive even the authorities, which were unaware of many of the loopholes. In the interim period – between Mr. Stadler's moving from domestic business to exporting – the entrepreneur used the political and economic commotion to his advantage. He framed himself, as if he intended to do business with another emerging market economy, with similar endowments as Hungary. Various different Russian marketing agencies conducted marketing and market research activities for Stadler LLC in segments of the economy to which Mr. Stadler had no formal ties, but which he informally was very well acquainted with. The prosecution took seven invoices as evidence. These amounted to 2.4 billion in costs, which meant that the entrepreneur from Akasztó could decrease his tax base by 989.5 million in the year in question alone.

The majority of the media focused on Stadler, the art collector, since this was more tangible than the above described processes. In 1993, on paper Mr. Stadler bought 22 paintings. Mr. Stadler paid for the lot of paintings in two instalments – in cash in both cases. The joint tally of the two invoices came to 820,483,600 forints – this meant a VAT rebate of 205,120,900 forints.[46] He conducted his purchases for his collection through a certain Sergei Antolevics Vexler – a Russian businessman. The investigators never found him, because the authorities could not be certain who this person really was. Through the cooperation of the Hungarian and Russian authorities during the Stadler investigation, it became apparent that none of the companies in Russia that Mr. Stadler conducted business with were actually registered.[47]

The Stadler case was the first instance in post-socialist Hungary, when a defendant could use the media to his advantage, thus putting pressure on the authorities and the Parliament as well. This proves that the battle for the media has to be won as well. In 1998, the initial first-degree court verdict sentenced Mr. Stadler to 9 years of incarceration and the confiscation of all his property. The Supreme Court set aside the earlier judicial decisions, and ordered a new procedure in the first instance. In 2001, the first degree court sentenced to Mr. Stadler to 5 years and six months. The second verdict of the Supreme Court reduced the sentence to 4 years and six months, without changing the findings of the first degree court, however claimed that prosecution of Stadler started almost ten years ago.[48]

After being released from prison, the ex-entrepreneur opened a shop in Solt, where he conducted commercial activities. Owing to his prior conviction, he was prohibited by law from taking up a leading role in any company, so his second and third degree accomplices were registered as the chief executives of the company. During the investigative phase of his second case, Mr. Stadler admitted that he founded and held the majority ownership in two companies. However, he also claimed that because of his prior conviction, he did not take an active role as an executive. He claimed that his second and third degree accomplices fulfilled their duties as executives. The two companies were registered at the homes of the two accomplices; however the actual offices of the companies were in Solt. During the 2008 economic crisis, Mr. Stadler was utilizing his vast network of acquaintances to buy up clothes and foodstuffs below market prices in eastern countries, and import them to Hungary. He also bought unpackaged detergents in massive amounts at wholesale prices, packaging and branding the detergent under his own name. He bought the second-hand clothes in massive quantities as well, and resold selected pieces to the residents of Bács-Kiskun County as new.

The tactics used by Mr. Stadler during the 1990s became successful once again in the 2000s, in large part due to the economic crisis. Mr. Stadler had more customers, and more illicit business associates than ever. According to the prosecution, between 2007 and 2010, Mr. Stadler caused 420 million forints worth of damages to the Hungarian State by issuing and accepting fraudulent invoices through companies in which he had interests, in order to apply for VAT refunds, in order to make illegal profits or decrease the

42 Interview with "B. I." retired police colonel 2013. 03. 31.
43 Kocsisné dr. Surányi Andrea – Garamvölgyi Ildikó – Pekala Károly: *Polgári jogi, gazdasági jogi ismeretek*. Rejtjel Kiadó, Budapest, 1999, 107. o.
44 Interview with "B. M." police colonel 2013. 02. 24.
45 Interview with "B. M." police colonel 2013. 02. 24.
46 Interview with "N. L." retired police colonel, 2013. 04. 17.
47 Interview with "B. M." police colonel 2013. 02. 24.
48 Négy év hat hónap Stadlernek *Index* 2003. 02. 12. (http://index.hu/bulvar/stadler0212/)

tax burdens of his companies. The Szeged Appellate Court sentenced Mr. Stadler to 4 years and 10 months incarceration, and confiscation of property worth 67 million forints in November of 2011. According to the investigation materials, he bought the massive amounts of clothes from Western Europe without providing invoices, and then with the help of his previous accomplice, Gyula Hrubi, he proceeded to produce fraudulent invoices to non-existent companies, claiming to have bought the clothes from them. However, since these companies were non-existent, they did not pay VAT. However, Mr. Stadler was able to apply for VAT reimbursement himself. It was suspected, that the clothes made their way to Eastern Europe by way of charity organizations, which illegally sold the clothes to Stadler and other criminal organizations. Since clothes arriving to Hungary from charity organizations could not be resold through commercial activity, it was necessary for Mr. Stadler to produce a paper trail. On paper he bought the detergents and other accessories at such a high price that he could again, write off some of his corporate tax base. Foundation fraud came to the forefront at that time because it was found that *One for Each Other Foundation* committed several frauds with the help of the Hungarian secret services.

CRIMINAL OR FOLK HERO? CONCLUSIONS

With his trademark shout of "*I am innocent*"[49] and with his attacks on politicians, Mr. Stadler became successful in the media. Law enforcement officials were most likely puzzled by the fact that Mr. Stadler became a favourite of the newly privatized media outlets. Various newspapers and magazines helped create the image of a folk hero. This was something that could not have happened in the time of state run media only a few years earlier. From sheepherder to billionaire entrepreneur: a real self made man. Since Mr. Stadler, the authorities take it for granted that cases have to be won not only in the court, but also in the media.

Mr. Stadler was already a successful businessman during the socialist period. At the time of the regime change in Hungary through his extensive network of contacts he was capable of selling products that seemed unsellable at the time. By organizing the shipping activities himself, Stadler was able to extend his range, and his profits – through illicit activities. During the time of the economic crisis, he used his Eastern European contacts to buy foodstuffs, clothes and detergents from various Western European countries. These products were usually of very low quality, and Stadler branded them with his own name after he left prison, in the hope of capitalizing on his newfound fame.

The tale of the entrepreneur from Akasztó illustrates how organized crime and business fused together following the regime change in Hungary. The change in the economic realities in the early 1990s, and the arrears in new laws allowed Mr. Stadler, balancing on the boundaries of legality and illegality to jump-start his career. As a successful businessman during socialism, building a vast web of informal contacts made it possible for Mr. Stadler to become successful as an exporter to the countries east of Hungary. Thanks to these contacts of his, Mr. Stadler was able to use buffer companies of his contacts during the 2008 crisis at a much lower price. All the confusion and chaos during the early 1990s in Hungary and the economic recession during the 2000s made it possible[50] for Mr. Stadler to become the entrepreneur of crises.

REFERENCES

1. Ballai József: A Stadler-dosszié - I. rész: A búsuló juhász. *Magyar Narancs* 2001. 02. 01. (http://magyarnarancs.hu/belpol/a_stadler-dosszie_-_i_resz_a_busulo_juhasz-62501)
2. Buzgalin, Alexandr – Koganov, Andrej: Totális privatizáció – méreg és orvosság (Tézisek) In: *A jelcini gazdaságpolitika alternatívái. – Szakértői jelentés*. Szovjet Füzetek VI. Magyar Russzisztikai Intézet, Budapest, 1992.
3. Csaba László: Tanács-talanul a keleti piacon. *Társadalmi Szemle*, 1991/6., pp. 3–16.
4. Csaba László: Volt-e sokkterápia Oroszországban? In: *A jelcini gazdaságpolitika alternatívái. – Szakértői jelentés*. Szovjet Füzetek VI. Magyar Russzisztikai Intézet, Budapest, 1992.
5. Diós Erzsébet: *Bankcsődök és bankárperek: bankbukások története tanulságokkal*. OKRI Szemle (szerk.: Virág György) 2009. pp. 81-100.
6. Elvirát a börtönből hódította meg Stadler. *Blikk*, 2005. január 21. (http://www.blikk.hu/blikk_aktualis/20050121/elvirat_a_bortonbol_hoditotta_meg_stadler)

49 Elvirát a börtönből hódította meg Stadler. *Blikk*, 2005. január 21. (http://www.blikk.hu/blikk_aktualis/20050121/elvirat_a_bortonbol_hoditotta_meg_stadler)
50 Interview with "N. L." retired police colonel, 2013. 04. 17.

7. Imrédy Péter: *A Stadler story 1. kötet A kisjuhásztól a nagy felvásárlóig*. Kastély-Bor Kft., Akasztó, 2008.
8. Stadler válasza az armanira *Index Videó*. 2007. 11. 04. (http://index.hu/video/2007/11/04/stadler_valasza_az_armanira/?s=tag:stadler)
9. Juhász Pál - Mohácsi Kálmán: Az agrárágazat támogatásának néhány összefüggése. *Közgazdasági Szemle*, XLII. évf., 1995. 5. sz. pp. 471-484.
10. Kéri László – Petschnig Mária Zita: *24 évszak*. Intera Rt., Budapest, 1995.
11. Kocsisné dr. Surányi Andrea – Garamvölgyi Ildikó – Pekala Károly: *Polgári jogi, gazdasági jogi ismeretek*. Rejtjel Kiadó, Budapest, 1999.
12. Castells, Manuel: *Az évezred vége. Az információ kora. Gazdaság, társadalom és kultúra III. kötet*. Gondolat Kiadó, Budapest, 2007, 206. o. [Az információs társadalom klasszikusai]
13. Márton Gábor: Felértékelődnek a keleti piacok Szegedma.hu 2010. 07. 14. (http://szegedma.hu/hir/szeged/2010/07/felertekelodnek-a-keleti-piacok.html)
14. Négy év hat hónap Stadlernek *Index* 2003. 02. 12. (http://index.hu/bulvar/stadler0212/)
15. Oil committee - Minutes of the Parliamentary investigative committee created to investigate any possible links between the oil business and organized crime. 2000. (http://www.parlament.hu/biz36/olaj/v006-021.htm)
16. Paládi József: *A zöldséges maffia*. Népszava, Budapest, 1988.
17. Rossiiskaya maffia sobiraet dos'ye na krupnykh chinovnikov i politikov. *Izvestiya*. 26th of January. pp1-2.
18. Mong Attila – Vajda Éva: *Az ártatlanok kora*. Elektromédia, Budapest, 2009.
19. Sárközy Tamás: *Magyarország kormányzása 1978–2012*. Park Könyvkaidó, Budapest, 2012.
20. Sinkovics Gábor: Stadler József: Jövök! Nemzeti Sport 2007. 12. 12. (http://www.nemzetisport.hu/migralt_cikkek/20071212/stadler_jozsef_jovok)
21. Dr. Tóth Mihály: Piacgazdaság és büntetőjog In: Lévay Miklós (szerk.): *Kriminológiai Közlemények 52*. Magyar Kriminológiai Társaság, Budapest, 1995.
22. Walepa, Monika: *Skeletons in the Closet. Transnational Justice in Post-Communist Europe*. Cambridge University Press, New York, 2010.

UDC: 343.85:343.62-055.2
343.85:343.54/.55-055.2

ANALYSIS OF MULTI-AGENCY COOPERATION IN REPRESSION OF DOMESTIC VIOLENCE – PROBLEMS AND OPPORTUNITIES OF IMPROVEMENT

Aleksandra Spasojevic[1]
Valjevo Centre for Social Care

Abstract: Domestic violence is a criminal offence with specific characteristics of perpetrators and victims, and methods of execution, and because of that it is necessary to handle it from multiple aspects. For its understanding multidisciplinary knowledge is necessary, and for its repression, coordination and cooperation of professionals from different professions is inevitable. Organs of formal social control participate in that process, and for their success a good multi-agency cooperation is a necessary prerequisite. Every official organ has in its jurisdiction standardized rules of action, but it also has an obligation to communicate with other sectors or agencies. Here, we will represent actual situation of multi-agency cooperation in repression of criminal offence of domestic violence and violence against women, on local area, and the methods of their cooperation, using current legal framework and practical experience. We will point out the cooperation between police, public prosecution and social service as key factors, without whose timely and adequate response it would not be possible to protect victims of domestic violence. In their treatment, these professionals have practical problems that we will point out through this analysis, but we will also give the proposals for their possible solutions in order to improve the current multi-agency institutional cooperation.

Keywords: multi-agency cooperation, domestic violence, police, public prosecution, centre for social work.

INTRODUCTORY CONSIDERATIONS

Domestic violence is a social phenomenon with global ranges. It represents an injury of basic human rights of family members, the right to live and to be secure, the right to freedom, physical and psychical integrity and sexual identity. Every human being is born free and equal in dignity and rights.[2] Human dignity and life are inviolable and physical and psychical integrity are inviolable too, and no one should be exposed to torture, inhuman treatment and humiliation acts or punishments.[3] Because of complexity of the problem, although those critical acts could be included by the law with other criminal acts, domestic violence is registered like a separate criminal offence.

In the sense of criminal law, domestic violence represents the use of violence, threat to attack life or body, impertinent and irrespective behaviour which threatens peace,[4] physical integrity or psychical state of a member of one's own family (Article 194, paragraph 1 of the Criminal Code).[5] In paragraph 4 of the same Article there is a qualified form of domestic violence that has death of a family member as consequence. However, if more severe consequences (like death) resulted from this criminal act, and for which the law provides severe punishments, then this punishment could be pronounced, if the perpetrator has been acting from negligence in the relation to that consequence.[6] On the contrary, if abuse has preceded the murder of a family member, it would be qualified as first degree murder (Article 114, paragraph 10 of the Criminal Code).

Considering the fact that the family is the primary object of criminal law protection, there is an obligation of the state to protect the family and make order in relations between its members. Earlier, the domestic violence was considered as internal, private matter of the family, but the consequences of violence go beyond the home. Then it is not a private issue, it is an issue of the entire society. The approach of everyone involved in the protection of victims of domestic violence is crucial, and sometimes crucial in the victims'

1 novisad.aleksandra@gmail.com
2 Universal Declaration of Human Rights, Resolution of the General Assembly of the UN, 217A (III) by 10.12.1948.
3 Ustav Republike Srbije „Službeni glasnik RS" br. 48/94 and 11/98/2006, 2. deo (cl.23, cl.24, cl.25).
4 Peace could be considered as fulfilling of physical and psysical security.
5 Krivični zakonik Republike Srbije, Službeni glasnik RS, бр. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009 i 121/2012). čl.194.Nasilje u porodici.
6 Ibid. Article 27

lives. It represents a response of the society, its willingness and maturity for repression of domestic violence, but it also gives away its problems and necessity for improvement. Accordingly, we should especially look back at the analysis and significance of multi-agency cooperation between police, the centres for social care and the public prosecution office, which represents the topic of this article.

Those are the official institutions which are first informed about a criminal act and which first come in touch with the afflicted individuals and perpetrators of the criminal act. Therefore, it can be assumed that the quality of their organization, coordination and cooperation, may affect the quality of evidence which contribute to the conviction and avoidance of secondary victimization of the victim.

The cooperation between the institutions in that way could be defined as a process of making partner relationships between those institutions in order to identify problems and with common goals in resolving them, but with respect to the principals of equality, appreciation and standardisation of opinions. Cooperation, help and support of experts or various specialists is necessary; also, the systematic approach in elimination of all risk factors and taking measures and actions is required in the procedure of victim protection of domestic violence.

Multi-agency approach and cooperation represents the force for comprehensive response of social community and institutions with the purpose of fighting this negative social phenomenon, approaching from different angles, but with one common goal - provision of better cooperation among all institutions and organizations in touch with victims and perpetrators of domestic violence.

Multi-agency approach is a process, which demands duration and consistency of procedures and treatment, and not one-time service and momentary contact. Namely, family system includes various factors and multiple needs that should be satisfied with psychological, safety, health, material and educational or legal services, so it is necessary that all or most of them unite, standardize and enable in legal way all in one place, and then enable their real use in expedient and simple way, within the shortest time possible.

LEGAL FRAMEWORK OF MULTI-AGENCY COOPERATION

Besides the already above-mentioned legal acts, the fight against domestic violence has been regulated and improved over the years, primarily through international documents. Some of the most important are the United Nations Convention on the Elimination of All Forms of Discrimination against Women,[7] the UN Declaration on the Elimination of Violence against Women,[8] Council of Europe Convention on preventing and combating violence against women and domestic violence[9], etc. and their importance is reflected in its contribution on improving national law on fight against domestic violence.

By defining and aligning the legal framework and by taking the examples of good practice from other countries, Serbia has recently begun to develop intensely multi-sector cooperation in combating domestic violence. Earlier, the cooperation almost did not exist, because there was no adequate legal framework which prescribed obligatory treatment and methods of work, and now, although we have a legal framework, it appears that cooperation again does not exist in some areas. Specifically, its quality is not at high level of efficiency, or it is at the level of necessity of the minimum standards or does not exist at all. In Serbia, there are a few cities and local governments that can commend with a high degree of coordination and effectiveness of multi-sector work in combating domestic violence.

Due to the adoption of the National Strategy for the Prevention and Combating Violence against Women in the Family and in Intimate Relationships,[10] the Republic of Serbia has an obligation to implement the following:

1) Strengthen the capacity of organizations and institutions that deal with the victims of violence;
2) Establish and enforce the mechanisms to ensure treatment within international obligations related to human rights in the area of sexual and gender-based violence;
3) Strengthen the legislative framework in the field of protection of victims of violence, and
4) Raise awareness of the public and citizens about the non-acceptance of violence as a model of behaviour in order to contribute to creating a social environment that would have a preventive function.

7 Zakon o ratifikaciji Konvencije Ujedinjenih nacija o eliminisanju svih oblika diskriminacije žena (CEDAW, 1992) „Službeni list SFRJ-Medjunarodni ugovori" br.11/81.
8 http://www.un.org/documents/ga/res/48/a48r104.htm. Declaration on the Elimination of Violence against Women, A/RES/48/104. The General Assembly of United Nations (1993).
9 http://www.conventions.coe.int/Treaty/EN/Treaties/Html/210.htm.Council of Europe Convention on preventing and combating violence against women and domestic violence. (2011).
10 Nacionalna strategija za sprečavanje i suzbijanje nasilja nad ženama u porodici i u partnerskim odnosima (2011). „Službeni glasnika Republike Srbije" br.021/2011. Uprava za rodnu ravnopravnost, Ministarstva rada i socijalne politike.

In this sense, the improvement of cooperation and raising capacity of institutions is one of the strategic objectives of the National Strategy, so the first three of the above mentioned obligations specifically affect the work of the state authorities. The basic precondition for the establishing of an effective multi-agency system of support and protection is to establish good cooperation between professionals from all social organized systems (system of health care, education, social and family law protection, police, judiciary).

When we talk about the legal framework that has enabled us clear acting, besides the current laws, we have to emphasize that the basis of multi-sector work is **Opšti protokol o postupanju i saradnji ustanova, organa i organizacija u situacijama nasilja nad ženama u porodici i u partnerskim odnosima**[11] (The General protocol of cooperation among the institutions, organs and organizations in situations of violence against women in the family and in intimate relationships). It regulates the ways of cooperation between marked participants:[12]

1) Police force;
2) Sector of social care (Centre for social work as the leader with coordinating role in multi-agency cooperation);
3) Health care services;
4) Educational institutions and services in the system of education;
5) The public prosecution office, and
6) Regular and misdemeanour courts.

For the sake of consistent application of the General Protocol, all participants in its implementation were obliged to bring in Poseban protocol o postupanju u slučajevima nasilja nad ženama u porodici i u partnerskim odnosima (The Specific Protocol about treatment within the cases of violence against women in the family and in intimate relationships). So, in 2013 these specific protocols were brought by the Ministry of Interior, Ministry for work, employment and social affairs, the Ministry of Health and Ministry of Education, with a more detailed elaboration of internal actions within their respective jurisdictions and in accordance with the basic principles and objectives of the General Protocol.

The main objective of the General Protocol is to establish more detailed mechanisms of coordination among the institutions which have the protection of victims of violence under their jurisdiction. It is necessary to ensure that each institution can act in accordance with its statutory powers and duties effectively and ensure the protection of women, victims of domestic violence in intimate relationships in an integrated and comprehensive manner, in order to promote the safety of the victim and responsibility of the perpetrator.

The protocol provides for detailed rules of treatment so each participant can provide quick and effective protection of women victims of violence, immediately after denunciation; then to protect the victim from further violence and to provide adequate legal assistance during and after the criminal proceedings; but also support institutions in achieving social, psychological, and health care for victims. This fast repressive treatment is not only acting on the offender and protects the victim of violence, but it also performs the preventive effect on all others, sending message that the violence is illegal.

One of the important clauses which is specified by the General Protocol and on which analysis this work is based on, is the prescription of the form, manner and content of cooperation among the authorized institutions, agencies and organizations, as well as other participants involved in detecting and combating violence and providing protection and support to people who suffer from domestic violence.[13]

Within each sector there are problems in the functioning, which originate from various sources, however the issues that are disturbing the efficiency of work even more are the problems in communication among the authorities of formal social control. To identify all present problems it is necessary to analyze the work of each state institution in charge of taking measures and actions in cases of domestic violence, as well as problems in their cooperation and coordination.

THE ANALISYS OF CURRENT SITUATION OF MULTI-AGENCY COOPERATION

By analyzing the prescribed guidelines for work on combating against domestic violence for each sector, we recognize that the multi-agency cooperation is obligatory, but also necessary if we want an effective social response and protection of victims of domestic violence.

11 Opšti protokol o postupanju i saradnji ustanova, organa i organizacija u situacijama nasilja nad ženama u porodici i u partnerskim odnosima (2012). Uprava za rodnu ravnopravnost, Ministarstvo rada i socijalne politike. Beograd. Vlada Republike Srbije. 2011.
12 Ibid. pg. 20
13 Op.cit. pg. 10-11.

Very important connection is necessary in co-operation of the police, public prosecutors and centres for social work in the local area. Their roles can be individually divided like this: police provides security and safety of victim, immediately stopping the violence, centre for social work provides accommodation in a safe environment, financial and social security and psychosocial support, a public prosecutor provides legal assistance to the victim by representing their interests in the name of the state and proposing sanctions for the offender (retention, security measures, detentions, imprisonment).

In practice we can identify different problems in achieving the above, each of these problems stems from various causes which cumulatively impair the efficiency of the work of the institutions of formal social control, which can be eliminated through:

1) the definition of common indicators for analysis, recognition and understanding of the dynamics of domestic violence;
2) the training and specialization of the staff who handles domestic violence cases;
3) the creation of mobile multi-agency teams for repression of domestic violence;
4) joint planning of the treatment of victims and/or perpetrators through case conferences;
5) forming teams for multi-agency coordination at the town/municipality level;
6) forming the units for the victim protection at the local level;
7) legislative prescribing of obligatory modes of cooperation among the institutions under threat of disciplinary measures;
8) mandatory crime scene investigation by the police or public prosecutor;
9) consistency in court practice and ensuring maximum protection of victims during the proceedings;
10) equalizing the treatment of victims in institutions in accordance with generally accepted international
11) standards and preventing secondary victimization;
12) the introduction of legally obligatory deadline actions of the competent institutions;
13) the adoption of one unique law regarding domestic violence;
14) continuous evaluation of the efficiency of the coordinated action of institutions;
15) intensive cooperation with local governments.

Indicators for analysis, recognition and understanding of violence and the dynamics of domestic violence may be different depending on the institution, and we can also say, depending on the staff member in charge. Thereby the assessment of security risk is directly conditioned, and then the assessment if what has happened was an act of domestic violence, how intense it was, how severe it was, and therefore causal assessment will depend on the mode of the treatment and relationship with the victim and the abuser, and searching for help from other institutions participants of protection.

The training and specialization of officers who operate in cases of domestic violence is closely related to the above. Training is essential within one sector, and more joint training within multiple sectors. Basic accredited training is passed only by a certain number of police officers, public prosecutors and employees of centres of social care, but all employees in accordance with their workplace, act in cases of domestic violence.

With the basic training of each officer we can get him or her to:

1) Have basic knowledge about violence against victims and perpetrators;
2) Have a clear understanding of common goals and principles in the protection of victims;
3) Know their roles well and know the basic roles of other sectors, as well as their professional obligations in relation to those roles - rules, limits, operation methods;
4) Introduce them to methods and instruments of exchange of information and consultation within and between sectors, accompanied by appropriate written documents and feedback.

However, there are more ideal solutions that require changes in the law and organization manner and for the state in the financial manner. Guided by the examples of positive practice in other countries, we can certainly adjust some modes of work to our circumstances.

Specialized officers in all sectors who are dealing only and exclusively with cases of domestic violence. The formation of special police unit[14] at levels of head case, dealing only with cases of domestic violence, but also in the centres of social care (team consisting of different educational backgrounds: social worker, psychologist, educator) and in the public prosecutor's offices where in these cases only certain prosecutors will work, is necessary.

14 http//:www.CPS domestic violence-good practice guidance, Attorney general 2005. Pg.8-10. The example of specialized units of police force for dealing in cases of domestic violence is police force in United Kingdom.

These officers should have a higher degree of training than basic, should constantly improve their knowledge, and they should be chosen for that workplace based on the sensitization and work performance success. Their efficiency could be higher in one section by releasing them from other cases, which would lead to more dedicated work, eliminating routine and superficial treatment. Every victim should be provided time, benevolent, and sensitive treatment by all employees in the system, preferably from the employee of the same sex who is specially trained to deal with such situations. On the other hand, by a suitable choice of these officials, we would reduce the influence of prejudices and stereotypes about victims of violence and perpetrators, and it would lead to a sensible approach that would return the confidence of victims of domestic violence in the police officer, in social worker, prosecutor, and in the state and the system. For good functioning and adequate protection of victims constant improving is necessary for the quality of service of employees of the institutions and constant investing in them.

Mobile multi-agency teams in the local area are formed by the specialist members of each sector, who deal with the cases of domestic violence, by implementing a unique model of protection 24 hours a day, in order to properly provide assistance and protection to people who suffered violence. This is achieved by coordinated and networked operations of all institutions through their delegated employees and immediately fulfilling the needs of victims. Mobile team members can establish an operational connection with the group of specialists in domestic violence.

Joint planning treatment for victims and/or perpetrators through conference case for individual cases. This activity is prescribed by the Protocol about work and cooperation and entrusted to the centres for social work to coordinate. It is believed that with the presence of mobile multi-agency teams, it would be easier to fulfil this obligation, considering that in the current treatment of institutions, at least, according to verbal report of employees, organizing conference cases is rare, and when it is organized almost always the actors from some sectors are absent because it is not obligatory.

Team for multi-agency coordination at the town/municipality level, which would be formed from the ranks of senior officers, superiors to those employees who handle the specific cases of domestic violence. Team members will have access to the data from their sector and they will be informed on their problems, and on monthly meetings they would evaluate what has been achieved in individual cases, particularly regarding the severe acts of violence, and they will improve coordination and provide support to officers for the problems encountered during the operation. Their role would be in management, monitoring, evaluation and quality improvement of interventions.[15]

Forming a unit for protection of victims at the city level (employed in specialized shelters) which could be made of a team of experts from the sector of social protection. Their role would be to care for victims, providing material and psychosocial support with a goal to long-term protection of the victim. This aspect of the work could be identified with the work of so-called Intervention centres in Austria, which we will discuss below.

Analyzing all of the above, there exists, as it is often mentioned in literature, a model that can be recommended in order to improve the protection of victims immediately after the denunciation of violence, and which at the same time includes coordinated work of the institutions. **Austrian model of emergency intervention**[16] in protecting victims, which is specified in the Act on the Protection from Domestic Violence (1997) contains three basic elements:

1. *Measures of eviction of offender from home and restraining orders in the period of 10-20 days*, the order imposed by the police, if there is threat to life, health and freedom of the victim. It is the police who evaluate the threat to life, health and freedom of the victim, and immediately take urgent intervention and eviction of the offender. The police inform the competent Intervention Centre on everything and once in three days check the field if the perpetrator adheres to measures. In case of violation of measures imposed by the police, the offender is punished and they order him to move out again, and if he refuses he will be moved out by force. If he violates this he may be arrested. If the violence is committed the police are responsible/obligated to press criminal charges.

2. *Long-term protection by the protective temporary injunction under a civil law* for three months or longer at the request of the victim. The court gives an order immediately or within a few days. With the order, the harassment may be prohibited of a victim by telephone, letters, on workplace, place of living or school and kindergarten mutual children. Characteristically, the measures of temporary order last until the end of the court process in a divorce case.

3. *Support to victims, prevention measures against violence and coordination of all interventions by opening Intervention centres.* They have a role to provide legal support to victims and ensure their protection; to plan security protection together with the victims, follow them in trials, maintain contact with victims after

15 http://www.cheshirewestlscb.org.uk/wp-content/uploads/2012/08/Multi-agency-practice-guidance-domestic-violence-maj-2013.pdf, Safeguarding children abused through domestic violence.

16 Details in: Logar, R.(2005). Austrian model of intervention in cases of domestic violence. (Austrijski model intervencije u slučajevima nasiqa u porodici). Evropska mreža protiv nasilja nad ženama. Autonomni Ženski centar, Beograd.

three months from the incident, have a close contacts with the offices of social protection in order to provide social help and social housing programs for 1-2 months, or to find accommodation for the victims, etc.

Legal prescription of obligatory guidelines and methods of cooperation between the institutions under threat of disciplinary measures. It is necessary that the guidelines be legally defined and obligated in any case, and the treatment should not be based on personal judgment of experts. The introduction of those categories can raise the level of conscientious treatment, because it will be easier to detect failures in the work, and to find the person who made it and punish it, and for the management it is provided to sanction the employee, in order to improve the quality of its work. As man is a human being who has developed an external motivation, this aspect should be used in a legal sense to employees.

The most common model of exchanging information in multi-agency cooperation is demanding written documentation/reports and contacts by telephone. Improving the ways of communication, its agreement could also be achieved on the exchange of information between the associates/sectors at the local community level.[17]

With the methods mentioned above, one part of efficiency improvement would be accomplished. Multi-agency cooperation would be raised to a higher level, clearly prescribing the unique model of cooperation, avoiding insufficient sharing of information between sectors, avoiding dependence treatment effects of personal sensibility of employees using personal contacts, adoption of (not)knowledge about treatment in their sector as well as about the treatment of other sectors and their responsibilities. However, we should solve other problems too.

Obligatory performance of the crime scene investigation by the police or the public prosecutor's is a recommendation that should be taken in situations whenever there are physical injuries of the victim or the offender and when traces of violent behaviour can be detected at the scene, which will be used to complete the criminal charges, which will not be based only on the testimony of the victim. It is unacceptable that the process of proving is based only on the testimony of the victim. In this way, the result of criminal proceedings and the weight of proving are transferred to the victim, which is a risk factor that violence will happen again.[18] In the analysis of this issue we should keep two facts on our mind. First, the strength of evidence does not lie in a single piece of evidence, but in the logical connection of all available pieces of evidence. Second, that the material evidence is the factual evidence, evidence which cannot be wrong, cannot be sworn falsely, that cannot be completely absent, only it can be misinterpreted.[19] The goal of the crime scene investigation is good processing, photographing and documenting of the physical/material evidence that are important for the success of the investigation.[20] In support of the need to perform the crime scene investigation whenever there are opportunities we should point out the fact that our Code of Criminal Proceedings adopted the principle that the purpose of proving is the material truth.[21] All experts recognize that most cases of violence are not processed until the end because the victim withdraws the testimony, and an opinion is that this can be prevented by obligatory performing of crime scene investigations, photographing the injury of a victim and/or offender and the crime scene, as well as by other methods that fall within the domain of collecting evidence, depending on the case.

In some court rooms a presence of experts is allowed for the victims (psychologists, specialists of low, etc.) who will explain to the judge the nature and dynamics of domestic violence and the victim's behaviour, if she does not want to testify or if she did not yet left the abuser; then the reading of the testimony of the victim can be used in court, evidence from other witnesses, recordings of calls to emergency services or giving the first testimony from the victim, the photographs of injuries and the photos of the crime scene. For England and Wales it is characteristic that the victim does not have to testify, but that its testimony can be read in court as evidence.[22]

Inconsistency of court practice and the absence of maximum protection of victims during proceedings can be connected as a necessary consequence of the already mentioned imperfections. Considering the work of the public prosecutors and judges in domestic violence cases, we can get the impression that it is quite based on an independent personal judgment.

The public prosecutor is obligated to prosecute *ex officio* the offender for the offense of domestic violence. The practice of prosecutor's office often shows that if the victim withdraws her testimony or changes it, and there is no other evidence, it usually leads to the dismissal of criminal charges. Violence may have happened, but the prosecutor estimates that there is insufficient evidence for charges. Here, we can ask a

17 http//:www.CPS domestic violence-good practice guidance, Attorney general 2005. pg.8-10

18 Đurđević, Z. (2014). Postupanje policije u slučajevima nasiqa nad ženama u porodici i u partnerskim odnosima u: Integrisani odgovor na nasilje nad ženama u Srbiji, Simeunović, B, Kolarić, D. Kesić, T & Đurđević, Z. Kriminalističko-policijska akademija, str. 113.

19 Kirk, P (1985). Crime Investigation (second edition).Krieger Publishing Company, Malabar, Florida.

20 Žarković, M. i dr. (2010). Policijsko postupanje prilikom obezbeđenja mesta krivičnog događaja kao preduslov za uspešnu forenzičku identifikaciju. Nauka, bezbednost, policija Br.2. str.72-73

21 Zakonik o krivičnom postupku. „Službeni glasnik RS" br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014.

22 Paradine, K. & Wilkinson,J.(2004).The Reporting, Investigation and Prosecution of Domestic Violence Cases. National Centre for Policing Excellence, Centrex. HMcpsi. pg.47-53

question of false denunciation by victim and the reasons why she withdrew her statement, and assessing the possibilities that the public prosecutor took criminal charges against the victim for false denunciation? In other situation when it also comes to the same (dismissal of criminal charges), also, a victim does not want to prosecute the offender or she withdraws her statement, but there is other evidence that the violence had happened. The victim in the regular proceeding is asked if she wants to join the prosecution, although, it has no legal basis on that, because it is not required to have signed and agreed proposal from victim to prosecute. In these cases, especially if the offense happened for the first time, if there is no continuity of charges, if the victim does not want to join the prosecution and/or if there are minor physical injuries, very often it does not go into further proceeding.

Also, many analyses of court convictions show arbitrary judgment. For the same offence of Article 194 of the Criminal Code and the same paragraph of that article, one can observe the differences in the convictions. By researching, it has come to the conclusion that the practice in Vojvodina is more rigorous, in Central Serbia they convict to the minimum sentences, and in the southern parts of Serbia it is most disposed to probation or opportunity.[23] It is believed that one part of these findings stems from the existence of stereotypes of officials, the level of their sensibility and education, as well as the ways of achieving the cooperation among the institutions in the process of proving and protection of victims. In investigation, besides communication with the police, also, the public prosecutor has possibility to request a report and opinion of the centre for social work and to participate in case conferences. In fact, this situation often produces that the opinion of centre for social work is not requested and it is not proposed as evidence in court proceedings, although it may contain certain information that may indicate to history and continuity of violence, psychological experience of the victim, or to indicate the existence of fear, etc.

Disparity of treatment of victims in institutions and secondary victimization. The difference in treatment varies from town to town, from officer to officer. The disparity in treatment and secondary victimization is the mirror of officers who do not have the knowledge, but they lack training, understanding, have gender stereotypes, prejudices, superficiality in work and lack interest for adequately doing their own job.[24] The victims in the proceeding are treated differently, from humiliation to respect, depending on the effects of different factors. The procedure for the majority of victims becomes exhausting, they must again repeat the statement to all institutions, go through the suffering all over again, be face to face with the abuser, with stigma and criticism of society, and during the time, all this leads to the victim's wishes to leave the offender as well as institutions and begin to live a "normal" life.

Institutions secondary victimize the victims of violence, usually ignoring the problem, denying its existence, minimizing its importance, dissatisfying the needs of the victim, judging, blaming the victim, have insensitive and unprofessional approach, etc. The existence of prejudice and patriarchal beliefs is still present particularly with regard to the role of family members, so the public officers who should provide help, do not resist it, too.[25]

The introduction of legally obligated deadlines for treatment in public institutions in order to prevent delays in proceeding and disparity of court practice that we have mentioned above. We should also hold to the recommendations of the European Court of Human Rights on respect of the rights of victims to trial within a reasonable period of no longer than one year, from the denunciation of criminal charge until a final judgment/conviction.

The legislator did not harmonize two important laws (Criminal Code and Family Law) in the field of protection against domestic violence for many years, so the question should be asked, does the bringing of one new law, that will overcome the existing contradictions and consolidate all forms of treatment and determinations related to domestic violence and multi-sector cooperation, more precisely, bringing **one law on protection from domestic violence**, could improve the work of the court?! When we talk about good practice, we should mention that the adoption of one law which has family as a protective object, proved applicable in other countries, as already mentioned, in Austria. The law should contain in itself all aspects of international conventions and standards that we have ratified over the last years with the introduction of special measures of protection of the victims as participants in criminal proceedings.

Evaluation of the effectiveness of coordinated actions is the necessity of systematic approach to the problem. We need mechanisms for internal and external assessment of the effects, and in accordance with the goals and principles of multi-agency cooperation in the General protocol[26] considering that our institutional system does not have enough specific and clear indicators of the treatment effects.

23 Petrušić, N, Konstatinović-Vilić, S. (2010). Porodičnopravna zaštita od nasilja u porodici u pravosudnoj praksi u Srbiji. Autonomni ženski Centar, Beograd.

24 Spasojević, A. (2014). Posledice nasilja nad ženama i sekundarna viktimizacija. U Zbornik radova: Nasilje u Srbiji-uzroci, oblici, posledice i društvene reakcije,Tom 2, Kriminalističko-policijska akademija, Fondacija „Hans Zajdel", Beograd str..444-455;451.

25 Jovanović, S. (2012). Nasilje u porodici u Srbiji učinioci, žrtve i društvena reakcija. Revija za kriminologiju i krivično pravo. Vol. 50, br.1-2, str. 245-263.

26 Opšti protokol o postupanju i saradnji ustanova, organa i organizacija u situacijama nasilja nad ženama u porodici i u partnerskim odnosima (2012). Vlada Republike Srbije, str.21.

We should point out that the need for intensive cooperation with local governments is recognized in the field of raising awareness of local communities about domestic violence through campaigns, press conferences and publications, but also within financial support for the approval of funds for financing women's shelters, psychological and legal support for victims of domestic violence.

INSTEAD OF A CONCLUSION

Multi-agency cooperation represents a need to develop a systematic multidisciplinary approach and structure in response to domestic violence through strategies and operationalized acting so that they would be more successful. Incoherence between relevant institutions makes it difficult to act in specific situations or implement emergency procedures in detecting, stopping violence, protecting victims, providing evidence and prosecuting perpetrators. It seems more and more that the efficiency, adequacy and sensitivity to treatment are a consequence of the work and effort of individuals, their individual development, learning, and personal sensibilities, although all of that is the necessity of treatment prescribed by the law.

When considering multi-agency cooperation in Serbia, the analysis of practice and procedure, we can assume that the current way of handling various institutions is characterized by:

1) Insufficient education and sensitization of employees who act with insufficient knowledge of the roles, responsibilities, methods of operation, capacity constraints and other sectors;
2) The absence of well-defined ways of exchanging information relevant to treatment;
3) The absence of formalized procedures of joint action;
4) The absence of binding deadlines for the treatment and impunity omissions in the work of employees;
5) Inconsistent case law and the protection of victims;
6) Underdeveloped practice of joint evaluation of the actions and measures of implemented model and the evaluation efficiency of multi-agency cooperation;
7) The absence of a single database and a system for sharing knowledge about the acts of domestic violence.

It is necessary to observe these defects at the local and national level and provide effective suggestions for resolving them in order to improve cooperation between institutions.

REFERENCES

1. Đurđević, Z. (2014). Postupanje policije u slučajevima nasilja nad ženama u porodici i u partnerskim odnosima u: Integrisani odgovor na nasilje nad ženama u Srbiji, Simeunović, B, Kolarić, D. Kesić, T & Đurđević, Z. Kriminalističko-policijska akademija, Beograd.
2. Kirk, P (1985). Crime Investigation (second edition).Krieger Publishing Company, Malabar, Florida.
3. Žarković, M. i dr. (2010). Policijsko postupanje prilikom obezbeđenja mesta krivičnog događaja kao preduslov za uspešnu forenzičku identifikaciju. Nauka, bezbednost, policija Br.2. str.71-86
4. Zakonik o krivičnom postupku.„Službeni glasnik“ br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014.
5. Zakon o ratifikaciji Konvencije UN o eliminisawu svih oblika diskriminacije žena (CEDAW,1992), („Službeni list SFRJ-Međunarodni ugovori“ br.11/81)
6. Jovanović, S. (2012). Nasilje u porodici u Srbiji učinioci, žrtve i društvena reakcija. Revija za kriminologiju i krivično pravo. Vol. 50, br.1-2, str. 245-263.
7. Konstantinović-Vilić, S. Nikolić-Ristanović, V.(2003). Kriminologija. Pravni fakultet u Nišu.
8. Krivični zakonik Republike Srbije, „Službeni glasnik RS“, br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009 i 121/2012.
9. Logar, R.(2005). Austrijski model intervencije u slučajevima nasiqa u porodici. Evropska mreža protiv nasilja nad ženama. Autonomni Ženski centar, Beograd.
10. Nacionalna strategija za sprečavanje I suzbijanje nasilja nad ženama u porodici i u partnerskim odnosima(2011). „Službeni glasnik RS“ br.021/2011, Uprava za rodnu ravnopravnost, Ministarstvo rada i socijalne politike.
11. Opšti protocol o postupanju i saradnji ustanova, organa i organizacija u situacijama nasilja nad ženama u porodici i u partnerskim odnosima (2012). Vlada Republike Srbije,

12. Paradine, K. & Wilkinson,J.(2004).The Reporting, Investigation and Prosecution of Domestic Violence Cases. National Centre for Policing Excellence, Centrex. HMcpsi. pg.47-53.
13. Petrušić, N, Konstatinović-Vilić, S.(2010). Porodičnopravna zaštita od nasilja u porodici u pravosudnoj praksi u Srbiji. Autonomni ženski Centar, Beograd.
14. Porodični zakon Republike Srbije „Službeni glasnik RS" br.18/2005.
15. Spasojević, A.(2014). Posledice nasilja nad ženama i sekundarna viktimizacija. U Zbornik radova: Nasilje u Srbiji-uzroci, oblici, posledice i društvene reakcije,Том 2, Kriminalističko-policijska akademija , Fondacija „Hans Zajdel", Beograd str..444-455.
16. Univerzalna deklaracija o pravima čoveka, Rezolucija Generalne skupštine Ujedinjenih nacija 217A (III) od 10.12.1948.
17. Ustav Republike Srbije "Službeni glasnik" br. 48/94 i 11/98/2006.
18. http//:www.CPS domestic violence-good practice guidance, Attorney general 2005.; 20.01.2015.
19. http://www.cheshirewestlscb.org.uk/wp-content/uploads/2012/08/Multi-agency-practice-guidance-domestic-violence-maj-2013.pdf, Safeguarding children abused through domestic violence;20.01.2015.
20. http://www.un.org/documents/ga/res/48/a48r104.htm.Declaration on the Elimination of Violence against Women, A/RES/48/104. The General Assembly of United Nations.(1993).
21. http://www.conventions.coe.int/Treaty/EN/Treaties/Html/210.htm.Council of Europe Convention on preventing and combating violence against women and domestic violence.(2011).

UDC: 343.85:343.51(510)

THE ANTI-COUNTERFEIT MONEY ORGANIZATION IN CHINA

Liu Dan[1]

National Police University of China, Department of Economic Crime Investigation, Shenyang

Abstract: The counterfeit money crimes are the internationally recognized crimes which have caused serious harm to society. The anti-counterfeit money campaign has never ceased since the birth of the RMB banknotes. Counterfeit money crimes are still rampant, yet have become more difficult to detect. The Joint conference of the State Council on cracking down on counterfeit currency in China is the highest form of organization. The coordination office of the Joint conference is located in the People's Bank of China. To combat counterfeit money, the Ministry of Public Security Bureau has set up the functional department up to now. Cracking down on the counterfeit money crime is a complex social system project. Long-term, comprehensive and intensified efforts should be made in the crackdown on counterfeit currency.

Keywords: anti-counterfeit money, organization, joint conference, investigation.

INTRODUCTION

Currency is the value symbol and the circulation medium of the commodity, the product of civilized society and commodity society, which embodies the humanity values and materialization orientation. Currency has long been known as the card of the country. Counterfeit banknotes, like the shadow of authentic currency, have been in existence since the birth of currency. Dying hard, banknotes counterfeiting has been a chronic problem encountered by countries around the world ever since currency came into being. The counterfeit money is the common enemy of the whole world and a difficult global issue. It not only infringed the public economic interests, disrupted the order of currency circulation, but also hindered independence and integration of the currency system, even endangered social stability and state power. In the world history, the struggle against counterfeit money has never stopped. The illegal act of disrupting currency administration order is widely regarded as the serious crime in the economic field.

THE FEATURES OF COUNTERFEIT MONEY CRIME IN MODERN CHINA

Owing to pursuing high profits, with fluke mind to risk, objective environment where huge quantity of cash flows in the market is, the geo-economic and cultural reason, the ability to identify the authenticity, the disorder of social control mechanism in some districts, since the mid-1990s, China's counterfeit money crime has become increasingly active. In this regard, the public security organs have organized a series of special combat and concentration actions in key areas and effectively curbed the rising trend of counterfeit money crime. However, affected by many factors, counterfeit money crime situation is still not optimistic. The responsibility for anti-counterfeit work is grave.

During the past several decades, the features of counterfeit money crimes in China were as follows:

1) The average annual incidence fluctuated at high levels, the major cases occurred frequently, and the scale of crime also escalated.
2) The regional pattern of counterfeit crimes was clear and the crimes relatively concentrated in key areas.
3) The objects of crime were diversified, aiming at counterfeiting the large denomination. While manufacturing and selling counterfeit small denomination money increased.
4) The subjects were vulnerable people, such as elderly people and women, who mostly lived in the urban and rural areas.
5) The criminal means was usually concealed and it was difficult to discover.

1 sunshine_dan@126.com

6) The criminal forms are compound. The counterfeit money crime mingled with other crimes, such as drug, pornography, false invoices, gambling.

7) The criminal has the characteristic of cluster, forming some relatively fixed groups.

8) The criminals ganged up. The family or the fellow-townsman was linked to the counterfeit crime, and the criminal networks and chains were formed.

9) The consequences of counterfeit money crimes were serious. This has been an important factor to threaten the country's financial security.

JOINT CONFERENCE OF THE STATE COUNCIL FOR CRACKING DOWN ON COUNTERFEIT CURRENCY

The Joint conference of the State Council for cracking down on counterfeit currency in China was established in 1994, with 19 members from relevant ministries. The coordination office of the joint conference is located in the People's Bank of China (PBC). Currently, the joint conference members have been expanded to 28 units, including Legislative Affairs Commission of the National People's Congress, Publicity Department of the Communist Party of China Central Committee, the General Office of the State Council, the Supreme People's Procuratorate, the Supreme People's Court, the Ministry of Public Security, Ministry of State Security, Ministry of Foreign Affairs, National Development and Reform Commission, Ministry of Education, Ministry of Finance, China Railway Corporation, Ministry of Transport, Ministry of Industry and Information Technology, State Administration for industry and Commerce, Civil Aviation Administration, State Administration of Press, Publication, Radio, Film and Television, Hong Kong and Macao Affair's Office of the State Council, Tai Wan Affair's Office of the State Council, China Banking Regulatory Commission, Industrial and Commercial Bank of China, Agriculture Bank of China, Bank of China, China Construction Bank, etc.

The Joint conference of the State Council for combating counterfeit currency is primarily responsible for the leadership of the state council, reflecting the circumstances of national anti-counterfeit currency struggle, making recommendations concerning the work, organizing and coordinating the relevant departments to combat and prevent counterfeit crime activities, carrying out anti-counterfeit currency propagation, education and management functions. For example, on July 31, 2013, the 44th Liaison Officers' Meeting of the Joint Ministerial Conference on Anti-Counterfeit Currency was convened in Beijing. In the speech, the proposal of establishing a liaison mechanism on anti-counterfeit currency in the banking sector was deliberated and adopted. The Banking Sector Liaison Officers' Meeting on Anti-Counterfeit Currency is composed of the ICBC, ABC, BOC, CCB, BOCOM, 12 national joint-stock commercial banks and the Postal Savings Bank.

The anti-fake money campaign has never ceased since the birth of the RMB banknotes. Under the leadership of the Communist Party of China Central Committee and the State Council and with the support of the general public, relevant agencies have cooperated closely in the anti-fake money campaign, making progress in many aspects.

First, the working mechanism has been improved progressively. As the convener of the joint conference for cracking down on counterfeit currency under the State Council, PBC has been playing the role of an organizer and coordinator in fighting and preventing counterfeit currency, and has been improving the management of forged banknotes and the public education campaign on this subject. Under the umbrella of the joint conference mechanism, a similar mechanism has been established at the provincial, city and county levels, with a total of 1,964 anti-fake money joint conferences at local levels. Cross-regional cooperation mechanisms have also been set up in some provinces.

Second, earnest efforts have been made to crack down on crimes related to money counterfeiting, and positive results have been achieved in dedicated campaigns targeting the areas seriously affected by counterfeit currency-related crimes. Since 2004, thanks to the Autumn Wind Campaign, the Sharp Sword Campaign, the Lightening Campaign, the Chrysanthemum Dedicated Campaign and the 09 Action, a batch of key cases have been cracked and large amounts of fake money have been seized before they went into circulation.

Third, public education campaigns have been delivered in an in-depth and consistent manner. The PBC and financial institutions have disseminated information concerning counterfeit currency widely, in both urban and rural areas, in a way well received by the general public. In particular, since 2006, more than 100,000 anti-fake money education campaigns have been conducted nationwide, sending more than 100 million hand-outs, disseminating relevant information to more than 200 million people.

Fourth, the long-term mechanism on anti-fake currency education has been preliminarily established and has taken effects. At the beginning of 2007, the office of the anti-counterfeit currency joint conference

proposed to establish, within three years, an education network in towns and villages with a population of more than 100 people. The network should be managed by dedicated people at every level and in every village and should conduct outreach activities on a regular basis. As for urban areas, the education network is mainly based in key communities, aiming to provide effective information dissemination, timely feedback and effective prevention. Good results have been achieved.

THE MINISTRY OF PUBLIC SECURITY OF THE PEOPLE'S REPUBLIC OF CHINA

In 1995, to combat counterfeit money, the Ministry of Public Security Bureau set up the functional department which has operated up to now. Public security organs nationwide have striven to crack down on counterfeit currency-related crimes, paying special attention to money forging cases. However, the source of counterfeit money crime has not been eradicated, and the recurrent peril of counterfeit money crime still exists. In January 2009, China's Ministry of Public Security launched a special campaign against fake banknote crimes after high-quality fake notes were found ahead of the shopping-spree Spring Festival holiday.

The nationwide campaign of "Action 09" aims at cracking down on crimes of producing, selling and spending fake notes, especially in 10 major provinces including Guangdong, Fujian and Zhejiang, said vice-minister of public security Liu Jin-guo, at a national teleconference. During the 10-month campaign, whoever reports dens producing fake money will be rewarded with 300,000 yuan (44,000 US dollars). People who inform against fugitives of notes crimes, or report cases of selling, transporting and purchasing fake money, will get cash rewards. The ministry ordered public security units to give priority to detecting fake money cases, finding out sources of fake money, rooting out producing dens and destroying transport network. The country has busted more than 4,400 fake money cases and destroyed 44 producing dens since 2006. Fake 100-yuan notes, most starting with serial number "HD90", have been reported in more than 10 provinces and cities. The case aroused public concern as some low-quality money detectors failed to detect the fake notes. To safeguard the banknote, also nicknamed as "the country's business card", joint efforts from governments, banks and media have been made over the past month. The ministry's figures showed that the monthly average number of new cases under police investigation dropped from 398 in 2009, to 125 in 2010, and further to some 64 in 2011, a 10-year low. In October 2009, the Economic Crime Investigation Department of the Ministry of Public Security decided to establish the anti-counterfeit office.

Since 2009, China's public security organs have actively promoted the establishment of specialized anti-counterfeiting organizations. The Ministry of Public Security and Guangdong, Anhui, Zhejiang public security organs have set up anti-counterfeit professional teams. On the provincial, municipal and county levels, public security organs designated more than 3200 full-time anti-counterfeiting liaisons, devoted major efforts to strengthening infrastructure, and established an anti-counterfeiting lab to achieve a breakthrough in counterfeit tracing. At the provincial, municipal and county levels, public security organs designated more than 3200 full-time anti-counterfeiting liaisons, devoted major efforts to strengthening infrastructure, established anti- counterfeiting labs to achieve a breakthrough in tracing the counterfeit.

THE CIRCUMSTANCES OF CRACKING DOWN ON COUNTERFEIT CURRENCY IN THE PRESENT SITUATION

Since 2009, under the organization and coordination of the joint meeting on anti-counterfeit currency in China, the members of anti-counterfeit currency bodies have communicated with overseas counterparts to grasp the situation of major international issues related to counterfeit money. China has actively exchanged intelligence and cooperated with the United States of America, the United Kingdom, the European Union and Asian countries in the field of anti-counterfeit currency to further promote the international information and regional cooperation mechanisms to combat the crime of counterfeiting.

In the course of the investigation of counterfeit money crimes, Chinese public security organs persist in the fundamental principle of chasing sources, digging dens, cracking down on gangs, cracking major cases from beginning to end. Investigating the cases is placed in a prominent position. Important clues are regarded as a breakthrough. Collecting and fixing evidence is regarded as the main job. Tracing the source of dens and destroying the criminal network are regarded as the basic objectives.

Broadening clues channels, actively obtaining case clues. (1) Mobilizing report from the masses. Through reporting telephone, setting propaganda points, sending messages, microblog, mobile car pro-

motion, television advertisement and other forms provide clues of counterfeit currency crime cases. (2) Obtaining valuable clues from secret power of the key industries, key districts, key positions and from railway stations, docks, entertainment venues and other complex areas. (3) Collecting clues from the staff of financial institutions and the business sector. In 2009, the Ministry of Public Security and the PBC jointly issued the note on further strengthening the anti-counterfeit work, made definite duty of financial institutions in the conduct of handling business. Any bank or any other banking institution who found more than 500 counterfeit RMB shall immediately notify the public security organs. Once a fake RMB denomination of more than 200 yuan is found, any bank or any other banking institution shall notify the public security organs in the same day. After receiving a report from financial institutions, police security organs should be quickly conduct on-site disposal. The counterfeit money suspect may be brought back to public security organ for the further survey. For better sorting counterfeit crime clues, promoting the establishment of financial institution monitoring system of counterfeit money, collecting the information about counterfeit money, counterfeit money holders, the time and the location of capture. So the public security organ or financial institution may draw the intelligence on key areas and key points of counterfeit seizure from statistical analysis.

An important role is played by criminal investigation technology. (1) Through the meticulous inquest or examination of involved storage scene of counterfeit money and suspected residence, extracting the suspect's fingerprint in contact with the position, the traces and articles such as the package of fake money, the cup that the suspect used, lipstick and cigarette butts that the suspect may contact, etc. (2) Using a wide variety of criminal technical methods, such as photographing, fingerprint identification, expert evaluation, etc. (3) Through handwriting identification of the suspect's sale account book and other documents, restoring the on-site torn notebook, the handwriting of the suspect may be confirmed. (4) Through analyzing and testing the sample of counterfeit money seized, identifying the printed version, the method of printing, printing ink used, comparing the sample captured and the sample of fake money in the case cracked down by public security organs.

Accurately grasp the filing conditions. In the substantive sense, criminal law is a law that defines the framework in which society conducts deterrence and punishment. To put it in another way, criminal law is a law that seeks to classify whether a conduct is a crime and if so, what kind of punishment or criminal liability shall be imposed for such conduct? As such, when we learn the substantive criminal law, we always tend to ask the questions: if A commits an act, does A's act constitute a crime? If yes, what kind of punishment should be imposed on A? While the question of whether an act constitutes a crime is defined by the substantive criminal law, the question of how to implement the substantive criminal law's goals is defined by criminal procedure law. Generally speaking, criminal procedure law comprises rules regulating the inquiry into whether an offence has been committed, and if so, who was it committed by. According to the Procedure Law of the People's Republic of China, the Public security organ shall, within the scope of its jurisdiction, promptly examine the materials provided by a reporter, complainant or informant and the confession of an offender who has voluntarily surrendered. If it believes that there are facts of a crime and criminal responsibility should be investigated, it shall file a case. If it believes that there are no facts of a crime or that the facts are obviously incidental and do not require investigation of criminal responsibility, it shall not file a case and shall notify the complainant of the reason. In order to enforce the provision of the criminal law, the Supreme People's Procuratorate and the Ministry of Public Security promulgated the Provisions relating to filing and prosecuting standards in the criminal cases of the public security organ having jurisdiction in 2010. Under the provisions, the lowest amount standard for crime of smuggling counterfeit currency, crime of counterfeiting currency or crime of altering currency is total RMB 2000 yuan or 200 pieces. The lowest amount standard for crime of selling or purchasing or transporting counterfeit currency, crime of buying counterfeit currency or exchanging counterfeit currency for genuine ones or holding or using counterfeit currency is total RMB 4000 yuan or 400 pieces.

Investigation involves the specialized investigatory work and related compulsory measures carried out according to law by the public security organs in the process of handling cases. Collecting the image data, and assisting investigation into the counterfeit money crime cases, especially noting the storage point for counterfeit money involved, the suspect processing point and public video surveillance data around the suspect's house for rent, so as to support outside tracking and the successful completion of arrest. Make use of the electronic technology to support the trial. Through examining the computer, a lot of evidence of electronic data involved with the case inspection may be successfully extracted and fixed. For supporting in the work of the trial and investigating the facts relative to the case, a number of related information associated with the suspect may be found through comparing and analyzing the collected data.

How to apply the intelligence to investigating counterfeit money crimes? For example, in recent years, with the determination of the public security organs to carry out the fight against the crime of counterfeiting, and as a result of constantly heightening public awareness of precaution, the rampant counterfeiting, selling and using counterfeit money crime has been effectively curbed, but the cases of using small denomination money are still serious, relatively concentrated on the numerous unmanned buses. Some bus

companies have borne the heavy economic losses in recent years. In order to understand the case circumstance of bus using counterfeit money in the special district, to work out the effective countermeasures, and to shrink space of using fake money in the bus, the economic crime investigation department of public security bureau has carried out extensive research into using fake money in each bus company and some of the bus stations. Seven problems of using the counterfeit money were analyzed by the economic crime investigation department. The first problem is the growing tendency to use the amount of counterfeit currency received from the bus in recent years. The second problem is receiving counterfeit coins basically, and there are many miscellaneous coins. The third problem is the large quantities of counterfeit money received through rural, urban and suburban bus lines. The fourth problem is mainly the staff beyond the city using the counterfeit money. The fifth problem is that the city bus terminal is the important source using counterfeit money. The sixth problem comprises anti-counterfeit practices and things encountered in the bus company. The seventh problem is the proposal for cracking down on counterfeit money crime. Through getting rid of the false, preserving the true from the these original information, proceeding from the outside to the inside, the investigators can draw some conclusions from the discussion, including the type of counterfeit currency, the amount of counterfeit currency received, the personnel of using counterfeit currency, the sites of using counterfeit currency, bus company practices and encountered problems. The recommendations aimed at countermeasures against fake notes are presented as follows: checking up on the passenger stations and bus stops, strengthening interrogation and inspection, collecting and researching the counterfeit money information, promoting the use of public transportation ticket payment, universal installation of counterfeit identification, etc.

CONCLUSION

We need to acknowledge that counterfeit money crime is transnational. Cash includes both local and foreign currencies. Many banks do not have rich experience in foreign currency business. The employees of a bank or of any other banking institution are not quite familiar with foreign denominations, especially the background of issuance, the features related to compositions, colors, pictures, dimensions and the other security features. They still need to practice more to gain the same rich experience as with the local currency. And the only way to address it effectively, efficiently and intelligently is by addressing it together.

We need more communication, information and expertise. All these are beneficial to the stability of currency and economy, finance and social order, and will assist in combating transnational currency crimes. Long-term, comprehensive and intensified efforts should be made in the crackdown on counterfeit currency, so as to safeguard the public interests in an effective manner. This means establishing a dialogue, developing and supporting initiatives, efficiently applying them across Asia, and even in the world.

REFERENCES

1. Liu Dan, Wan Jin-dong, Liu Ye (2010). Construction of the System of the Counterfeit Money Crime Prevention. China Public Security, 2010(4), pp. 110-113.
2. Chen Xiang-min, Liu Dan (2009). Journal of Chinese People's Public Security University (Social Sciences Edition), 2009(2), pp. 135-139.
3. Criminal Law & Criminal Procedure Law (2007), China Legal Publishing House, pp. 249.
4. Chen Bao-shan (2006). Shuibanchi. China Financial Publishing House, pp. 148-149.
5. Ma De-lun (2011). Chinese card Renminbi. China Financial Publishing House, pp. 294-296.
6. The People's Bank of China (2009). Fighting Counterfeit Currency: A Joint Responsibility For All. http://www.pbc.gov.cn/publish.
7. The People's Bank of China (2013).The 44th Liaison Officers' Meeting of Joint Ministerial Conference on Anti-Counterfeit Currency Held in Beijing. http://www.pbc.gov.cn/publish.

UDC: 343.91-053.6(510)

EXPLORING INFLUENTIAL FACTORS OF JUVENILE DELINQUENCY IN CHINA

Wei Wang[1]

National Police University of China, Department of Public Security Fundamentals, Shenyang

Abstract: Youth crime has been increasing rapidly since the Economy Reform and Open-door Policy in 1979 and has become a serious social problem in China. Researches on explanations of juvenile delinquency, however, are relatively limited. An integrated model is addressed through a self-reported survey with 377 respondents. The respondents are high school students in the city of Shenyang, aged from 16 to 18. Data from the questionnaire survey suggests that these three theories could explain Chinese youth crime. Two separate Ordinary Least Squares (OLS) models are built for analyzing delinquency of males and females. Predictors related to delinquent friends are directly associated with violent delinquency among Chinese adolescences. Males and females are influenced by different factors when they are involved in delinquency. This paper concludes with a discussion of establishing an integrated model of protection programs to prevent juvenile delinquency in China.

Keywords: juvenile delinquency, delinquent friends, school attachment

INTRODUCTION

Juvenile delinquency has been the dominant theme in criminology for several decades. Many of these theories have been established, tested, amended and retested numerous times. This procedure of theoretical development has continued for more than one century in western countries, but there have been few theories translated to non-western nations. China, in particular, has been ignored and isolated by the world of criminology for a long time[2]. One of the reasons for this ignorance is that, after the foundation of the People's Republic in 1949, China presented itself internationally as an almost crime free society, with a very low crime rate between 1950s and 1960s[3]. Moreover, official crime statistics were not reported whatsoever during the 1970s due to the 'Culture Revolution'.

More recently, while both scholars and policymakers have become concerned about juvenile delinquency as a social problem, the research is still relatively limited and short of empirical data. Moreover, few studies have tested western theories of juvenile delinquency in the Chinese environment partly due to the difference of culture backgrounds and the unique political orientation of "socialism with Chinese characteristics". The criminological research in China is relatively preliminary and there is a "lack of standardized research method"[4], considering the discipline's relatively short history and the government's traditional ignorance of social science studies in the country.

This study aims to fulfil the gap of lacking empirical research on juvenile delinquencies in the Chinese context and attempts to explain how social factors may affect deviant behaviours conducted by adolescences. This paper will first discuss the definitions of several key concepts. Research on this issue is also analyzed. It follows with the methods and data collecting process. Results and discussions are presented at the last part of the paper.

DEFINING JUVENILE DELINQUENCY IN CHINA

In legal systems, the word "juvenile" was created to describe any person under the legal age of adult, which is 18 years of age in most countries. Legislators also provided a minimum age for young offenders, indicating that children under that specific age would be exempted from punishment because they lack criminal intent. Thus "juvenile" can indicate various ages of children according to young offender acts or criminal laws in different countries. In the United States, the minimum age of criminal responsibility was

1 shrubww@yahoo.com
2 See Bakken, 2005
3 See Guo, 1999
4 See Zhou & Cong, 2001

set at seven; Canada extended the jurisdiction of juvenile court from twelve to eighteen years; children above the age of fourteen years could be held responsible for criminal acts in Germany[5].

China, contrary to the western countries, has a long history of separating juvenile from adult justice and punishment. For instance, during the Han Dynasty (206 B. C. – 220 A. D.), the first emperor set up criminal laws with the clear remission for children, senior citizens, women, and individuals with disabilities. A child under the age of eight years, who committed a crime other than murder, would not be punished. An offender who was younger than ten years old would be exempted from death penalty and corporal punishment. In the Chinese legislative history the consideration and leniency towards juvenile offenders have existed consistently for thousands of years, and these traditions have been inherited by the communist regime. According to the Criminal Law, a juvenile in China refers to any person aged from fourteen to eighteen years. However, despite these age limitations in the Criminal Law, the term "juvenile", in China, sometimes does not exactly refer to children from fourteen to eighteen years old. In several categories of official criminal statistics and research literature, the definition of a juvenile is extended to the mid-twenties. Indeed, in China, "juvenile" is not a precise concept in both the justice system and the academic world. However, for the convenience of research and comparison, in this study, the word juvenile is based on the definition of juvenile in western literature and the Criminal Law of China and refers to children aged from fourteen to eighteen years.

Delinquency frequently refers to the violation of law committed by a juvenile. It is another concept with multiple meanings and various definitions in different countries and societies as well. Delinquency is dependent upon social norms. Most definitions of juvenile delinquency could be generally divided into three categories by different emphasis: the legal definition, the role definition, and the societal response definition[6]. After several bills and acts were passed by legislatures, juvenile court was initiated at the beginning of 20th century and since that time juvenile delinquency has legally been referred to "any act that, if committed by an adult, would be a crime"[7]. Some activities of youth were not criminal in the criminal law, but still disturbed the peace or infringed on the broad interests of communities. The legislators also considered these kinds of behaviour as illegal, such as truancy, running away from home, and consumption of alcohol beverages. Thus the status offense refers to several types of conduct which would not be considered as crimes if committed by an adult, but which are illegal and inappropriate for juveniles. The role definition of juvenile delinquency focuses on juveniles, "who sustain a pattern of delinquency over a long period of time and whose life and identity are organized around a pattern of deviant behaviour"[8].

As norms are created by society and delinquency is a norm-violating behaviour, the social response to behaviour is a crucial factor to decide if it is delinquency or not. This definition indicates that delinquency is a result of social interaction. Typically, a juvenile becomes delinquent legally and officially when labelled by judge or jury at a juvenile court. Due to culture differences, delinquent behavior varies from one country to another. With the consideration of all three categories, delinquent behaviour in China is quite different from that in North America. Legally speaking, delinquency in China is not entirely referred to as any conduct which would be a crime if committed by an adult. According to the Judicial Explanation by the Chinese Supreme Court, implemented in January of 2006, there are several exceptions for illegal conduct for juveniles. For instance, under the age of sixteen, a juvenile has limited criminal responsibility only for homicide, aggravated assault, rape, robbery, drug dealing, arson, explosion, and poisoning. Most misconduct considered as delinquency in western countries will not be legally "delinquent" in China and will not be, in many cases, prosecuted in the formal justice system. However, social audiences, such as parents, teachers, and peers still judge them as delinquency informally. Moreover, it is highly possible that teachers may provide a 'delinquent' label to those children who rob, steal, or commit an assault.

In addition, status offense does not legally exist in any laws related to juvenile in China. Truancy, running away from home and consumption of alcoholic beverages do not violate laws and are not considered delinquency per se. According to the social response definition, however, truancy and running away from home are still considered as delinquency by the social audience in the Chinese context.

In this study, the definition of delinquency is based on a sociological perspective, incorporating the legal definition, the role definition, the social response definition and the specific concerns of the situations in China. It is a broad concept, referring to any conduct which violates laws or is considered as inappropriate for juveniles by the social audience in the Chinese context. As the research population includes high school students, not young offenders in jails, this paper excludes serious delinquency for which juveniles can be held responsible, such as homicide, aggravated assault, rape, severe robbery, drug-dealing, arson, explosion, and poisoning, and only explains minor offenses, such as fight, theft, minor assault, and truancy.

5 See Albrecht, 2004
6 See Bynum and Thompson, 2007
7 Bynum and Thompson, 2007: 8
8 Bynum and Thompson, 2007: 12

STUDIES ON JUVENILE DELINQUENCY IN CHINA

Only a few studies on Chinese juvenile delinquency can be found in western literature, and some of them are not adequately supported with empirical data. Bao and his colleagues[9] first used general strain theory to explain juvenile delinquency in the Chinese context. They examined both direct and indirect effects of negative interpersonal relations on delinquency and found that the combination of strain and anger increased the risk of criminal conduct, and that negative relationships with other people in juveniles' immediate life environment, especially family and school, had significant impact on delinquent behaviour. Consistent with this research, Bao et al.[10] examined whether social support from family, school, and peer group would mediate the relationship between strain and delinquency. They found that males were more likely to join in delinquent peer groups to alleviate strain, whereas females preferred cross-domain support for managing interpersonal strain. Liu and Lin[11] reported that strain variables were positively associated with delinquency for males and females. Strain of status achievement, such as frustration with course grades, career, and college education, was more strongly associated with boys' delinquency, whereas girls were more influenced by strain linked with physical well-being. Lower self-control, association with delinquent peers, deviant attitude, and father's education were also positively related to delinquency. Drissel's[12] longitudinal birth cohort survey revealed that young offenders were typically from lower-class, and had low education and strong association with delinquent peers. He also found that delinquent youths were influenced by subterranean values which were produced by social and economic changes in China, such as pursuing "big money" and "power and influence", ignoring reputation and family. Zhang and Messner[13] reported that weaker family attachment would result in stronger association with deviant friends that had positive relationship with delinquency and that youths from low SES family or having deviant family members were more likely to commit crime. In addition, several studies discussed explanations of juvenile delinquency in China based on labelling perspectives and analyzed the impact of peers[14], self-esteem[15], the relationship between official severity of punishment and interpersonal estrangement[16], and the effectiveness of reintegrative shaming theory. Moreover, many scholars have devoted more effort to studying the juvenile justice system[17] and the Law on Protection of Juveniles rather than the explanations of the problem[18].

The research on juvenile delinquency written in the Chinese language is still limited and problematic as most studies remain philosophical, with little empirical evidence. Perspectives of biological characteristics of the individual, family structure, failure of school education, and rapid changes of social structure are all presented typically in one single paper with little empirical data[19]. When discussing family factors, researchers usually argue that delinquency is caused by broken family, negative relationship with parents and the parental indulgence of children. Lack of introduction to basic law and justice education in school and neglect by teachers are considered school-related predictors of delinquency. Almost all above research discusses prevention strategies ideologically and philosophically based on the Chinese Marxist theories, but none of them provides evidence supported from the real world, although there are various relative prevention programs supported by the Communist Youth of League or other social organizations in most cities.

THE CURRENT STUDY

This study will explore several important social factors and examine how these factors may have an impact on juvenile delinquencies in China. As previous studies have indicated that for understanding juvenile delinquency, a single criminological theory may not provide a thorough explanation to the issue. The current study attempts to establish an integrated model to explain juvenile delinquency in China. Data were derived from a survey of students in December, 2014, in five high schools in Shenyang, about 700 kilometres north from Beijing, the capital of Liaoning Province and a typical inland city in China. The sample contains 377 students, almost evenly divided between males (47%) and females (53%), aged from 16 to 20 years, and enrolled in the 10th to 12th grades in public schools. A total number of students was 3,550 during the investigation period and the sample represented around 10% of the research population.

9 See Bao et al., 2004
10 See Bao et al., 2007
11 See Liu & Lin, 2007
12 See Drissel, 2006
13 See Zhang & Messner, 2005
14 See Zhang, 1994
15 See Zhang, 2003
16 See Zhang & Messner, 1994
17 See Guo, 1999; Zhao, 2001
18 See Zhang & Liu, 2006
19 See Wang, 2007; Tan, 2008; Wu & Cui, 2008; Wu, 2004

An anonymous survey was employed to collect data and a self-reported questionnaire was designed in the Chinese language to better reflect the actual meanings of the responses. High school students were invited to participate in this study during their self-studying period typically from 3:00 pm to 4:30 pm. There were no teachers or administrators in the classrooms when students were filling out the questionnaires. All questionnaires were anonymous and no identifying marks were on the questionnaire, which was put, sealed in a brown envelope, and returned by the participants, no matter whether it was completed or not. Four hundred questionnaires were sent out to students in five different high schools, and 385 of them were returned. The number of valid and completely answered questionnaires was 377.

The average age of the respondents was 17.6 years old, and 3.7% of respondents were older than 18 years. The sample was almost evenly divided among males (47%) and females (53%). Most fathers of the respondents had graduated from high school or above (60%), and most mothers were reported as having high school certification or above (64%), while few fathers and mothers graduated from colleges (14% and 16%). Less than 15% of the respondents reported that their family income levels were in poverty or near poverty.

MEASUREMENTS

Dependent Variables

Two indicators were constructed for the dependent variables. The first measure was self-reported violent behaviour including seven items presenting the frequency of involvement in violent activities in the most recent three years. Respondents were asked how often (from none to more than twenty times) in the recent three years they committed violent offense, were involved in gang fights, and carried a weapon to school. A total of 34.9% of respondents indicated they were involved in violent behaviour at least once (Cronbach's alpha= .792).

Academic misconduct in this study was constructed with two items including absent from school and cheating on examinations (Cronbach's alpha = .594). Around half of respondents (48.9%) reported at least one of these two acts and significant differences were found between males and females ($p < .001$).

Property delinquency in this study included three variables: shoplifting, stealing money or things worth less than $50 Chinese dollars, and stealing more than $50 (Cronbach's alpha = .595). This scale was also different among boys and girls ($p < .05$).

Independent Variables

Differential association was measured in two categories: friends' delinquency and numbers of delinquent peers. Friends' delinquency was gauged with a 9-item scale, which represented the frequency of deviant conducts which the respondents' friends committed in past three years, from 1 = never to 4 = always (Cronbach's alpha = .814).

Parental attachment was measured with two items to indicate the extent of adolescents' association with their parents: 1) "I get along with my parents" and 2) "I respect my parents". Respondents were asked to rate the level of their agreement with these two descriptions from 1 = strongly disagree to 5 = strongly agree. School attachment was measured with attitude towards school and the closeness with teachers in this study. Respondents were asked to identify their feelings toward school, from 1 = strongly dislike to 4 = strongly like. They rated their agreement with the statement "I get along with most teachers of mine" at five different levels from 1= strongly disagree to 5 = strongly agree to indicate their relationship with teachers. Involvement was measured with a single item, "Generally, I spend little time on my studying".

Control Variables

In this study, SES was an additional measure to predict delinquency. It was measured with parents' education level and family income level. Both father's and mother's highest education levels were employed by (1 = more than high school, 2= high school graduated, 3 = less than high school). Respondents were asked to estimate their family income at five different levels from wealth to poor, and values of "wealth" and "comfortable" were recoded to 1 = high; category 2 = medium was constructed by "adequate"; "difficult" and "poor" were combined to 3 = low. Parental abuse was measured by being physically abused and mentally abused by parents. The participants were asked to describe how frequently they were physically/mentally abused by their parents (1 = never, 2 = sometimes, 3 = often, and 4 = always).

RESULTS

Males and females are reported separately because the direct and indirect predictors are different in these two models. Only those variables which provided significant Pearson correlations with endogenous variables were selected as independent variables in each single OLS regression analysis. Table 1 showed all coefficient correlations for the males' model. The model could explain approximately 46% of variance in violent behaviour, 41% variance in academic misconduct, and 14% in property delinquency. Two independent variables were significant in the violent behaviour model; two variables statistically predicted academic misconduct; none significantly affected property delinquency. Females' model was presented in Table 2. This integrated model could explain approximately 28% variance in female violence, 27% variance in academic misconduct, and only 4% for property delinquency. "Friends' delinquency" and "school attachment" were two direct predictors of female violence; academic misconduct was impacted by "friends' delinquency" and "parental attachment"; and "friends' delinquency" was a single significant predictor of property delinquency. The current study appears to provide little explanation of property delinquency. One of the possible reasons for this weakness might be lack of sufficient cases of property delinquency. The total sample number was 377 and only 8% of participants reported they had committed property delinquency. When separated by gender, the valid cases declined rapidly. Therefore, the hypothesis of integrated model might be inadequate for property delinquency.

Table 1 *Influential factors and delinquency (Male)*

Independent Variables	Violent behaviour		Academic misconduct		Property delinquency	
	Beta	Sig.	Beta	Sig.	Beta	Sig.
Friends' delinquency	.164*	.065	.087	.341	.009	.932
Numbers of delinquent peers	.413***	.000	.206**	.017	.161	.118
Parental attachment	---	---	-.014	.842	-.048	.556
School attachment						
Attitude to school	-.027	.708	-.058	.431	-.129	.147
Commitment						
Self-reported course grades	---	---	.018	.784	---	---
Involvement						
Spend little time in studying	-.028	.681	.174**	.023	-.039	.645
Abuse by parents						
Physical	-.022	.730	---	---	---	---
	R^2 = .460		R^2 = .413		R^2 = .143	

Table 2 *Influential factors and delinquency (Female)*

Independent Variables	Violent behaviour		Academic misconduct		Property delinquency	
	Beta	Sig.	Beta	Sig.	Beta	Sig.
Friends' delinquency	.391***	.000	.331***	.000	.139	.060*
Parental attachment	-.081	.268	-.173**	.022	---	---
School attachment						
Attitude to school	-.140*	.062	-.054	.492	---	---
Get along with teachers	---	---	-.045	.524	---	---
Commitment						
Self-reported course grades	---	---	.030	.679	---	---
Involvement						
Spend little time studying	-.023	.758	.061	.449	---	---
Abuse by parents						
Physical	.022	.763	.056	.373	---	---
Mental	.011	.886	-.026	.744	---	---
	R^2 = .277		R^2 = .269		R^2 = .043	

DISCUSSION

Differential association was consistent with previous studies and the strongest predictor of violent behaviour for both boys and girls[20]. This variable was also the strongest predictor of academic misconducts for boys, while it was ranked as the second strongest predictor for girls. The quantity of delinquent peers was a better indicator of male delinquency, while the extent of delinquency which girls' friends conducted was more significantly associated with delinquency.

For boys, both parental attachment and school attachment had negative effects on strain, indicating that strong attachment would reduce the experience of negative events and relations, while for girls, only school attachment affected general strain, and subsequently had negative effect on violence. In addition, social bonds had direct impact on academic misconduct, although the effective variables were different between boys and girls. Previous studies also provide similar results regarding the relations between social bonds and deviance[21]. The finding showed that males with high involvement in conventional activities were less likely to be involved in school based deviance, and that parental attachment was more effective to predict female deviance in school than that for males. In the current study, different types of experience of abuse were found to be indirectly associated with self-reported delinquency among genders. Physical abuse was a better predictor of both violent and academic misconduct for boys, while being mentally abused by parents was significantly associated with general strain and differential association, and indirectly affected female delinquency.

CONCLUSION

The current study examines the impact of several influential factors on juvenile delinquency and has several policy implications. First, some programs on role-model establishment might be helpful. *Big Brothers/Big Sisters* is one of the best-known programs to build up connections with pro-social individuals who can provide youths with positive values of law abidance and discourage involvement in delinquency. Volunteers such as teachers, college students, police officers, athletes, business owners, and doctors will accompany one younger person face to face for certain hours in a week to discuss the issues in the child's life, and provide support of his/her personal, social, academic, and other conventional activities. The above projects could be employed to prevent Chinese juvenile delinquency.

In addition to controlling the influence of delinquent peers, the current study also provides evidence of the importance of parents in the prevention programs. Family is the primary and vital place for children to get socialized. It is unfair to only blame children for their delinquency; parents also hold responsibility for problematic youth because unpleasant family environment, parental rejection, and family violence are all sources of juvenile delinquency. It could be arguable that parents need to 1) communicate with children openly and encourage them to talk about their life and interest; 2) set up clear and consistent rules and discipline at home; 3) provide effective supervision; 4) find peaceful resolutions to conflict; 5) keep children away from violence in home, media and community; and 6) be aware of children's friends and places where they usually hang out. These suggestions establish effective supervision, positive parent-child relationships, and family support, which could strengthen parental bonds and eliminate strain created by family. In addition, programs focusing on successful parenting in schools or communities could be also useful because a large number of Chinese parents lack effective skills to raise and educate their children. Moreover, parental discipline and punishment should be appropriate and adequate. The old words "spare the rod, spoil the child" might not be as effective as it worked in the "good old days". Family education is indeed important, but it should be acceptable to children. Some parents have no intention to abuse their children, but just use an unappreciated way to educate them. When the children consider discipline or punishment as abuse, they are more likely to associate with antisocial peers seeking support and release.

REFERENCES

1. Albrecht, H. J. "Youth justice in Germany". In *Youth crime and youth justice: Comparative and cross-national perspectives.* (Eds. M.Tonry & A. N. Doob. Chicago, 2004: The University of Chicago Press.

2. Bakken, B. 2005. *Crime, punishment and policing in China.* Lanham: Rowman & Littlefield.

3. Banyard, V. L., Cross, C., & Modecki, K. L. 2006. Interpersonal violence in adolescence: Ecological correlations of self-report perpetration. *Journal of interpersonal violence, 21(10): 1314-1332.*

20 See Thornberry et al., 1994; Warr & Stanford, 1991

21 See Banyard et al., 2006; Le et al., 2005

4. Bao, W., Haas, A., & Pi, Y. 2004. Life strain, negative emotions, and delinquency: An empirical test of general strain theory in People's Republic of China. *International journal of offender therapy and comparative criminology, 48(3), 281-297.*

5. Bao, W., Haas, A., & Pi, Y. 2007. Life strain, coping, and delinquency in the People's Republic of China: An empirical test of general strain theory form a matching perspective in social support. *International journal of offender therapy and comparative criminology, 51(1): 9-24.*

6. Bynum, J. E., & Thompson, W. E. 2007. *Juvenile delinquency: A sociological approach*. Pearson Education, Inc.

7. Drissel, D. 2006. Subterranean sources of juvenile delinquency in China: Evidence from birth cohort surveys. *Asian criminology, 1(2): 137-154.*

8. Feng, S. 2001. Crime and crime control in a changing China. In *Crime and social control in a changing China.* (Eds. J. Liu, L. Zhang, & S. Messner) Westport: Greenwood Press.

9. Guo, X. 1999. Delinquency and its prevention in China. *International Journal of Offender Therapy and Comparative Criminology, 43 (1): 61-70.*

10. Le, T. N., Monfared, G., & Stockdale, G. D. 2005. The relationship of school, parent, and peer contextual factors with self-reported delinquency for Chinese, Cambodian, Laotian or Mien, and Vietnamese youth. *Crime and delinquency, 51*(2): 192-219.

11. Liu, R. X., & Lin, W. 2007. Delinquency among Chinese adolescents: Modeling sources of frustration and gender differences. *Deviant behavior, 28(5): 409-432.*

12. National People's Congress. 1997. The Criminal Law of the People's Republic of China. *Gazette of the Standing Committee of the National People's Congress of the People's Republic of China*. No 2.

13. Thornberry, T. P., Lizotte, A. Krohn, M., Fanworth, M., & Jang, S. 1994. Delinquent peers, beliefs, and delinquent behavior: A longitudinal test of interactional theory. *Criminology, 32(1): 47-83.*

14. Warr, M., & Stanford, M. 1991. The influence of delinquent peers: What they think or what they do? *Criminology, 29(4): 851-866.*

15. Zhang, L. 1994. Peers' rejection as a possible consequence of official reaction to delinquency in Chinese society. *Criminal justice and behavior, 21*(4): 387-402.

16. Zhang, L. 2003. Official offense status and self-esteem among Chinese youths. *Journal of criminal justice, 31(2): 99-105.*

17. Zhang, L., & Messner, S. F. 1994. The severity of official punishment for delinquency and change in interpersonal relations in Chinese society. *Journal of research in crime and delinquency, 31*(4): 416-433.

18. Zhang, L., Messner, S. F., Lu, Z., & Deng, X. 1997. Gang crime and its punishment in China. *Chinese Sociology and Anthropology, 31 (4): 8-14.*

19. Zhang, L., & Liu, J. 2006. China's Juvenile Delinquency Prevention Law: The law and the philosophy. *International journal of offender therapy and comparative criminology, 51(5): 541-554.*

20. Zhao, G. 2001. The Recent Development of Juvenile Justice in China. In *Crime and social control in a changing China.* (Eds. J. Liu, L. Zhang, & S. Messner) Westport: Greenwood Press.

21. Zhou, L., & Cong, M. 2001. Criminology in China: Perspectives and development. In *Crime and social control in a changing China.* (Eds. J. Liu, L. Zhang, & S. Messner) Westport: Greenwood Press.

UDC: 343.37
343.53

CHARACTERISTICS OF ECONOMIC CRIMES IN THE FIELD OF DOCUMENTARY EXAMINATION AND MAIN COUNTERACTION TRENDS

Yanling Wang[1]
Hui Zhang
China Criminal Police College, Forensic Science Department, Shenyang

Abstract: Economic crime includes corruption, bribery, smuggling, money-laundering and credit card fraud. The main motivation of economic crimes is great benefit. From the regional perspective, the transfer of economic crime is from the southeast coast to the central and western regions. Means of crime shows a collusion trend of internal and external personnel. The influence of economic crime is sometimes international.The main methods and tools of majority economic crimes are computer, net and express. Necessary measures should be taken to combat economic crime. As individuals, we should strengthen the education of people and establish the correct values. The paper deals with the strengthening of the financial bill management, the secret control of communication, mail, telegraph, telephone and network, actively carrying out international cooperation in law enforcement as to establish wide report network and strengthen the daily supervision and block the loopholes in the system.

Keywords: economic crime, document examination, counteraction trend.

Economy penetrates the social life. Therefore, economic crime is everywhere. Economic crime, as a high incidence of multiple situation, has increasingly become the mainstream of crime, seriously disrupting the order of the market economy. Additionally it is a threat to national economic security. From the domestic point of view, the current financial, trade, finance, securities, and other fields of the economic crime cases occur frequently. Huge amounts of money are involved. Eeconomic crime has become a hazard factor of national economic security. From an international perspective, competition in the integration of the world economy, and the international economic competition brings more risk and uncertainty to the economic security of our country. The economic struggle has increasingly evolved into a political struggle, and an issue of economic security in the proportion of national security.

THE MAIN MOTIVATION OF ECONOMIC CRIMES IS GREAT BENEFIT

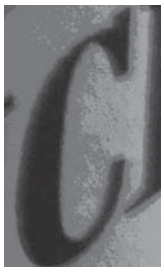
In order to change the living conditions, the unemployed in the city and the floating population want to gain wealth. But they lack the basic conditions for legitimate competition or appropriate opportunity. Therefore, some people commit economic crime mainly concentrated on the profiteering industry. They obtain huge profits from the illegal acitivities, such as infringement of trademark crime in the course of creating fake alcohol.

There is a kind of alcohol named Mao Tai in China which is made from Guizhou province with a long history. It is very expensive. Suspects pay more attention to it. They made fake Mao Tai alcohol while they made false trademark at the same time.

1 040423xiaoxiao@sina.com

Unknown

Samples



All photos are unknown, and the pattern of printing is lithographic printing.

The photos on the left are unknown while the photos on the right is/are a/some letter(s) of the photos on the left . We can judge from the characters of printing that the unknown trademarks belong to lithographic printing.

Samples

Relief printing

The photos on the left are samples while the photos on the right is/are a/some letter(s) of the photos on the left. We can judge from the characters of printing that the sample trademarks belong to relief printing. We can see from the point of printing the method of printing is different between the unknown and the samples.

FROM THE REGIONAL PERSPECTIVE, THE TRANSFER OF ECONOMIC CRIME IS FROM THE SOUTHEAST COAST TO THE CENTRAL AND WESTERN REGIONS

In 2009 the counterfeit money crimes caused widespread concern in the community, and even social rumors appeared high simulation of counterfeit money with the beginning of "HD90". The main trend of counterfeit money crime is from the southeast coast to the central and western regions. The southeast areas belong to developed areas. The central and western areas belong to developing areas. The flow path of counterfeit money crime is from Guangdong province to Anhui province and Henan province. The main cities of counterfeit money crime belong to the provincial capital cities. The main areas belong to the southeast developed areas.

The main trends of counterfeit money crime

The flow path of counterfeit money crime

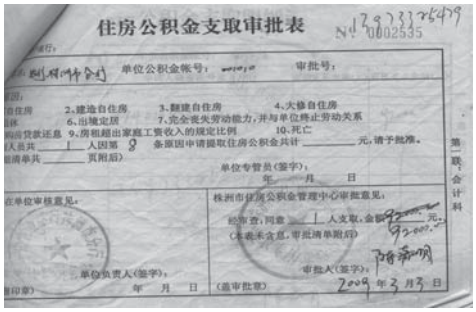
The main city of counterfeit money crime

The main province of counterfeit money crime

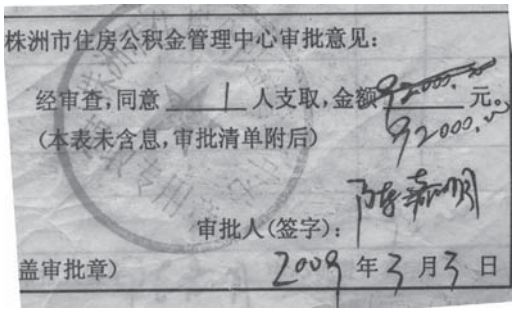
MEANS OF CRIME SHOW A COLLUSION TREND OF INTERNAL AND EXTERNAL PERSONNEL

The cultural degree of suspects who commit economic crime is generally high, many people even have professional knowledge, specialized experience or the advantage of their position in economic, trade, finance, accounting or law, and have long been engaged in economic activities of the relevant fields. They make careful planning and seek illegal economic interests through a legal loophole, so the economic crime in the west is referred to as "white-collar crime". Collective crime phenomenon is highlighted. Some criminal cases are exposed. The members of a leadership team in the county or cities are suspected and finally destroyed by the judicial organ.

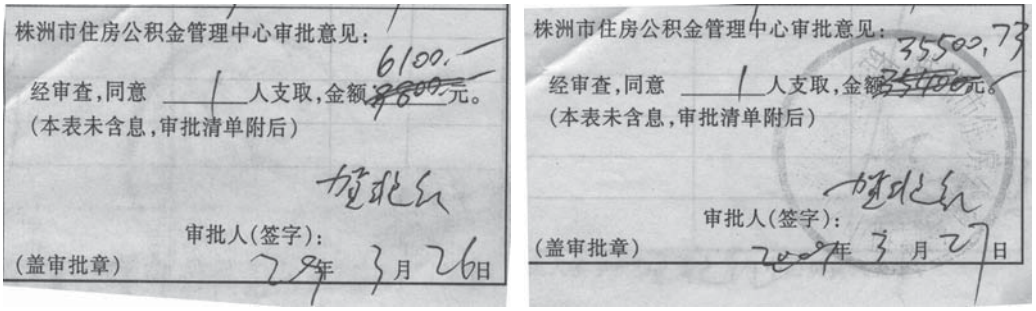
Accumulation fund crime is a usual economic crime. The handwriting of internal personnel has been imitated. The suspect is another colleague of internal personnel of the administration of accumulation fund. The handwriting examination helped the police to see that a layout characteristic and mode of correct mistakes of the questioned document are consistent with that of samples. The handwriting examination helped the police to lock the suspect of accumulation fund crime.


住房公积金支取审批表

Questioned document of fund crime


株洲市住房公积金管理中心审批意见：
经审查，同意 1 人支取，金额 92000. 元。
（本表未含息，审批清单附后）
92000.
审批人（签字）：
盖审批章）
2009 年 3 月 3 日

Part of the questioned document

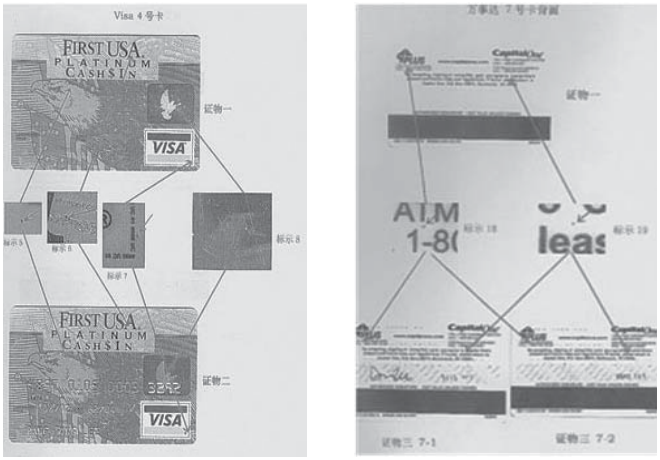


The layout and mode of correct mistakes are consistent with that of questioned document

THE INFLUENCE OF ECONOMIC CRIME SOMETIMES IS INTERNATIONAL

Some economic crimes, such as corruption, bribery, smuggling, money laundering and credit card are involved in international relevant fields. Credit cards are used frequently. A credit card fraud exists all over the world. That is to say the influence of economic crime is international.

The police in the USA arrested two suspects who had fake credit cards. The Chinese police found a factory which made fake credit cards in Guangdong Province. Through information sharing, American police and Chinese police dealt with the case totally. Having examined the printed documents, we found out that the fake credit cards held by two suspects came from the factory in Guangdong Province. The international police cooperation between American and Chinese police helped not only two suspects to be arrested but it also helped the original source of the fake credit cards to be discovered.



Printing characteristics of these cards are the same

THE MAIN METHODS AND TOOLS OF MAJORITY ECONOMIC CRIMES ARE COMPUTER, NET AND EXPRESS

Computer, net and express have the advantage featuring convenience, quickness and concealment. Financial systems professionals use their computer technology in economic crime. Some economic crimes are involved in the firearms, drugs and ivory smuggling by mail. Frequently some people with higher education background go abroad. They traffick firearms part, drugs and ivory by express mail to domestic. Domestic staff sell firearms parts and ivory through the network at high prices to other people. Some of them refine methamphetamine from these drugs.

NECESSARY MEASURES SHOULD BE TAKEN TO COMBAT ECONOMIC CRIME WE SHOULD STRENGTHEN THE EDUCATION OF PEOPLE AND ESTABLISH THE CORRECT VALUES

To prevent economic crime, we must strengthen the education of citizens, which is the most fundamental measure of preventing economic crime. We must strengthen the ideological education of relevant personnel, establish a correct outlook on life and values and improve the ability to resist the temptation of money of the genus. The outlook on life and values have changed toward the abyss. We should take proper means to protect state, the collective and the individual property, protect the legitimate interests of operators, and maintain the normal operation of the market economy order.

THE STRENGTHENING OF THE FINANCIAL BILL MANAGEMENT OF FINANCIAL, TAXATION, BANKING, SECURITIES, TRADE AND OTHER PROFESSIONAL FIELDS

The main fields of economic crime are financial, taxation, banking, securities, trade and other professional fields.These fields accumulate huge amounts of money and run the risk of economic crime. Financial institutions should manage various important blank vouchers strictly, especially customer signature cards. On the other hand,these fields involve the emergence of corruption. Only by doing so can we avoid the huge loss of tax.

THE SECRET CONTROL TO COMMUNICATION, MAIL, TELEGRAPH, TELEPHONE AND NETWORK

Communication, mail, telegraph and network are the main communication way and means. The police should strengthen the effective supervision of communication, mail, telegraph and telephone. Only in this way, can we grasp the information timely, form an integrated force to fight organized crime, improve the fight against organized crime level.

ACTIVE CARRYING OUT OF INTERNATIONAL COOPERATION IN LAW ENFORCEMENT

According to the deepening of China's opening-up policy, foreign cases and fled overseas suspects rising situation, and the public security organs at all levels continue to increase international cooperation in law enforcement efforts, many aspects in the police cooperation, case investigation, the booty arrest, information exchange, business training, and the country (territory) outside the police, law enforcement departments to carry out a very fruitful cooperation. According to statistics, in 2005 the national public security organs arrested 53 suspects of economic crimes on the return flight. The arrest of a large number of fugitives eliminates the hidden danger of economic crime.

TO ESTABLISH WIDE REPORT NETWORK AND STRENGTHEN THE DAILY SUPERVISION, BLOCK THE LOOPHOLES IN THE SYSTEM

Since 2012, "network exposure -- -- check processing" has become a new way of corruption cases in the Commission for Discipline inspection. There are about 179 "office officials" and 5 provincial and ministerial level officials who have been punished for crimes since 2012. Network anti-corruption cannot stop at "sexy photos, expensive matches and large amount of houses".

CONCLUSION

Economic crimes in the field of document examination involve all aspects of social life. Personally, economic crime can make the person suffer losses. From the national level, economic crimes disrupt the order of national economy, even threaten national security. Only when we strengthen all aspects of management, including taxation, banking, securities, trade and other professional fields, and actively carry out international cooperation in law enforcement, strengthen the daily supervision, block the loopholes in the system, can we build a strong socialist democracy country.

REFERENCES

1. Jia Yuwen, Zou Mingli, Complete Works of Chinese Forensic Science ,first ed., Chinese People's Public Security University, BeiJing,2002
2. Ordway Hilton, Scientific Examination of Questioned Documents, Revised ed., CRC Press, 1992
3. Wang Yanji, Wang Shiquan, Course of Forensic Science, first ed., Chinese People's Public Security University,BeiJing,2006

Topic VI

FORENSIC LINGUISTICS

UDC: 811.111'367:811.163.2'367'367

SEMANTIC ANALYSIS OF COLLOCATIONS WITH THE NOUN "EVIDENCE" IN ENGLISH AND THEIR TRANSLATIONAL EQUIVALENTS IN MACEDONIAN

Vesna Trajkovska[1]
University "St. Kliment Ohridski", Bitola, Faculty of Security, Skopje
Radomir Trajkovic[2]

Abstract: In order to achieve higher level of accuracy and precision in the expression of their thoughts, speakers of a particular language should possess great lexical skills, which include the correct use of collocations, i.e. word combinations in the language in question. This aspect also plays a significant role in the process of translating texts from one language into another, when the translators are faced with the task of identifying the semantic distinctiveness of the collocations in the source language and finding their adequate lexical equivalents in the target language, which cannot always be easily accomplished. This is particularly true when the collocations belongs to a specific field for which the lexical corpora of the respective languages do not offer enough lexical solutions for one-to-one correspondence regarding the transfer of their meaning.

The paper deals with the analysis of the semantic content of adjectives and verbs which collocate with the noun "evidence" in English, and their corresponding equivalents in Macedonian. It also includes an overview of prepositions collocating with "evidence", as well as the analysis of longer phrases containing this noun in both languages. The authors trace the etymology and semantically analyze the lexical solutions in English and Macedonian as far as the words collocating with the noun "evidence" are concerned, and provide detailed elaboration on their semantic distinctiveness, in an attempt to find out to what extent the semantic content of the collocations in both languages overlap.

Keywords: evidence, translation, language, meaning, English, Macedonian.

INTRODUCTION

When learning English as a foreign language, students are exposed to simultaneous acquisition of grammatical and lexical knowledge, which intersect between each other and help them in creating grammatically and lexically correct sentences that will enable them to clearly and unambiguously express their thoughts. While grammar knowledge is important for the appropriate structuring of the sentence, the appropriate use of lexical items is essential for accurately expressing one's thoughts through the selection of adequate words which denote the specific semantic features of the concept lexicalized by them.

Accumulation of lexical knowledge is a long process, and, as their proficiency in English grows, learners are expected to demonstrate greater mastery of the appropriate use of words in various contexts. In order to achieve higher level of proficiency, it is necessary for them to master the lexical rules for properly combining words within an expression. In linguistics, these proper word combinations are referred to as *collocations*. The noun *collocation* comes from the Latin word *collocatio*, meaning "arrangement, ordering", and was introduced by J. R. Flirth to denote "characteristic word combinations which have developed an idiomatic semantic relation based on their frequent co-occurrence"(Bussmann, 2006:200). These proper word combinations are of particular importance in the acquisition of English for specific purposes, due to the fact that people specializing in a specific area use the specific vocabulary of that area, and often the meanings of the words in that area do not coincide with their meanings in other domains, or they collocate with different words. This is particularly true for words with several meanings, which are translated differently in other languages. To illustrate this phenomenon, we will take the example with the verb *produce*, a collocate of the noun *evidence* which is the subject of the analysis in this paper. The verb *produce* has several meanings in collocations with nouns belonging to different domains. Thus, when used in industrial context it is used as the synonym for *manufacture*, so in collocations like *produce goods* it is translated into Macedonian as *proizveduva*, and the whole expression is translated as *proizveduva stoka*. In the context of art, on the other hand, it denotes the action of creating work of art, and is usually translated as *sozdava/tvori/kreira*, so the

1 trajkovska_vesna@yahoo.com
2 radomir.trajkovic@gmail.com

collocation *produce a painting*, for instance, would be translated into Macedonian as *sozdava slika*. However, if we use *produce* as a collocate of *evidence*, it denotes the action of showing i.e. exhibiting evidence to the public, so in this context the Macedonian equivalent for *produce* would be *iznesuva*, and the respective English collocation *produce evidence* would be *iznesuva dokazi*.

Taking into account the importance of collocations in specific domains of the use of the language, in the sections that follow we will present an analysis of a selected number of English collocations with *evidence*, as they are used within the domain of forensics, and identify their closest Macedonian equivalents, focusing on specific examples of the translation of collocates with similar semantic contents in both languages. The noun *evidence* is taken with its meaning of "facts, objects, or signs that make you believe that something exists or is true" (Longman, 1995:465), as an uncountable noun. Its English collocations will be contrasted with the collocations of its Macedonian equivalent *dokaz* as a countable noun – a specificity which will determine the use of the appropriate form of its collocates.

ADJECTIVES COLLOCATING WITH THE NOUN EVIDENCE

When analyzing the use of adjectival collocates, we must bear in mind the fact the English noun *evidence* differs from its Macedonian counterpart on the grounds of its countability. The English noun *evidence* is used as an uncountable noun, i.e. a noun denoting something which cannot be counted and is seen as a mass, and has only one (singular) form in terms of the grammatical category number. On the other hand, the Macedonian noun *dokaz* is a countable noun, which consequently means that it can have both singular and plural form – *dokaz* (sing.)/*dokazi* (pl.), on the basis of which the choice and the appropriate form of the adjectives are determined. In order to show the semantic nuances carried out by synonymously used collocations, in this section we will give an overview and semantic analysis of several English adjectives which often are interchangeably used by English speakers that we considered most relevant to the topic being discussed.

English speakers have at their disposal several different adjectives for expressing high level of relevance of *evidence.* One of the most commonly used adjectives for expressing this notion is the adjective *compelling*, meaning "tending to convince or convert by or as if by forcefulness of evidence" (Webster, 1993:463). The notion of the "force" of evidence is derived from its root verb *compel* whose etymology goes back to the Latin verb *compellere* meaning, *inter alia*, "to force or compel" when referring to persons.[3] Within the context of forensics, *compelling evidence* would practically mean evidence that is strong enough to convince a person regarding their relevance. The identical notion is expressed by the adjective *convincing*, rooted in the verb *convince*, within the expression *convincing evidence*. According to etymologists, the root verb convince is derived from the Latin verb "convincere" meaning "to overcome decisively",[4] and since the 16th century has been used with the meaning "to overcome in argument",[5] which is practically the key semantic element which determines its semantic contents within the context of evidence. In this group we will also mention the adjective *persuasive* rooted in the verb *persuade*, in the expression *persuasive evidence*. The verb "persuade" is etymologically related to the Latin verb "persuadere", which means "to bring over by talking".[6] Taking into account the interchangeability in the use of the synonymous verbs *convince* and *persuade*, a logical conclusion can be drawn that both *convincing evidence* and *persuasive evidence* can be used for expressing the same notion. In Macedonian, on the other hand, all these adjectives can be translated with a single equivalent *ubedliv/-a/-o/-i*. Thus, the sentence - *There was compelling/convincing/persuasive evidence that he had murdered his wife* - will be translated as *Imaše ubedlivi dokazi deka si ja ubil soprugata*.

Greater lexical richness of the English language is also reflected in the collocations *conclusive evidence, irrefutable evidence* and *incontrovertible evidence.* According to legal dictionaries, *conclusive evidence* refers to evidence "which cannot be contradicted by any other evidence".[7] It is derived from the Late Latin word *conclusivus*, from *conclus-eas* the past participle stem of *concludere*, and has been used with the meaning "definitive, decisive, convincing" since the 17th century.[8] It is derived from the verb *conclude* etymologically rooted in the Latin verb *concludere*, meaning "to shut up together, to end, close". As far as *irrefutable* is concerned, it also refers to something which one cannot refute, i.e. "prove to be wrong or false; disprove". *Irrefutable* is the opposite of *refutable*, which is derived from *refute*, whose etymology goes back to the Latin verb "refutare" meaning "drive back; rebut, disprove; repress, repel, resist, oppose".[9] *Incontrovertible* is an-

3 http://www.etymonline.com/index.php?allowed_in_frame=0&search=compel&searchmode=none (retrieved on 31.01.2015)
4 http://www.etymonline.com/index.php?allowed_in_frame=0&search=convince&searchmode=none (retrieved on 31.01.2015)
5 Ibid (retrieved on 31.01.2015)
6 http://www.etymonline.com/index.php?allowed_in_frame=0&search=persuade&searchmode=none(retrieved on 31.01.2015)
7 http://legal-dictionary.thefreedictionary.com/conclusive+evidence (retrieved on 31.01.2015)
8 http://www.etymonline.com/index.php?search=Conclusive (retrieved on 31.01.2015)
9 http://www.etymonline.com/index.php?term=refute&allowed_in_frame=0 (retrieved on 31.01.2015)

other adjective that denotes a similar concept. According to dictionaries it refers to something which is "not able to be denied or disputed".[10] It is the opposite of *controvertible*, derived from the verb *controvert*, which is formed by back formation from the noun *controversy*, in Latin "*controversus*" with the meaning "turned against, disputed, questionable" (Klein, 1966:346).

On the grounds of these definitions, we can agree that defined this way there is a great degree of overlapping of the semantic contents which allows for the synonymous use of *conclusive, irrefutable* and *incontrovertible* with the noun *evidence*. Consequently, we can say that, for instance, *There is conclusive/irrefutable/ iincontrovertible evidence that he assassinated the President*, where each of the adjectives used carry a very similar meaning. As for their Macedonian equivalents, these three collocations are usually translated as *nesoborliv(i)/nepobiten(-ni) dokaz(i),* and they can be accepted as the most appropriate translation of the concept in question. Thus, the previous sentence will be translated as *Imaše nesoborrlivi/nepobitni dokazi deka toj izvršil atentat vrz Pretsedatelot.* It is interesting to note that the typical Macedonian equivalents for this concept are formed with the negative prefix ne-, while the examples presented above show that the English speakers can use both non-prefixed and prefixed verbs.

As far as the expression of the notion of great quantity of evidence is concerned, the speakers of English have at their disposal a plethora of synonymous adjectives collocating with the noun *evidence*. Before we present the adjectives in this group, we must bear in mind the fact that evidence is an uncountable noun in English and can be modified with a limited number of adjectives which modify uncountable nouns. The Macedonian equivalent *dokaz*, on the other hand, is a countable noun and can also be modified with adjectives normally used in collocation with countable nouns.

Bearing in mind the uncountable nature of evidence, one of the commonest adjectives used for expressing the notion described above is the adjective *abundant*, which can often be encountered in sentences like *There was abundant evidence at the crime scene*, in order to refer to evidence in large quantities. According to etymologists, the adjective *abundant* entered the English lexical corpus in the 14th century through the Latin word *abundantem* – the present participle of *abundare*, meaning "to overflow",[11] and its today's use is spread in various domains. The same adjective can also be used with a preposition carrying the identical meaning in the reformulated sentence *The crime scene was abundant in evidence*. The noun *evidence* also collocates with the verbal and nominal counterparts of *abundant*. Thus, sentences like *There was an abundance of evidence at the crime scene*, or *The crime scene abounded in evidence* can normally be heard among native English speakers, keeping the same meaning explained above.

The adjective *plentiful* is another synonym with the same semantic contents. It is composed from the root *plenty* and the suffix *–ful*, and it is derived from the Old French word *plentee*, i.e. the Latin word *plenitatem*, meaning "fullness". Combined with the noun *evidence*, the phrase *plentiful evidence* denotes a great amount of evidence, just as the previously elaborated phrase *abundant evidence*. In addition to *abundant* and *plentiful*, we can mention the adjective *extensive* which collocates well with *evidence*, carrying the same semantic contents. It is etymologically rooted in the Latin word *extensivus*, which is derived from *extens-*, which is the past participle stem of *extendere*, meaning "to stretch out, spread".[12] As we can see, it has a very similar etymology with the previously elaborated adjectives *abundant* and *plentiful*, which allows the speakers to use them in their speech interchangeably. Bearing this in mind, we can either say *There was extensive evidence against the perpetrator*, or *There was abundant/plentiful evidence against the perpetrator* and in all three cases our interlocutor will not have any doubts that what we refer to is a great amount of evidence. From a semantic point of view, it is not important whether the evidence is relevant to a specific case or not, what matters here is actually the emphasis on the quantity.

The notion lexicalized by these adjectives can most closely be expressed by the Macedonian adjective *brojni* in the collocation *brojni dokazi*. Apart from this adjectival form, Macedonian speakers can also use a noun form. For this purpose the most adequate solution would be the noun *mnoštvo*, and the collocation would be *mnoštvo dokazi*. On the other hand, it is also possible to use a noun with a preposition. In this case, great amount of evidence can be expressed by the noun *izobilstvo*, so the whole collocation would be either *izobilstvo od dokazi* or *dokazi vo izobilstvo*.

A large amount of evidence can also be expressed by the collocation *ample evidence*. The adjective *ample* originates from the Middle French word *ample*, i.e. from the Latin word *amplus*, meaning "large, spacious" and can be used in numerous contexts modifying nouns belonging to various domains. Although its etymology is very similar to the ones of the previously elaborated examples, according to its contemporary use *ample* is encountered with the meaning "enough or more than enough"[13] mainly with uncountable nouns (ex. *ample evidence, ample space*, *ample time* etc.), but when used with countable nouns it denotes the quality of being large (e.g. *ample chair*, *ample garden,* etc.) This semantic nuance is also evident in the English – Macedonian dictionaries where *ample* is, *inter alia*, translated as "obemen, dovolen" (Мурговски,

10 http://www.oxforddictionaries.com/definition/english/incontrovertible (retrieved on 31.01.2015)
11 http://www.etymonline.com/index.php?term=abundance (retrieved on 31.01.2015)
12 http://www.etymonline.com/index.php?term=extensive (retrieved on 31.01.2015)
13 http://www.oxforddictionaries.com/definition/english/ample (retrieved on 31.01.2015)

2001:40), so logically this translational equivalent is used for the collocation *ample evidence*. As an illustration, the sentence *There was ample evidence about the police officer's involvement in the murder* could be translated as *Imaše dovolno dokazi za vmešanosta na policaesot vo ubistvoto*. We might say that the emphasis here is both on the amount and the sufficiency of the evidence, i.e. its relevance to the respective situation.

As far as the opposite notion is concerned, we can say that the English speakers mainly use the adjectives *insufficient* and *scant* so as to denote the quality of not being sufficient, i.e. "barely sufficient or inadequate".[14] Both adjectives are translated into Macedonian with the single equivalent *nedovolen/-no/-na*, so the sentence *She won't be persecuted due to insufficient/scant evidence* will be translated as *Nema da ja gonat poradi nedovolno (dali e pridavka ili prilog) dokazi.*[15] Here, the insufficiency of evidence is denoted both from the aspect of quantity and quality, relevance or adequacy.

Finally, there are cases when Macedonian speakers borrow adjectives from English in order to describe certain quality of the noun *evidence*. From the aspect of semantics, the borrowed word in Macedonian keeps its original meaning, within the domain in which it was borrowed. In recent years there is a growing tendency for importing Anglicisms into the Macedonian lexical corpus, but we must agree that this practice is not always necessary. We will illustrate our opinion with the adjective *conflicting* in the collocation *conflicting evidence*, which is often translated as *konfliktni dokazi*, particularly in texts translated from English. This collocation refers to evidence which is "incompatible or at variance; contradictory"[16] and for expressing this quality Macedonian speakers can use the adjective *protivrečen* which semantically is the closest equivalent of *conflicting*, so for them *protivrečni dokazi* would be a more appropriate choice. Macedonian speakers can also use the collocation *kontradiktorni dokazi*, with internationalism with a longer history in the Macedonian lexical corpus.

VERBS COLLOCATING WITH THE NOUN EVIDENCE

The noun *evidence* collocates with a great number of verbs, denoting different types of actions. As was the case with adjectives, there are a lot of examples when the English lexical corpus offers several synonyms which are translated with a single Macedonian equivalent. To support this statement, we selected the verbs *collect*, *gather* and *assemble*.. The verb *collect* is derived from the Latin word *collectus*, which is the past participle form of *cogliere*, meaning "gather together",[17] and is usually defined as "bring or gather together". In the context of crime scene investigation, it denotes the action of bringing together evidence from the spot, in order to prepare it for further processing and analysis. It is used in sentences like *The police officers collected the evidence from the crime scene*. In Macedonian, the verb *collect* is typically translated as *sobira* or its modified form *pribira*, so the whole sentence will be translated as *Policajcite gi sobraa/pribraa dokazite od mestoto na nastanot*. However, the verb form is not the only one used in this context. Namely, the derived noun *collection* can often be found as a collocate of *evidence*, in sentences like *The police officers worked on evidence collection*. This can undoubtedly be considered as a proof of the widely accepted use of *collect* and its derivates among English speakers. In this example, collection will be translated with the Macedonian gerund form sobiranje, so the Macedonian version of the sentence would be *Policajcite rabotea na sobiranje na dokazite.*

As far as the verb *gather* is concerned, we may agree that it shares more or less the same semantic contents with *collect*, and can replace it in most cases. According to etymologists, it originates from the Proto-Germanic word *gadurojan* which means "bring together, unite".[18] Although it has developed new meanings throughout history, when used as a transitive verb it usually means "bring together and take in from scattered places or sources".[19] As we can see from the definition, *gather* has the specific semantic feature of bringing together scattered places, while *collect* may have a more general definition of bringing things together. However, this distinctiveness is more evident in their use in other contexts while in the context of crime scene investigation it is blurred, bearing in mind the fact that evidence is normally scattered at the crime scene, so both its collection and gathering necessarily involve the act of taking it from the whole area and putting it together. This means that the previous sentence can be reformulated as *The police officers gathered the evidence from the crime scene*, without any changes in the meaning, and have the same translation into Macedonian due to the fact that both *collect* and *gather* are translated as *sobira/pribira*.

14 http://www.oxforddictionaries.com/definition/english/scant (retrieved on 31.01.2015)
15 The collocation *insufficient/scant evidence* can also be translated with an extended phrase including a gerund form of the verb *nema*. Thus, another possible translation of the sentence would be *Nema da ja gonat poradi nemanje dovolno dokazi.* This type of expression is typical of journalist style. Namely, the journalists choose to use a more dramatic expression which would emphasize the negative point, i.e. the "NOT having something", so instead of using an adjective with a negative prefix, they insert a negative verb before the adjective in its positive form.
16 http://www.oxforddictionaries.com/definition/english/conflicting (retrieved on 31.01.2015)
17 http://www.etymonline.com/index.php?term=collect (retrieved on 31.01.2015)
18 http://www.etymonline.com/index.php?term=gather (retrieved on 31.01.2015)
19 http://www.oxforddictionaries.com/definition/english/gather (retrieved on 31.01.2015)

For denoting the same concept, the English speakers may also use the verb *assemble*. It is derived from the old French verb *assembler*, meaning "to gather, assemble" (Klein, 1966:115) which can be used in various contexts. Thus, it is generally used to refer to gathering of people, objects, pieces of things in one place, and this semantic feature of bringing together is also included in the context of assembling evidence. Defined this way, it can freely replace both *collect* and *gather* in collocation with *evidence*, with the same translational equivalent in Macedonian – *sobira/pribira dokazi*.

Apart from cases of asymmetrical synonymy similar to the ones presented above, there are numerous situations when Macedonian synonymous verbs can express, to a high degree, the semantic nuances expressed by their corresponding English synonyms. For the purpose of our paper, we will single out the English verbs *inspect* and *examine*, which are often used interchangeably despite their slight semantic differences. Namely, both verbs are used within the wider concept of analyzing evidence, but a more detailed semantic analysis shows certain specificities of both verbs which make them near, not absolute synonyms. The specificity of *inspect* is reflected in its etymological root, i.e. the Latin word *inspectus*, which is the past participle form of *inspicere*, meaning "to look into".[20] As its etymology suggests, the essence of this concept revolves around the act of looking, an act performed by one's eyes,[21] which practically implies the existence of a physical object that can be looked into, or a situation that can be "eye witnessed". Consequently, when a person inspects evidence he/she performs an act of physically and visually checking tangible evidence. This notion is replicated in the corresponding Macedonian verb *pregleda*, which is rooted in the verb *gleda*, the equivalent of the English verbs *see/look/watch*. As a result of this specific semantic feature, the English sentence *The crime-technicians are inspecting the evidence* should be translated as *Krim-tehničarite gi pregleduvaat dokazite*, as its closest semantic equivalent.

On the other hand, the notion of examining refers to a slightly different concept. Namely, the verb *examine* is originally derived from the Latin verb *examinare*, meaning "to test or try; consider; ponder".[22] Based on this definition, we can conclude that *examine* is a wider concept which includes more detailed analysis, checks and testing and which can be applied both to tangible and intangible objects, ideas, statements, arguments, etc. In Macedonian, this notion is most closely lexicalized by the verb *ispita*, so a sentence like *All evidence must be examined carefully* will be translated as *Site dokazi mora vnimatelno da se ispitaat*, without deviations of the semantic content of this concept.

However, it is interesting to note that there are cases of verbal English collocations with *evidence* which do not have their corresponding counterparts in Macedonian. To illustrate this specificity, this time we will use a collocation with *evidence*, where *evidence* is used not with the meaning of "facts, objects, or signs that make you believe that something exists or is true" (Longman, 1995:465), but with its meaning of "information given in a court of law in order to prove that someone is guilty" (ibid:466). In this category we will single out the verb *give*, which is used in the collocation *give evidence* with the meaning "give information and answer question formally and in person in a law court or at an inquiry".[23] In Macedonian the whole phrase is translated with the verb *svedoči*, whose English equivalent in the form of a verb is *to testify*. In spite of the existing gap in the Macedonian lexical system, we can agree that, given this definition, *svedoči* (*testify*) can be accepted as the closest semantic equivalent which reflects to a great extent the semantic content of the collocation *give evidence*. Thus, the sentence *She refused to give evidence in court* would be translated as *Taa odbi da svedoči na sud*.

PREPOSITIONS COLLOCATING WITH THE NOUN EVIDENCE

As far as prepositions collocating with *evidence* are concerned, there are situations when the English preposition is replaced by its literal Macedonian equivalent, but there are also cases of non-literal translation. In this section we will mention the collocation *as evidence*, which is literally translated as *kako dokaz*, in sentences like *His cell phone was used as evidence in court* and its Macedonian counterpart *Negoviot mobilen telefon bese upotreben kako dokaz na sud*. Literal translation is also typical of the collocation *evidence against*, where the preposition *against* is translated as *protiv*, which is its commonest equivalent in the Macedonian lexical corpus. Thus, the sentence *They had enough evidence against the perpetrator* would normally be translated as *Imaa dovolno dokazi protiv storitelot*. Similarly, the preposition *for* is typically translated as *za*, within the collocation *evidence for*, in phrases like *evidence for terrorism*, which is translated as *dokazi za terorizam*.

On the other hand, in some situations it is not possible to provide one-to-one correspondence as far as the choice of the Macedonian equivalent is concerned, when the literal translation of the original English

20 http://www.etymonline.com/index.php?term=inspect (retrieved on 31.01.2015)
21 For more information on this concept, go on: http://www.vocabulary.com/dictionary/inspect (retrieved on 31.01.2015)
22 http://www.etymonline.com/index.php?term=examine (retrieved on 31.01.2015)
23 http://www.oxforddictionaries.com/definition/english/evidence (retrieved on 31.01.2015)

preposition does not convey the notion expressed by it in the English collocation. As an illustration we will take the example with the preposition *in*, which is usually translated as *vo*, but within the collocation *in evidence* it is translated as *kako*. Therefore, the sentence *The weapon was produced in evidence*, will be translated as *Oružjeto bese izneseno kako dokaz*.

CONCLUSION

From the overview and the semantic analysis of the collocations presented in the paper, we can draw a conclusion that the English noun *evidence* can be used with various adjectival, verbal and prepositional collocates. This wide spectrum of collocations is a proof of the richness of the English lexical corpus, which abounds in synonyms expressing identical or similar concepts, used as collocates of *evidence*. Although in many cases the English collocations semantically coincide with their Macedonian equivalents, in some examples the Macedonian language shows fewer options for denoting the original English concept. In those situations, a detailed semantic analysis is necessary for transferring the meaning of the original word as closely as possible, so as to avoid possible misunderstandings.

REFERENCES

1. Bussmann, Hadumon. 2006. Routledge Dictionary of Language and Linguistics. London/New York: Routledge
2. Klein, Ernest. 1966. *A Comprehensive Etymological Dictionary of the English Language*. Amsterdam/London/New York: Elseviere Publishing Company
3. Longman Dictionary of Contemporary English.1995. Longman Group Ltd
4. Webster's Third New International Dictionary (unabridged). 1993. (Philip Babcock Gove *ed.)*.Cologne:K nemann Werlagsgesellschaft Mbh
5. Мургоски, Зозе. 2001. *Голем англиско македонски речник*. Скопје: Автор
6. http://legal-dictionary.thefreedictionary.com/conclusive+evidence (retrieved on 31.01.2015)
7. http://www.etymonline.com/index.php?allowed_in_frame=0&search=compel&searchmode=none (retrieved on 31.01.2015)
8. http://www.etymonline.com/index.php?allowed_in_frame=0&search=convince&searchmode=none (retrieved on 31.01.2015)
9. http://www.etymonline.com/index.php?allowed_in_frame=0&search=persuade&searchmode=none (retrieved on 31.01.2015)
10. http://www.etymonline.com/index.php?search=Conclusive (retrieved on 31.01.2015)
11. http://www.etymonline.com/index.php?term=abundance (retrieved on 31.01.2015)
12. http://www.etymonline.com/index.php?term=collect (retrieved on 31.01.2015)
13. http://www.etymonline.com/index.php?term=examine (retrieved on 31.01.2015)
14. http://www.etymonline.com/index.php?term=extensive (retrieved on 31.01.2015)
15. http://www.etymonline.com/index.php?term=gather (retrieved on 31.01.2015)
16. http://www.etymonline.com/index.php?term=inspect (retrieved on 31.01.2015)
17. http://www.etymonline.com/index.php?term=refute&allowed_in_frame=0 (retrieved on 31.01.2015)
18. http://www.oxforddictionaries.com/definition/english/ample (retrieved on 31.01.2015)
19. http://www.oxforddictionaries.com/definition/english/conflicting (retrieved on 31.01.2015)
20. http://www.oxforddictionaries.com/definition/english/evidence (retrieved on 31.01.2015)
21. http://www.oxforddictionaries.com/definition/english/gather (retrieved on 31.01.2015)
22. http://www.oxforddictionaries.com/definition/english/incontrovertible (retrieved on 31.01.2015)
23. http://www.oxforddictionaries.com/definition/english/scant (retrieved on 31.01.2015)
24. http://www.vocabulary.com/dictionary/inspect (retrieved on 31.01.2015)

Topic VII

CYBERCRIME

UDC: 343.351:336.745
343.85:[004:007
005.922:004
343.533::004

APPLICATION OF ALFRESCO SYSTEM IN PREVENTION OF MONEY LAUNDERING

Marija Miladinovic Sevic[1]

Abstract: Persons and organizations which are involved in the fight against money laundering and crime and terrorist financing, in accordance with the law and other regulations, are also required to collect, update and store information of different characteristics from other, different sources in accordance with the same laws and regulations. These information and data include information about clients and customers, processed or original, often containing the results of their analysis and reports with respect to knowledge about and monitoring of clients and account holders and their activities and operations. All of these subjects are required to keep and maintain records, submit information, data, documentation and analysis to competent authorities and inform about suspicious activities and transactions.

There are computer programs that have much helped in the collection, analysis, presentation of and sharing the information that are relevant to all entities involved in the fight against this and other forms of crime. Software systems have become necessary, especially those that allow for quick and easy storage, sharing, analysis, search, and use of data and documents of importance. With the development of information technology, these systems have become more accessible and affordable than what is believed. Alfresco document management system is a system of open source, free of charge, which allows not only content managing, but also collaboration, data warehousing, advanced search services interoperability of content and record managing. Alfresco provides an opportunity for modularity and adjustment to requirements of user and is functional in all operating systems. Alfresco can be extremely useful in the strategic fight to prevent money laundering and terrorist financing and is not limited only to those forms of crime.

Keywords: prevention of money laundering, financing of crime and terrorism, Alfresco systems, document management.

INTRODUCTION

New challenges in securing and preserving both national and international security are the result of economical, social and political instability of the modern world. Trends in international trade, capital flows, capital, and movement of people in the 21st century are devoid of many of the previous limitations and get new manifestations. But, new opportunities are also generating new risks. Leading challenges in the 21st century are: the threat of international organized crime, drug trafficking, human trafficking, production and trade of weapons of mass destruction, etc. The base of each of these challenges is a challenge itself: laundering money obtained through illegal actions, its placement into the legal money flow and the concealment of the true identity of the owner.

"White collar crime" is a term that is in its broadest sense a part of computer and financial crimes. It is the type of crime that does not involve violence, and for the same reason, it is often not interesting and intriguing enough to be considered as a serious threat. This type of crime is particularly socially dangerous because the non-disclosure and impunity of perpetrators offend the morals of society.

The subjects participating in the fight against money laundering and terrorist financing are required to collect, update, and store information about their customers, to analyse and process such information, to perform activities and measures and monitor their parties, their activities and operations. They must assess risks, analyse and manage the risks of money laundering, keep and maintain records and provide information, data, documents to the competent authorities, as well as inform them on suspicious transactions.

The importance of information technology in these processes is indisputable. Software systems that contribute to easier collecting, updating, searching and processing data and information, have become indispensable. Some systems have been prescribed as required by financial institutions and considered as minimum standards for management information systems in financial institutions. Quality and useful tools need not be expensive and inaccessible. Informatisation of the subjects, companies, public administration bodies, institutions and the like can contribute to a faster and more efficient work together with the free purchase and minimum implementation costs.

1 plavimish@gmail.com

Upon completion of this research a number of possible uses of this tool will be considered for the fight against money laundering and terrorist financing, together with the possibility of implementing this tool in the system of institutions involved in fight against money laundering and terrorist financing, starting from the Administration for Prevention of Money Laundering, together with authority competent for supervision and subjects to which the data is forwarded, which trigger the initiative to start the proceedings.

ALFRESCO PLATFORM

Alfresco is a content management system built by a team of experienced experts in the industry, which originates from the following companies: Documentum, Vignette and Interwoven. Alfresco is an integrated solution for document management, Web content management, collaboration, data warehousing, content interoperability services (CMIS) and records management. It is a complex service with many settings for different loads and use[2]. Alfresco is used for collecting, exchanging and archiving documents that users can easily browse through. The basis of the document management is a web feature that can be used from any browser and operating system, and is suitable for a variety of actions that are specifically for document management.

Main functions of the Alfreco platform are:

- Content and documents creating
- Import of the documents either directly, either by scanning the paper documents
- Content Categorization
- Verzioning
- Locking/unlocking the documents
- Erased documents management
- Advanced search of the documents by content or attributes.
- Integrated workflow, complex workflow support, dashboard task management
- Compliance - Secure Document Lifecycle Management
- Tracking documents and insight into the current status of processing
- Team collaboration by using e-mails, forums, discussions
- Transformation engine, transformation services – from MS Office to ODF/PDF, PowerPoint to Flash
- Organize users through user groups and roles
- Records of user actions
- Security and user management with users, groups and roles
- Document Level Security
- Reliable documents exchange
- Documents confidentiality
- Access rights control
- The procedure for making regular backups[3]

Alfresco offers document management using familiar interfaces to get rapid user adoption built on a repository that offers transparent, out-of-sight services for full ECM: Virtual File System - Replace shared drives and offers the same interface, Email-like rules - Configure plug-in rules to automate manual processing and offers out-of-sight compliance Google-like search - Search directly from the browser, Yahoo-like browsing - Automatic meta-data extraction and categorization, SmartSpaces - Best practice collaboration spaces and Transparent lifecycle support[4].

Library services: check-In/Out - minor and major version control, Auditing - who created, who updated, when created, when updated, Document cross linking - across multiple spaces. It supports Microsoft Office Share point protocol, and document management with Microsoft Office tools.

The advanced component for web content management is useful for management and creation of the intranet and internet web portals. The basic advantage is the integration of the module for documents management, which means that users can operate with all necessary resources (text, graphic design, multimedia content) as with separate documents available through the Alfresco repository. Authors can use standard tools for web design using technology of shared discs or WebDAV protocol. Editors can easily control mul-

2 http://www.alfresco.com/resources/documentation
3 http://wiki.alfresco.com/wiki/Product_Overview
4 http://wiki.alfresco.com/wiki/Product_Overview

tiple versions of web pages and manage the lifecycle of the content. Thanks to Alfresco's orientation to the open source and Java technologies, web sites can easily be extended to the interactive possibilities based on the Alfresco repository, web scripts or REST composition.

Content management is a function that enables users to collect, classify, control and destroy various official documents. Alfresco is certified for DoD 5015.02[5] standard, and is developed to support other standards too. Document creating and review does not require any additional tool installation. In doing so, all the settings related to security and business rules and processes are retained.

Alfresco architecture - Alfresco includes most modern and elegant open source components and frameworks. Reusing of these components is what has enabled Alfresco to develop their product very quickly and stay abreast of the latest technology and standards.

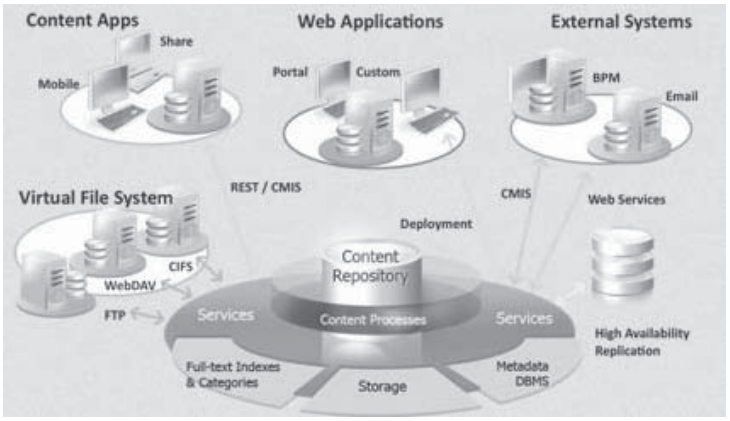


Figure 1 *Alfresco System*[6]

Figuure 1 displays Alfresco system. Alfresco has a very open, service-based architecture that supports a number of standards[7]. At the core of the Alfresco system is a repository supported by a server that persists content, metadata, associations, and full text indexes. Repository is available through Web DAV, CIFS-a (Common Internet File System) i FTP.[8]

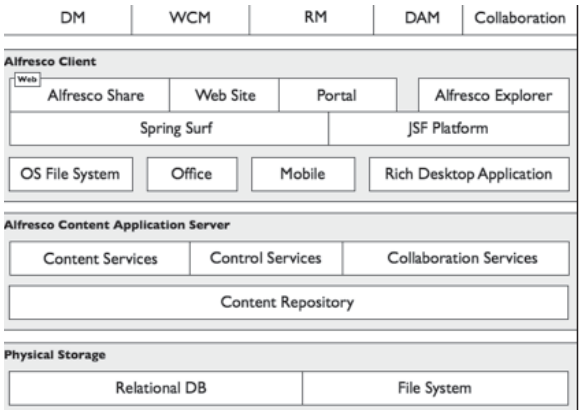


Figure 2 *Alfresco Architecture*[9]

The out-of-the-box applications (running immediately after installation, without configuration, adjustments and changes) offer standard solutions, such as document management, content management and web content management. This is based on Spring platform, which provides the ability to modularize functionality, such as versioning, security and rules. Alfresco uses scripting to simplify adding new functionality and develop new programming interfaces.[10]

5 http://www.js.pentagon.mil/whs/directives/corres/pdf/501502std.pdf
6 http://docs.alfresco.com/4.1/concepts/system-about.html
7 http://docs.alfresco.com/community/index.jsp
8 http://wiki.alfresco.com/wiki/Product_Overview
9 http://docs.alfresco.com/4.2/concepts/alfresco-arch-about.html
10 http://www.alfresco.com/community

According to Alfresco official documentation, there are many ways to slice and deploy the system. This is the first level in the Alfresco structure, figure 2. For each of them or all together, there are options for collaboration and advanced search.

The solutions are typically split between clients and server, where clients offer users a user interface to the solution and the server provides content management services and storage. Solutions commonly offer multiple clients against a shared server, where each client is tailored to the environment in which it is used.

Alfresco has two web clients (Clients application): Alfresco Share and Alfresco Explorer

Alfresco Share – deployed to its own tier. Separate from Alfresco content application server. It is focused to the collaborative aspects of content management and streamlining the user experience. It is implemented using Spring Suft and its advantage is that it can be customized without Java Server Faces knowledge.

Alfresco Explorer – deployed as part of Alfresco content application server. The Explorer is very customizable and exposes all features of Alfresco content application server. It is implemented using Java Server Faces.[11]

The clients exist for portals, MS Office, mobile platforms and desktop as well. Using JLAN technology, Alfresco looks and acts like a folder drive. JLAN is Java server-side implementation of the CIFS protocol, which lets the user interact with Alfresco as any other file of drive, with the difference that the content is stored and managed by Alfresco content application server.

Content application server – includes content repository and services for building ECM solution. Standards that define the content repository are: CMIS (Content Management Interoperability Services) and JCR (Java Content Repository – JSR 170-286)[12]. These standards provide the specification for content definition and storage, content retrieval, versioning and permissions. They provide a reliable, scalable and efficient implementation.

Content application server provides categories of services built upon the content repository:

- Content services – transformation, tagging, metadata extraction. Includes logical content organization, folder management, version and security control. It supports content control through workflow, as well as social and collaborative applications. On different tile levels, these services include: Java, Scripting, REST, Web services, client interfaces such as Alfresco Explorer and Alfresco Share.
- Control services - workflow, records managements
- Collaboration services – wiki, activities, social graph[13]

Clients communicate with Alfresco content application server and its services through numerous supported protocols. HTTP and SOAP offer programmatic access while CIFS, FTP, WebDAV, IMAP, and Microsoft SharePoint protocols offer application access. The Alfresco installer provides an out-of-the-box prepackaged deployment where as Alfresco content application server (with embedded Alfresco Explorer) and Alfresco Share are deployed as distinct web applications inside Apache Tomcat (open source web server, developed by Apache Software Foundation.[14])

Alfresco content application server is the core of the Alfresco. Its main function is to obtain functioning of the ECM services. Public and remote interfaces are the only part of the server which is visible to a client. There are two types:

1) Remote API – for server service interaction.

2) Protocol bindings – for mapping services for use by a protocol compliant client.[15]

As it is displayed in the picture 3, server is comprised of several layers. It includes configuration, authentication, permissions, and transactions that cut across all capabilities. Infrastructure shields server from being tied to transaction managers or caching mechanisms.

11 http://docs.alfresco.com/community/index.jsp
12 http://docs.alfresco.com/community/index.jsp
13 http://docs.alfresco.com/community/index.jsp
14 http://en.wikipedia.org/wiki/Apache_tomcat
15 http://docs.alfresco.com/community/index.jsp

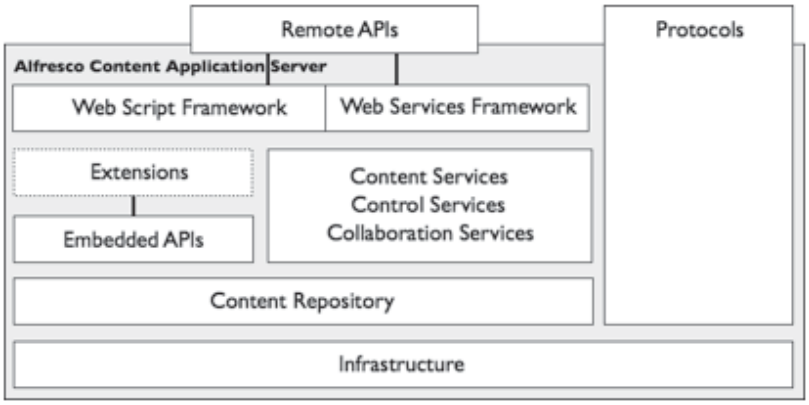


Figure 3 *Alfresco Content Application Server*[16]

Storage device also has search ability, thanks to adjusted request system on Apache Lucene. It supports the following options:

- Metadata filtering
- Matching paths
- Searching the full text
- Combinations of the above[17]

Set of protocols for client – server communication is shown on the figure 4.

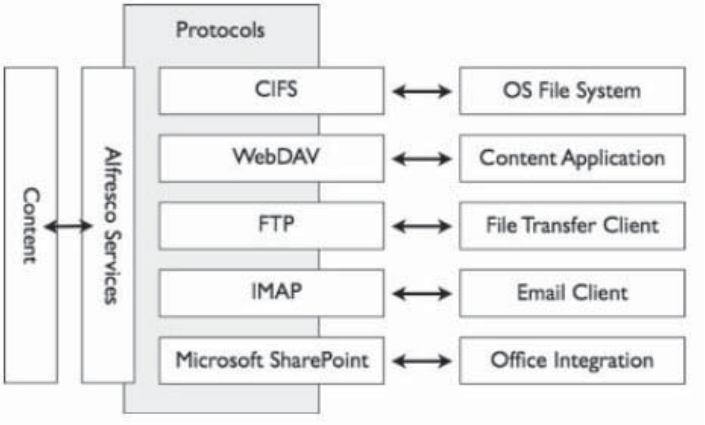


Figure 4 *Application server protocols*[18]

- CIFS – Common Internet File System – is the standard way in which computer users share files across corporate intranets and the Internet. In the case of Alfresco, it makes Alfresco act as a file share drive. Each client who knows how to read and write from file drive will be able to do that in Alfresco.
- WebDAV - Web-based Distributed Authoring and Versioning – extensions for HTTP that allows collaboration and document management on the web servers.[19]
- FTP – File Transfer Protocol – standard network protocol used to transfer computer files from one host to another host over a TCP -based network.
- IMAP – Internet Message Access Protocol – standard protocol for accessing email from your local server. Alfresco behaves as mail server, and allows to the clients such as MS Outlook, Apple Mail and Thunderbird to connect and use folders and documents in the repository[20].
- Microsoft SharePoint Protocol – Enables Alfresco to behave as SharePoint server.

16 http://docs.alfresco.com/4.2/concepts/content-server-about.html
17 http://docs.alfresco.com/community/index.jsp
18 http://docs.alfresco.com/4.2/concepts/content-server-about.html
19 http://docs.alfresco.com/community/index.jsp
20 http://docs.alfresco.com/community/index.jsp

DIGITAL SIGNATURES IN THE ALFRESCO SYSTEM

The implementation of digital signature module for documents in Alfresco, enables end-users to digitally sign a document very easily, directly from the Alfresco, using smart cards or keystore files. Generated signatures are stored as XML files in the Alfresco repository, according to XML Signature specification.

According to XML Signature syntax[21] it is possible to create XML document which contains all necessary information about digital signature of any electronic resource. Together with syntax, XML Signature specification defines rules for generating XML document that represents digital signature, as well as rules for signature verification of such a document.[22].

Architecture of digital signing module – Digital signing module in the Alfresco is realized as a client-server application. Server-side is actually Alfresco plug-in that supports digital signing, and client-side enables user to create digital signature for any document and pass it back to Alfresco server. Client's application is introduced to enable usage of smart card keys or keystore files which are physically stored at the users, not on the Alfresco server.

User starts digital signing by selecting actions for digital signing of relevant documents. As a result of this action is opened page for digital signing of the desired document. Selecting the appropriate option on this page creates JNLP (Java Network Launch Protocol) file which is sent to the user. This JNLP file describes the application of digital signing, including the parameters of the application. Launching JNLP file via Java Web Start technology on the user's computer, downloads application for digital signing. Then, the user enters the required authentication data. Upon the execution of this activity, the application will digitally sign the document, and then forward the signed certificate to Alfresco server, to enable further verification of the signature. Alfresco server, ie. his module for digital signing, formates XML document of the submitted parameters in accordance with XML Signature specification and notifies the client whether a method is successfully implemented.

JNLP file generating - The process of generating JNLP file for the application of digital signing is initiated by clicking on the appropriate link on the page for digital signing of the document. By this click JNLPGeneratorServlet will be executed and an JNLP file will be generated. This JNLP file will be send back to the client. For JNLP file generating JNLPGeneratorServlet relies on JNLPGenerator class. This class generates JNLP file based on the appropriate template.

The example of the template for generating JNLP file, i.e. the values which will be replaced by the JNLP Generator must be specified within ${} declaration. In this example, JNLP template parameters are:

- host: the name of the comptuter where Alfresco server is located
- locale: locale of the application for digital signing
- hashcode: heš kod which is digitally signed
- cookie: cookie of the current user's session

JNLP Generator-servlet uses ExtendedXMLSignature class for the purpose of generating the hash code. This class represents an upgrade of the XML Signature class from Apache XML Security project.[23] ExtendedXMLSignature class enables creating of the XML document according to XML Signature specification, where the generating document process is divided into two steps. The first phase, which occurs during the JNLP file generation, is creating of the <ds:SignedInfo> element, i.e. generating its hash code. This hash code client signs the document through the digital signing application[24].

For the purposes of generating <ds: SignedInfo> element, it is necessary to calculate the hash code of the document is digitally signed [25]. AlfrescoCurrentSpaceResolver class enables ExtendedXMLSignature to reach an appropriate document that should be signed in the Alfresco system. Reaching the document ExtendedXMLSignature calculates hash code based on document content.

The second phase occurs during the generation of the document with digital signature. It is a setting of the digital signature and certificate for signature verification into XML file which represents digital signature.

21 Dournaee, B., XML Security, McGraw-Hill,2002,ISBN 0-07-222808-3
22 XML Signature Specification, http://www.w3.org/Signature/
23 Apache XML Security, http://santuario.apache.org
24 XML Signature Specification, http://www.w3.org/Signature/
25 XML Signature Specification, http://www.w3.org/Signature/

APPLICATION FOR DIGITAL SIGNATURE

Application for digital signature is modelled as in the class diagram in the figure 5. Signature class is basic class of the application. This class uses appropriate specialization of the SignaturePanel class, depending on the manner in which it is signed.

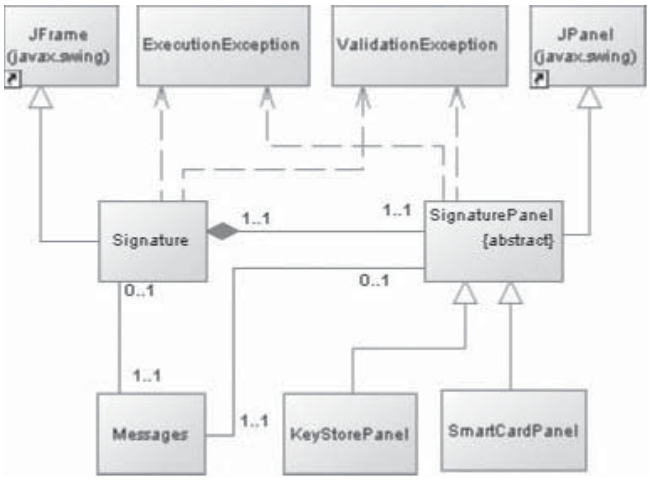


Figure 5 *Application classes*[26]

In case that the signing is done by using smart cards, SmartCardPanel class is used, while in the case of using keystore file the KeyStorePanel class is used. Implementation of SmartCardPanel requires the appropriate authentication data specific to a particular type of storage keys. Also, through this implementation process was implemented digital signature that basically can vary depending on the storage media keys that are used (smart card or keystore file). Errors that can occur during the execution of certain operations, are modeled by ExecutionException and ValidationException classes. Errors can occur during the validation of entered data. Message class lets user load labels and application messages for defined lokal.sdfa.

Generating of a document with a digital signature and verification of digital signature – Address to which is forwarded a digital signature and a certificate of the user, is specified as a parameter to the application. This address is in the fact the address of the SignatureServlet. This servlet relies on SignatureDocumentCreator class and creates a new XML document in Alfresco system that includes a digital signature of the document. Signature Document Creator creates this document by using Extended XML Signature class, i.e. the second phase of the process: generating the XML document with digital signature, setting out the signature and the certificate that performs validation of the signature.

Thanks to VerifySignatureEvaluator class, action for starting digital signature verification occurs only for documents which represent a digital signature of any other document.

Verification of a digital signature under the Alfresco is implemented by SignatureVerificationBean class. This class performs verification through XML Signature class. For access to a document whose signature is verified, XML Signature uses AlfrescoCurrentSpaceResolver class.

Digital signature is created by XML Signature specification and it can be verified not only in Alfresco system, but also, outside of it.

ALFRESCO APPLICATION SYSTEM IN PREVENTION OF MONEY LAUNDERING AND FUNDING OF TERRORISM

Offense of money laundering is a specific criminal activity, because it is a consequence of the previously committed crime, but also a starting point for future criminal activity. Assets obtained by criminal activity is invested by organized criminal groups to legitimate business. That is the way of legalizing the money obtained in a illegal manner. Precisely because the primary purpose of money laundering is the concealment of the performance of other serious criminal offences, the offence of money laundering has a much broader negative impact on a whole society.

26 Goran Sladić, Branko Milosavljević, Stevan Gostojić, „DIGITALNO potpisivanje dokumenata u Alfresco sistemu", http://www.e-drustvo.org/proceedings/yuinfo2009/html/pdf/158.pdf

International initiatives and national legislation established the basic framework of prevention of money laundering and combating the funding of terrorism.

In the republic of Serbia, Serbian Criminal Code and the Law on Prevention of money laundering and combating the funding of terrorism are the basis of the strategy of countering money laundering.

The term „money laundering" occurs in the United States during the Prohibition (prohibition of selling alcoholic beverages), in the thirties of the previous century, when criminals earned money from the illegal production and smuggling of alcoholic beverages portrayed as earnings that were achieved in the chain of laundry washing machines and cars. For these phenomena began to use the term "money laundering", from where Criminological Sciences takes the term. In the classic sense, money laundering is a series of actions designed to cover the tracks of criminal proceeds. Stated another way, it is "the process by which one conceals the existence, illegal source, or illegal application of income, and then disguises that income to make it appear legitimate." (President's Commission on Organized Crime, The Cash Connection, at 7 (Oct. 1984).).[27]

Money laundering is an extraordinary threat to the integration of financial institutions. It is disadvantageous to all parties that operate legally. Launderers generally do not seek to achieve the highest rate of profit on laundered money. Money can travel from countries with good economic policies under which they might generate more profit, in the country with a worse policy and lower returns of investment funds. So, because of money laundering it can happen to funds to be invested less rational, and that can greatly disrupt existing economic trends.

Organized criminal groups can perform money laundering in a following ways:

- participation in the privatization of social capital,
- establishing the companies whose core business is foreign trade and foreign exchange operations.
- participation in tenders for projects funded from public expenditure (such as public works and generally large investments in infrastructure)
- Public procurements[28].

In accordance with current law, the crime of money laundering includes:

1) conversion or transfer of property acquired through the commission of a criminal offence;

2) concealment or misrepresentation of the true nature, source, location, movement, disposition, ownership of or rights with respect to the property acquired through the commission of a criminal offence;

3) acquisition, possession, or use of property acquired through the commission of a criminal offence;.[29]

For the purposes of this law, terrorism financing means the providing or collecting of funds or property, or an attempt to do so, with the intention of using them, or in the knowledge that they may be used, in full or in part:

1) in order to carry out a terrorist act;

2) by terrorists;

3) by terrorist organizations. [30]

The financing of terrorism means inciting and aiding and abetting in the provision or collection of property, regardless of whether a terrorist act was committed or whether property was used for the commission of a terrorist act[31].

Actions and measures for the prevention and detection of money laundering and terrorism financing shall be taken before, during the course of, and following the execution of a transaction or establishment of a business relationship.[32]

These actions and measures include the following:

- Knowing the customer and monitoring of their business transactions ('customer due diligence');
- Sending information, data, and documentation to the APML;

27 https://www.ncjrs.gov/App/publications/Abstract.aspx?id=166517
28 http://www.bezbednost.org/upload/document/cv_uprava_pranje_novca.pdf
29 Law on the prevention of money laundering and the financing of terrorism, , Official Gazette of the Republic of Serbia, no. 20/2009, 72/2009 i 91/2010
30 Law on the prevention of money laundering and the financing of terrorism, , Official Gazette of the Republic of Serbia, no. 20/2009, 72/2009 i 91/2010
31 Law on the prevention of money laundering and the financing of terrorism, , Official Gazette of the Republic of Serbia, no. 20/2009, 72/2009 i 91/2010
32 Law on the prevention of money laundering and the financing of terrorism, , Official Gazette of the Republic of Serbia, no. 20/2009, 72/2009 i 91/2010

- Designating persons responsible to apply the obligations laid down in this Law (hereinafter referred to as: a compliance officer) and their deputies, as well as providing conditions for their work;
- Regular professional education, training and improvement of employees;
- Providing for a regular internal control of the implementation of the obligations laid down in this Law;
- Developing the list of indicators for the identification of persons and transactions with respect to which there are reasons for suspicion of money laundering or terrorism financing;
- Record keeping, protection and keeping of data from such records;
- implementation of the measures laid down in this Law in obligor branches and majority-owned subsidiaries located in foreign countries;
- implementing other actions and measures based on this Law. [33]

ICT STRAGEGY OF ADMINISTRATION FOR THE PREVENTION OF MONEY LAUNDERING

Republic of Serbia has adopt the law and EU directives, as well as international standards in the field of money laundering developed by FATF[34]. There are 40 recommendations and 9 special recommendations which are set as main standards in the field of combating money laundering, terrorist financing and other related threats to the integrity of the international financial systems. In accordance with all those regulations, National strategy against money laundering and terrorism financing is adopted and published in the "Official Gazette of the Republic of Serbia" no. 89, October the 1st 2008.

Recommendations for the operative level[35] require that the IT system in the Administration for the Prevention of Money Laundering should be further developed. It require development of such a IT system that would facilitate the implementation of the objectives of the strategy, which include the reduction of crime in relation to money laundering and terrorist financing, the implementation of international standards whose implementation allows membership or favorable status of international organizations, development of a system of cooperation and responsibility of all participants in the fight against money laundering and terrorist financing, improving cooperation between the public and private sector in the fight against money laundering and terrorist financing, ensuring transparency of the financial system.

As in neighboring countries, as well as in Serbia, it si neccessary to establish and appropriate business process using technology. Technology will be used to enable and support the detection of suspicious transactions organized crime activities and to provide proactive and timely exchange with reporting entities and authorities.

Strategy of information and communication technologies should be implemented to support business goals and objectives of financial intelligence system. It is necessary to implement the electronic reporting system that will enable the efficient and timely exchange of information between reporting entities and authorities.

The strategy discusses the technology in three main parts:

1) Business applications - specific to the role of the Government in the fight against money laundering

2) Office automation (word processing and other forms of automation)

3) Infrastructure (hardware and software network support)

Table 1 *High level IT requirements*

<table>
<tr><td colspan="5">Application</td><td rowspan="6">Security</td></tr>
<tr><td>Data collection</td><td>Data analysis</td><td>Case documentation</td><td>Data management</td><td>Reporting</td></tr>
<tr><td colspan="5">Office automation</td></tr>
<tr><td>e-mail</td><td>File exchange</td><td>Text editing</td><td colspan="2">Presentation</td></tr>
<tr><td colspan="5">Infrastructure</td></tr>
<tr><td>Servers</td><td>Clients</td><td>Communication</td><td colspan="2">Interface</td></tr>
</table>

Main components in each part are shown in the Table1. Security model is described in all levels, representing the need for consideration of technical controll and security in all of three levels.

33 Law on the prevention of money laundering and the financing of terrorism, , Official Gazette of the Republic of Serbia, no. 20/2009, 72/2009 i 91/2010

34 Financial Action Task Force, http://www.fatf-gafi.org/

35 http://www.podaci.net/_z1/3123817/N-sbppnf03v0889.html

Strategically, the main objectives of the strategy of information and communication technologies are:

1) renewal, replacement and implementation of core business applications to meet business needs
2) upgrade infrastructure in recent platform to be supported by major business applications and a unique approach to work
3) development of electronic interfaces and timely electronic exchange of information
4) adequate security to support all previous strategic objectives.

Business applications are applications specifically designed and implemented to support the primary functions of the Financial Intelligence Unit, which is the detection of money laundering and terrorist financing. These applications should provide the necessary technical and technological support to the financial intelligence to perform its tasks efficiently and effectively.

Internationally, there is a need to collect and process data from banks, insurance agents, lawyers, financial services and other organizations and individuals who belong to the obligators under the current law on prevention of money laundering. This obligation includes reporting of all financial transactions in an amount of at least EUR 15 000, as well as transactions that are considered suspicious. In accordance with the law, these reports are submitted if the subject suspects that the certain transaction has features that are not considered normal for the relevant person or organization.

The key business activities include:

1) Data collection from obligators. These data are submitted electronically to the web, xls, doc, pdf or xml formats
2) Data Analysis - Using analytical tools for data processing in order to identify trends and connections of potentially suspicious transactions.
3) Case documentation - Document management of cases relating to suspicious transactions. Recording details about the suspects and the appropriate intelligence. Even at this point, Alfresco system can be used for data and documents management.
4) Document Management - An application that allows documents to be added to the case, such as Alfresco.
5) Reporting – A set of statements or reporting tools and interface connections that enable further reporting to the competent authorities.

Figure 6: summary of the main business activities undertaken by financial intelligence:

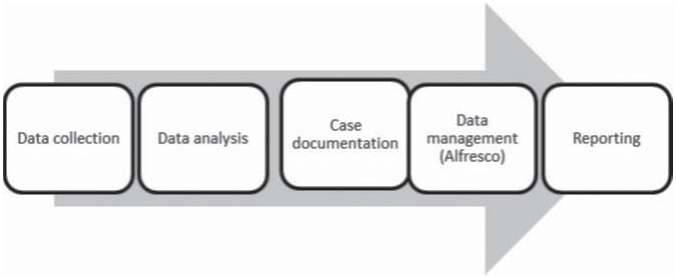


Figure 6 *Main business activities*

Data Collection - This mechanism could be a web-oriented solution that would enable online submission and receipt of the documents on the transactions from banks and other payers. The mechanism should enable the collection of data from all organizations and persons who in accordance with the law must report suspicious transactions. It would be desirable if the information of all obligators would arrive in a single format, such as XML, which would have been easy for the further processing and use, and which would ensure compatibility with other systems.

Data analysis -Data processed should be submitted electronically, without being in a format that will allow the use of analytical tools. Initially, the data should be coming from the described mechanisms for data collection.

The database is filled out online financial transactions secured by a system of data collection, but in the further processing it also should be able to accept data from the document management system.

Case documentation – Cases and investigations are progressing and there is the increasing need of monitoring the status of a case. It is necessary to enable reporting to the competent authorities such as the police and prosecution.

The strategy includes obtaining the case management system that can send and update the status of the cases to other subjects through electronic messages. It is understandable that there is a possibility to include the needs of case management systems within the specifications for the document management system, and that Alfresco could fully meet the needs.

Document management- Obligors obtains a large amount of additional information, and a lot of these information are submitted in paper form. Appropriate content management system should be able to connect obligors with a document management system through the website.

Notifications, new tasks and new messages can be sent to staff reminding them to check their accounts, to carry out activities or provide additional information.

Reporting - The obliged entities under the Law send to the Administration reports on suspicious transactions and persons. The Administration then analyses these reports and collects any additional data about them. If it finds reasonable grounds to suspect money laundering or terrorist financing in a specific case, the Administration then discloses such data to the relevant bodies, primarily the competent prosecutors' offices and police.

Some of the reports are based on text documents, while others must include detailed financial and other information. Information ,that are required for reporting should be in the electronic database, and writing tools must be in the screening system for case management and document management systems. Alfresco DMS could also fully cover this function.

Automation of Office programs - There is a need for automating Office applications. The need for software that allows all users to write text (word processing), create spreadsheets (spreadsheets) and presentation (presentations). A numerous users would benefit from the access to the drawing software, such as Microsoft Visio.

The strategy states that the organization will have continuous need for each of these applications. Given that users are familiar with the work within these applications, implies that this software package will continue to be the basis for all future upgrades.

Strategy predicts that automation software for Office programs should be improved in Microsoft Office 2010. The purchase of drawing software – MS Visio is also anticipated, especially for IT sector and other (mall number of) users.

It is necessary to implement some of the options for local correspondence between departments, beside the official OWA - Outlook Web Access, which is executed over the internet. One of the options is to introduce local exchange server. Exchanging e-mails at the local level provides the following benefits:

- Exchanging administrative, internal e-mails between departments, including the exchange of confidential content between departments, faster transfer of information without need for internet.
- Manage workflow – activities management would be included in case management system and
- General management of financial intelligence system and local control.

Infrastructure - The existing infrastructure includes:

1) Client - PC and laptop computers

2) Servers - devices for applications and data storage

3) Network and communication equipment

Clients - There should be a continuous plan for 5 year period that would include replacing PCs and introduction of a standard computer configuration

Specified minimum configuration is based on the order that the ICT team prepared for 7 desktop computer in November 2012.

Standard specification for PC is given at the Table 2.

Table 2 *Standard specification for PC*

Component	Description
Processor	Intel Core i3 or i5
RAM	8Gb
Hard drive	2x 320Gb Sata ii
Graphics	1Gb
LAN port	Gigabyte
Multimedia	DVD +- RW
Monitor	Min 19inch plasma
Operating system	Windows 7

Specification for a laptop is given at the Table 3.

Table 3 *Standard specification for the laptop*

Component	Description
Processor	Intel Core i3
RAM	4Gb
Hard drive	500Gb
Graphics	1Gb
LAN port	Gigabyte
Wi-Fi enabled	
Multimedia	DVD +- RW
Monitor	15,6”
Operating system	Windows 7

Specification for notebook is given at Table 4.

Table 4 *Standard specification for notebook*

Component	Description
Processor	Intel Atom 1.6 GHz
RAM	2Gb
Hard drive	320Gb
LAN port	Gigabyte
Wi-Fi enabled	
Monitor	10,1”
Operating system	Windows 7

Servers **–** needed storage capacity and servers should support applications and network management. Currently, storage needs are based on the access to Network Attached Storage – the server storage. The advantage of these devices is apart from being cost – efective solution, which is managed via the web. They also can work independently from the network devices. Safety of data depends on the predecribed authoriyation and structural file.

The strategy envisages the following initial storage needs:

Storage specification is given at Table 5

Table 5 *Storage specification*

Component	Description
Processor	2.3 GHz Dual Core
RAM	1Gb
Hard Drive	2x 320GB Sata ii
External USB ports	4
eSATA ports	2
LAN ports	2 X Gigabyte
HDD (replaceable)	4 HDD x 1TB

Application servers - their specification depends on the needs of the application. The strategy envisages wherever is possible to deploy a server by using virtualization software to reduce the need for space, save energy and resources as well as the need for further upgrading the UPS.

Microsoft Exchange Server - enables local storage of e-mails and a possibility of sending e-mails within the team or between teams.

Domain Controller - This server would be implemented as Active Directory and would centrally manage user authentication, access, and so on. The advantage is that team could centrally create and delete user accounts, assign, create and delete passwords and other, through group procedures

Virtualization – Virtualization software might be VMware or HyperV.

Windows Server 12 or Open Source – Linux – In case that open source system – Alfresco is chosen as a solution for DMS. Windows Vista / 7 / 8 – it is an intention for clients to standardize at MS Windows

platforms whereever is possible. This would allow the team to more easily maintain systems and develop a standard configuration for client computers.

Network – In nest five years network design should change and further improvements are needed. The main elements and design assumptions are as follows:

Existing CAT 5-6 network cable is acceptable for a defined period. ICT team has started replacing existing switches with switches that can be managed. Currently selected the Cisco Catalyst 3560 Series WS - c .This individually manage local network and allows certain restrictions on the network, which can be of great benefit.

Internet network needs to be upgraded in order to cover the creation of the server control domain (Domain Controller Server) allowing centrally managed user accounts, privileges and establishing a central security and other group policy. This will include the implementation of an Active Directory domain (AD) for each network. Enable user authentication, etc.. Both networks should continue to be physically separated from one another.

Each network should have a specific client computers that are connected to them. 15 employees who need access to a secure network, need to have two devices for computer clients; one connected to both of networks. KVM switch is needed to allow a single screen, keyboard and mouse to be used on each table. Internet users must have a computer. Clients on the secure network must be additionally secured with a password of appropriate length and it is necessary to configure the Mac Address & port authentication, what means that only authorized devices will be able to connect. The Internet also should have a domain controller and print capabilities. Outlook Web Access (OWA) to the e-mails, allowed by the central office is considered to be adequate for a period of 5 years.

Security – Administration is considered a sensitive part of the criminal justice environment and the security of their system of information and communication technology is considered very important. That is determined by strategic goals of the electronic data exchange with parner organizations including the police and the prosecution.

This strategy defines minimum security standards:

- All users will have individual user identification (UserID) and password to access the network and business applications. This will allow the application of the certification principles;
- Users should be divided into ordinary and privileged users (administrators), and all users must have a minimum level of access
- Passwords will be set to the minimum size and complexity. ICT policy states that it takes at least 9 characters.
- All business applications will be able to test audit, and that must be conducted. Regular reports will be drawn up and reviewed by the security officers in the department, who will monitor every concerning transaction.
- Systems should be configured to ensure that the patch - Security Updates are regularly applied in order to reduce the possibilities for disruption of the known weaknesses or abuse;
- System tools and functions are not necessary for normal operation of the system and applications, and should be removed;
- Internet access should be controlled through procedural and technical policy, and use of the Internet should be recorded. The overall Internet traffic should be treated through a proxy server that enables secure remote management access.

Planed activities – The Strategy predicts that Administration will move forward to the new integrated system during the next five years. Following issues are suggested:

1) Improving infrastructure by providing centralized storage, increasing the possibilities of the central management and the degree of correlation
2) Installation and use of i2 iBase 8 Database
3) The implementation of a case management system and documents (Case Management Document Management System (DMS) along with enhanced reception of data, and
4) Implementation of advanced electronic integration together with the competent authorities

The approach is based on available resources and the stipulated time period necessary for the implementation of applications to work with the case and the procurement of the combined system for receiving data, case management and documentation (Data Capture, Case and Document Management System).

It is anticipated that the infrastructure has two phases to establish. The first relates to the implementation of server storage and create a central folder structure. The second phase is the implementation of enhanced LAN network security.

The need for data analysis can be solved by implementing a database iBase 8 to allow a greater use of analytical software I2, which is already sold.

Purposes related to the receipt of information, case management and documents (Data Capture, Case Management and Document Management) can be realized through a single solution, so that each part of the functionality is implemented in a modular way. A perfect choice would be just Alfresco. Business processes related to the cases will be promoted in order to support the necessary investments.

CONCLUSION

When choosing the right document management system users primarily assume that the system should be able to easily transform paper and electronic documents in the kind of file that will be easy to process, search, distribute and facilitate the work and co-operation on it. The best software includes tools for tracking the flow of documents to ensure the following of appropriate processes and procedures. The system should include multiple levels of security, so as the curious eyes would not have access to sensitive documents without proper permission. Search tools are of equal importance. If the program can read your files and scanned documents, search is easy to start and not only searching the text but also in other types of records. The best document management software will create metadata to help organize your documents and later allow an easy retrieval of documents and files.

Through the example of Alfresco module that enables digital signature and the verification of signatures within Alfresco, we have shown the mere act of signing on the client and creating the signature in Alfresco, in the form of an XML document that is in accordance with XML signature specification. In the early stages of use of the document management systems, one of the major problems was that most of the documents had to be signed, and that meant that original electronic document contained a scanned copy of manually created signature. This caused a lot of problems such as unnecessary redundancy of data, and breaking the workflow on stages before and after signing the document. The absence of valid digital signatures for electronic documents disabled the full utilization of the DMS, and the functioning of any organization, especially police and the Administration without the use of paper.

First, the introduction of legal regulations, which in some countries happened even before the decade and a half, ensured the validity of digital signatures and has led to the increasing importance of existence of this functionality in modern data management systems. Complete module in the Alfresco system allows user to create a digital signature for any document using smart cards or keystore files. A digital signature is created by the XML Signature specification, and it can be verified not only in the Alfresco system but also outside of it. Direct relevance of this module with the undisputed importance of the document management system, is the increasement of the efficiency of the fight against the money laundering and funding of terrorism by strengthening the role of information technology as a tool for collecting and analysing not only financial information but also all other data and content that can be important in combating these types of crimes.

In the second example, as part of a strategy of information and communication technologies within the Administration for the prevention of money laundering, we have shown the place and importance of data management systems. Administration for the prevention of money laundering cooperates and communicates with numerous subjects: Ministry of Interior, National Bank of Serbia, the Republic Prosecutor's Office, Ministry of Justice, professional associations, the court and educational institutions such as colleges and academies and the associations of journalists. For such a system of subjects, we have shown the functionality of Alfresco that would directly contribute to strengthening the mechanisms and procedures and improving the technical infrastructure for the collection, analysis and exchange of data.

We tried to present in detail the Alfresco content management system in this article. We present the possibility of its usage in the area of criminal activities prevention, such as money laundering and funding terrorism. Considering how information technology contributes in combating various forms of crime, here the emphasis is on the free system of open source and open standards. At the same time, as it is presented through the examples, Alfresco is fully functional, safe and extremely usable in the fields of prevention of money laundering and the financing of terrorism.

ACKNOWLEDGEMENTS

This work was partly supported by a grant from the Ministry of Education and Science, Republic of Serbia [Project number III44007] and [Project number TR34019].

REFERENCES

1. Dournaee, B., XML Security, McGraw-Hill,2002,ISBN 0-07-222808-3
2. Microsoft corporation i koautori, Andz Ruth, i Kurt Hudson, Sertifikat Security, str.34-37
3. Thony, J.-F. (1996) Processing Financial Information in Money Laundering Matters: The Financial Intelligence Units,European Journal of Crime, Criminal Law and Criminal Justice, Volume 3, 257-282.
4. Vujakić Milica, Primena sistema za upravljanje dokumentima DocuWare u školama, master rad, Matematički fakultet, Jun 2009.
5. Vujanović Nikola, Postavljanje sistema kvaliteta prema zahtevima serije standarda JUS ISO 9000, JUSK, Beograd, 1994
6. Zurawski Richard, The Industrial Information Technology Handbook, Google Books, 28/1-5

Regulations

1. Nacionalna strategija za borbu protiv pranja novca i finansiranja terorizma („Sl. glasnik RS“, 89/2008);
2. Pravilnik o metodologiji za izvršavanje poslova u skladu sa Zakonom o sprečavanju pranja novca i finansiranja terorizma (Sl. glasnik RS“, 7/2010 i 41/2011);
3. Preporuke za prijavljivanje sumnjivih transakcija, poznavanja i praćenja stranke i zabrane dojavljivanja;
4. Law on the prevention of money laundering and the financing of terrorism, , Official Gazette of the Republic of Serbia, no. 20/2009, 72/2009 i 91/2010

Internet sites

1. http://www.alfresco.com/
2. http://www.apml.gov.rs/srp/
3. Apache XML Security, http://santuario.apache.org
4. http://docs.alfresco.com/community/index.jsp
5. http://en.wikipedia.org/wiki/Alfresco_%28software%29
6. http://en.wikipedia.org/wiki/Amigaguide
7. http://en.wikipedia.org/wiki/Apache_tomcat
8. http://en.wikipedia.org/wiki/DDLC
9. http://en.wikipedia.org/wiki/Document_file_format
10. http://en.wikipedia.org/wiki/Document_management_system
11. http://en.wikipedia.org/wiki/Enterprise_content_management
12. http://en.wikipedia.org/wiki/Metadata
13. http://en.wikipedia.org/wiki/ODMA
14. http://en.wikipedia.org/wiki/Plucker
15. http://en.wikipedia.org/wiki/SOAP
16. http://en.wikipedia.org/wiki/Telnet
17. http://en.wikipedia.org/wiki/WebDAV
18. http://pbadupws.nrc.gov/docs/ML1221/ML12216A008.pdf
19. http://www.pupin.rs/organizacija-imp/imp-racunarski-sistemi/
20. http://skerndl.blogspot.com/2010/12/osnovni-internet-protokoli.html
21. http://wiki.alfresco.com/wiki/Product_Overview
22. http://windowsitpro.com/mobile/going-wireless
23. http://www.alfresco.com/community
24. http://www.alfresco.com/resources/documentation
25. http://www.dartmouth.edu/~library/recmgmt/forms/DocLifeCycle.pdf?mswitch-redir=classic
26. http://www.js.pentagon.mil/whs/directives/corres/pdf/501502std.pdf
27. http://www.snowbound.com/solutions/document-lifecycle
28. http://www.tutorialspoint.com/wap/wap_architecture.htm
29. Internet Engineering Task Force (IETF), http://www.ietf.org
30. https://wynyardgroup.com/solutions/intelligence-2/financial-crime-2/
31. World Wide Web Consortium (W3C), http://www.w3.org/
32. XML Signature Specification, http://www.w3.org/Signature/

UDC: 351.86(497.2)
341.232(4-924.5)
338.2(4-672EU)

EUROPEAN POLICIES FOR STRATEGIC ORIENTATION OF BULGARIA IN THE FIELD OF DEFENCE – DANUBE STRATEGY

Desislava Petrova[1]
Technical University of Gabrovo

Abstract: Restructuring of the Bulgarian army which has been carried out in recent years, is oriented to change organizational and managerial nature. After Bulgaria's accession to NATO and after completion of the organizational and managerial restructuring, a time has come to invest considerable effort and resources used in the modernization of armaments, military equipment and other equipment. Processes to innovate and invest in the army have intensified greatly [1]. As a partner in NATO, Bulgaria must have a modern system for resource allocation for defense, including resources for modernization and rearmament of the army. To meet the strategic objectives, a large amount of financial resources is required. Our country has sufficient financial potential to fully update our armament. Since it can be expected to increase the resources allocated to the modernization of the army, it is necessary to build such a system for their management, to ensure the most effective spending. World practice is rich in experience and knowledge in the field of innovation management and investments, including in the field of defense. Developed modern approaches and methods provided with software and communication tools that enable rational execution of these processes.

The emphasis in the article is the Danube Strategy present on Figure 1.

Keywords: Danube strategy, European policies.

INTRODUCTION

At the end of 2010 the European Comission proposed (Communication of the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions from 8.10.2010) an overarching Strategy of the EU for the Danube Region. The Danube Strategy covers 14 European countries, 8 of which are EU Member States – Austria, Bulgaria, the Czeck Republic, Germany, Hungary, Romania, the Slovak Republic, Slovenia and 6 non Member States: Bosnia and Herzegovina, Croatia, Moldova, Montenegro, Serbia and Ukraine.

In a more integrated way the Strategy aims at contributing to [2]:

- the utilization of the potential of the Danube region by particularly fostering the efforts to overcome the economic crisis in a sustainable way;
- the improvement of the social and cultural development, competitiveness, environment management and growth based on the effective use of resources;
- the modernisation of transport corridors;
- the increase of security, etc.

Danube Region security

1 des_petrova@abv.bg

All available EU sources of funding will be used, without reserving new funds, setting new rules or creating new institutions. The Commission coordinates the Strategy development in close collaboration with the countries involved. The Ministry of Regional Development and Public Works (MoRDPW) is the National Coordinator of the Danube Strategy and coordinates the work on its development from Bulgarian side. In June 2011 the Council of the EU endorsed the Strategy. At its first meeting on 21 November 2011 in Brussels the High Level Group adopted the targets of the Strategy.

The Strategy contains a detailed Action Plan which is based on four pillars:

- connecting the Danube region (e.g. improving mobility, encouraging more sustainable use of energy from renewable sources and encouraging all the activities in the area of culture and tourism);
- protecting the environment in the Danube region (e.g. restoring the water quality, managing environmental risks and preserving the biodiversity);
- building prosperity in the Danube region (e.g. developing the knowledge society through research, education and information technologies, supporting the competitiveness of the enterprises and investing in people and skills);
- strengthening the Danube region (e.g. promoting the institutional capacity and improving the cooperation on tackling organized crime).

11 Priority Areas, all of which are jointly coordinated by two Danube countries, have been set up within these 4 pillars.

- Bulgaria coordinates Priority area 3 "To promote culture and tourism, people to people contacts" in partnership with Romania;
- Bulgaria coordinates Priority area 11 "To work together to promote security and tackle organized and serious crime" in partnership with the Federal Republic of Germany.

The task of the coordinators is to provide assistance in the process of implementation of the Strategy by agreeing a working program and establishing together with the countries involved and partners sources of funding.

The Coordinators are helped by Steering Groups represented by all 14 Danube countries.

PRIORITY AREA 11

Together with the Federal Republic of Germany Bulgaria took on the coordination under Priority Area 11 "To Work Together to Promote Security and Tackle Organized Crime". The Ministry of the Interior of Bulgaria partners The Federal Ministry of the Interior of Germany and the State Ministry of the Interior of Bavaria.

The targets proposed under Priority Area 11 are the following:

- Efficient exchange of information between the relevant law enforcement actors with the aim of improving security and tackling serious and organized crime in the 14 countries by 2015;
- Effective cooperation between the relevant law enforcement actors by 2015;
- Promoting the rule of law and the fight against corruption.

PRIORITY AREA 11 COORDINATION BUREAU

The Coordination Bureau provides assistance to the Priority Area Coordinators in order to guarantee the qualitative, responsible and innovative implementation of the Strategy through:

- establishing and maintaining contacts with the National Contact Points and the experts from the participating countries, the European Commission and different stakeholders;
- developing together with all the parties involved a work program and taking all necessary steps to report the progress;
- agreeing with the Priority Area Coordinators and coordinating together with the Steering Group the assessment of the project ideas which are being submitted;
- facilitating the practical aspects of the work including the organization of meetings of the Steering Grou.

The MoI is committed to implementing the tasks of the Priority Area 11 Coordination Bureau.

EUROPEAN COMMISSIONER HAHN ANNOUNCES PRIORITY AREA COORDINATORS FOR EU STRATEGY FOR DANUBE REGION

In order to develop the huge economic potential of the Danube European Commission proposes at the end of 2010 a comprehensive strategy for the Danube Region, which covers eight Member States and six other European countries. This strategy focuses on specific priority areas of action, such as improvement of navigability, water quality, cooperation on security issues and opportunities for tourism. For implementation of the strategy in place, Commissioner for Regional Policy Johannes Hahn and Hungarian Foreign Minister Janos Martonyi announced which countries and regions will lead priority areas of work and they have established 11 priority areas.

The strategy aims to close cooperation between countries, so that optimum use of all available funding from EU, without committing new funds to set new rules or creating new institutions. Strategy brings a new and ambitious dimension to cooperation in the region and each Member State is responsible for at least one area of work and a number of countries not members of the EU will also play an active role. Danube region stretches from Germany to the west to Ukraine in the east. It faces a number of challenges including untapped shipping potential, lack of road and rail connections and lack of coordination in the field of education, research and innovation. Cooperation in the "macro-regional framework" aimed at achieving more effective coordination. Such an approach has been applied successfully for the first time in the Baltic Sea region and does not imply new laws or institutions but rather strengthens links between different policies and a wide range of stakeholders. This form of cooperation can be applied to solve problems such as flash floods, destruction of important habitats for biodiversity in Europe and illicit trafficking. It can also give rise to new opportunities - for example by improving navigation on the river and interconnection of national energy markets aimed at preventing the emergence of a shortage of electricity and fuel shortages.

To achieve the objectives of the strategy has a number of actions which contribute significantly to the implementation of the broader objectives of sustainable and smart growth set in the strategy „Europe 2020". Member appointed as the coordinator for the priority areas are presents in the next table:

Priority Area	Countries
1) To improve mobility and intermodality	Inland waterways Austria Romania Rail, road and air Slovenia Serbia (Interest: Ukraine)
2) To encourage more sustainable energy	Hungary Czech Republic
3) To promote culture and tourism, people to people contacts	Bulgaria Romania
4) To restore and maintain the quality of waters	Hungary Slovakia
5) To manage environmental risks	Hungary Romania
6) To preserve biodiversity, landscapes and the quality of air and soils	Germany (Bavaria) Croatia
7) To develop the knowledge society (research, education and ICT)	Slovakia Serbia
8) To support the competitiveness of enterprises	Germany (Baden-Württemberg) Croatia
9) To invest in people and skills	Austria Moldova
10) To step up institutional capacity and cooperation	Austria (Vienna) Slovenia
11) To work together to tackle security and organised crime	Germany Bulgaria

CONCLUSIONS

Restructuring of the Bulgarian Army is oriented toward changes of organizational and managerial nature. The Danube Strategy aims close cooperation between the countries so that optimum use of all available funding from EU, without committing new funds to set new rules or creating new institutions. Strategy brings a new and ambitious dimension to cooperation in the region and each Member State is responsible for at least one area of work and a number of countries not members of the EU will also play an active role.

The Strategy contains a detailed action plan based around four pillars:

- Connecting the Danube Region (e.g. improving mobility, encouraging sustainable energy and promoting culture and tourism);
- Protecting the environment in the Danube Region (e.g. restoring water quality, managing environmental risks and preserving biodiversity);
- Building prosperity in the Danube Region (e.g. developing research capacity, education and information technologies, supporting the competitiveness of enterprises and investing in people's skills);
- Strengthening the Danube Region (e.g. stepping up institutional capacity and improving cooperation to tackle organised crime).
- It also proposes a number of time-limited targets for focus efforts, including:
- develop efficient multimodal terminals at Danube river ports to connect inland waterways with rail and road transport by 2020;
- implement the Danube wide flood risk management plans - due in 2015 under the EU Floods Directive – and include significant reduction of flood risk by 2021;
- reduce nutrients to restore eco-systems of the Black Sea to 1960 levels by 2020;
- invest 3% of GDP in Research and Development by 2020.

REFERENCES

1. Tzvetkov, Tz., Innovation and Investment in Defense, Sofia 2004, ISBN 954-494-618-7
2. www.europa.eu

UDC: 343.533:004.738.5(497.11)
351.862.4(497.11)

LACK OF COMPUTER EMERGENCY RESPONSE TEAM IN THE REPUBLIC OF SERBIA – A SECURITY CHALLENGE

Dejan Vuletic[1]
Jovanka Saranovic[2]
Strategic Research Institute, Ministry of Defence of the Republic of Serbia
Jan Marcek[3]
University of Defence, Belgrade

Abstract: Computer Emergency Response Team (CERT) strives for safer cyber space for all organizations and citizens by responding to information security incidents, analyzing threats, and exchanging information with trusted partners around the world. The paper gives a brief description of the role, purpose and mission of a computer emergency response team. The final part of the article analyzes the situation in Republic of Serbia and gives recommendations on this issue.

Keywords: computer incident, cyber security, emergency response.

INTRODUCTION

Global trend shows a rapid increase in cyber attacks. The intensity of today's targeted attacks has grown in sophistication. The fundamental role of a sovereign government in defense against cyber threats is to maintain normal functioning of the society in times of crisis, protect essential services and critical national infrastructure, etc.

Managing cyber security through a national strategy is a necessity inherent to all national governments in the 21st century. Critical infrastructure in most nations, from transportation and power generation to food supply and hospitals, depends on Information and Communications Technology (ICT). The reliance on complex and constantly evolving technology is pervasive across all sectors of critical infrastructure, making it very difficult for national governments to understand and mitigate risks related to this technology.[4]

ABOUT CERT

A National CERT is a significant operational component of a national approach to executing cyber security strategy.[5]

History of CERT is related to appearance of malicious programs. This kind of team was first created at Carnegie Mellon University as a consequence of the appearance of the computer worm (Morris Worm).

A National CERT is a team that responds to computer security or cyber security incidents by providing necessary services to a defined constituency to effectively identify threats, coordinate at national and regional levels, as well as provide information dissemination. It also acts as a focal point for the constituency in matters related to cyber security. CERT primarily focuses on the response to ICT related security incidents on behalf of one or more stakeholders. In order to provide an overarching cyber security service to a constituency, most CERTs render out services such as reactive services, proactive services and security quality management services. At a minimum, a National CERT should provide incident response services to a defined constituency.

There are several acronyms used to describe teams providing similar types of services such as:

- CERT (Computer Emergency Response Team)
- CERT or CERT/CC (Computer Emergency Response Team / Coordination Centre)

1 dejan.vuletic@mod.gov.rs
2 jovanka.saranovic@mod.gov.rs
3 jan.marcek@mod.gov.rs
4 Haller J., Merrell A.S., Butkovic J.M., Willke J.B., *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability*, Software Engineering Institute, Carnegie Mellon University, Pittsburg, 2010, p.1.
5 *Ibid*, p.22.

- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)
- WARPs (Warning Advice and Reporting Points)[6]

The benefits of having a CERT. Having a dedicated IT security team helps an organization to mitigate and prevent major incidents and helps to protect its valuable assets. Further possible benefits are:

- Having a centralized coordination for IT security issues within the organization (Point of Contact, PoC).
- Centralized and specialized handling of and response to IT incidents.
- Having the expertise at hand to support and assist the users to quickly recover from security incidents.
- Dealing with legal issues and preserving evidence in the event of a lawsuit.
- Keeping track of developments in the security field.
- Stimulating cooperation within the constituency on IT security (awareness building).[7]

National CERT. A CERT with a national focus, considered as security point of contact for a country. This type of CERT usually does not have direct constituents, as the national CERT only plays an intermediary role for the whole country.[8]

These CERTs are focused on and provide services and support to their defined constituency for the prevention of, handling, and response to cyber security incidents. However it is also possible for a country to designate an entity as a national CERT to serve a principle entity serving Government or government-related organizations.[9]

A CERT needs to act as a focal point for incident reporting and to be easily reached by users. A CERT has three essential attributes:

- a central location in relation to its constituency
- an educational role with regard to computer security
- an incident handling role.[10]

CERT is key tool for Critical Information Infrastructure Protection (CIIP). Currently, there are hundreds of CERTs in the world.

National CERT issue instructions, guidelines, recommendations, advices and opinions in the case of incidents in cyberspace that are of importance for information security in specific country.

CERT is formed on the basis of the law (e.g. Information Security Law) or by another government regulation. The scope of CERT's work does not include operational troubleshooting and concern about the protection of computer systems, initiation of criminal charges, punishment and arbitration of disputes.

The existence of national CERT does not exclude the presence of other CERTs in the country. The role of the national CERT is to coordinate their work.

National CERT cooperates with relevant bodies at national institutions (Ministry of Interior, Internet service providers, private IT companies ...) and internationally (e.g. Forum of Incident Response and Security Team - FIRST).

In order to create an effective CERT, Carnegie Mellon University believe that there are four core principles all CERTs must have:[11]

- Technical Excellence**:** The National CERT should have the most up-to-date resources and advice and in order to maintain this advantage, the advice they give must be sound which requires high levels of technical excellence. This may lead to the CERT only being initially with a small number of good quality capabilities rather than lots of poor quality capabilities.
- Trust**:** If the organizations and end users do not explicitly trust the CERT then they will be unable to share data with the CERT and will not be able to use all the facilities on offer. The trust is crucial for partner organizations and the organizations themselves would want confirmation that the CERT can handle sensitive information responsibly.

6 *Computer Emergency Response Teams (CERTs) An Overview*, Global Cyber Security Capacity Centre, University of Oxford, 2014, p. 6.
7 *A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT*, European Union Agency for Network and Information Security, 2006, p. 7. www.enisa.europa.eu
8 *Ibid*, p. 9.
9 *Computer Emergency Response Teams (CERTs) An Overview*, op.cit., p. 8.
10 *Ibid*, p.6.
11 *Ibid*, p.8.

- Resource Efficiency**:** The CERT must be constantly adapting by analyzing potential new threats and their potential impact. This will then help to steer the allocation of funding sources to test, which treats and incidents are truly of interest to the CERT.
- Cooperation**:** The CERT should cooperate as fully as possible (taking into account the sensitivity of some of their clients' data) with national stakeholders, government and other National CERTs so that the knowledge can be shared and they can collaborate on complex problems.

A CERT can most easily be described by analogy with a fire department. In the same way that a fire department has an emergency number that you can call if you have or suspect a fire, similarly a CERT has a number and an email address that you can contact for help if you have or suspect a computer security incident.[12]

Another similarity between fire departments and CERTs is that responding to emergencies is only part of the service provided. Just as important is trying to prevent emergencies from occurring in the first place. So just as a fire department offers fire safety education to raise awareness and encourage best practices, CERTs produce technical documents and undertake education and training programs for the same purpose. In the area of improvement, a fire department will influence laws to ensure improved safety codes and fire-resistant products. Similarly CERTs participate in forums to improve baseline security standards.[13]

Without providing at least a component of the incident handling service, the team cannot be called a CERT. Consider the analogy with a fire department. A fire department may provide a range of services (fire prevention, awareness, training), and it may undertake fire safety inspections. But at the core is the emergency response component.[14]

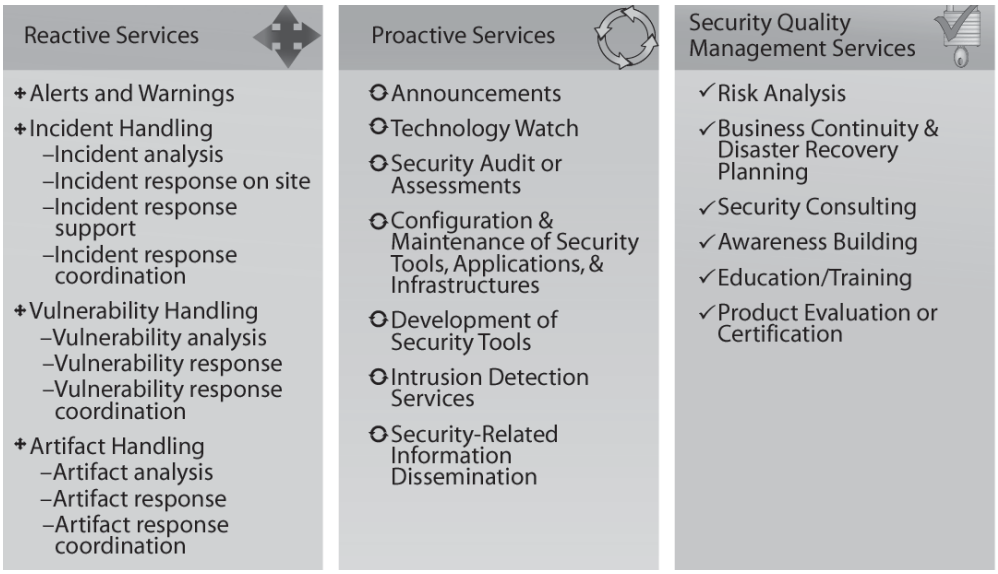
Constituency. During the course of its operation, every CERT will interact with a wide range of entities. The most important of these is the specific community that the CERT was established to serve: its constituency. A CERT constituency can be unbounded (the CERT will provide service to anyone requesting it), or it can be bound by some constraints. Most commonly, CERTs have bounded constituencies that tend to be a reflection of the CERT funding source. The most common constraints that are used to bound a constituency include national, geographical, political (e.g., government departments), technical (e.g., use of a specific operating system), organizational (e.g., within a given corporation or company), network service provider (e.g., connection to a specific network), or contractual (e.g., the customers of a fee-for-service team).[15]

CERT Services. For a team to be considered a CERT, it must provide one or more of the incident handling services: incident analysis, incident response on site, incident response support, or incident response coordination. The incident handling service includes incident analysis with at least one of the other incident handling services: incident response resolution, incident response support, or incident response coordination (see below for detailed explanations of the differences). In practice, we see that CERTs commonly offer other services in addition to the basic incident handling service, depending on the needs of its constituency. These additional services might be provided by the CERT alone or in cooperation with other organizational units (such as the IT or security department).

There are many services that a CERT can offer. The Services that each CERT provides should be based on the mission, purpose, and constituency of the team. CERT services can be grouped into three categories (see the next figure):[16]

- Reactive services. These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CERT work.
- Proactive services. These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.
- Security quality management services. These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CERT performs or assists with these services, the CERT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

12 West-Brown J.M, Stikvoort D. Kossakowski K.P., *Handbook for Computer Security Incident Response Teams (CSIRTs),* Software Engineering Institute, Carnegie Mellon University, Pittsburg, 2003, p. 2.
13 *Ibid*, p. 2
14 *Ibid*, p. 9.
15 *Ibid*, p. 11.
16 *Ibid*, p. 23.



CERT services[17]

SERBIA AND CERT

Information and Communications Technology infrastructure, computer systems and users in Serbia are exposed to and suffer from most of the cyber threats and attacks affecting the rest of the world. These include malicious software, electronic fraud, web defacement, etc

Cyber threats are recognized by Serbian laws, strategic and doctrinal documents. Information Society Development Strategy in the Republic of Serbia until year 2020 defines that it is necessary to establish a national CERT that will be responsible for computer incident management at the national level.[18] However, CERT is not yet established.

It is urgent that the Government of Serbia should focus on setting up a National CERT which must be appropriately positioned within the government's institutional and organizational structure as soon as possible.

There is a definite need to set up a National CERT capability in Serbia. In parallel with the formation of a National CERT for Serbia, there are also some priority areas that need immediate attention and action, including the following:

- Providing training to improve the skill-sets and competency of the personnel that will manage the National CERT in areas of cyber security;
- Improving the overall readiness, availability and reliability of ICT infrastructure and services to the public as well as the private sector;
- Developing applicable policies and regulations for telecommunication and ISPs;
- Developing and implementing cyber security awareness campaigns to the general public;
- Passing, implementing and continuously improving cybercrime legislation

In order for Serbian CERT to effectively deliver its services, several key requirements need to be identified. Most important of all is the human capacity development.

The Serbian CERT's stakeholders are responsible for the strategy and direction of the CERT and/or have a responsibility for information security within Serbia.

Serbian CERT will be serving only government agencies and the ministries within Serbia, in its early stages. CERT will have the following constituents at its initial stage:

- All government agencies
- Critical information infrastructure operators

17 *Ibid, p. 25.*
18 *Information Society Development Strategy in the Republic of Serbia until year 2020,* p. 24. www. digitalnaagenda. gov.rs

It is predicted that Serbian CERT will become the focal point to coordinate information flow, response to cyber attacks and remediation of cyber security incidents for the whole of Serbia.

Serbian CERT should start small; utilizing the available resources, then it will evolve as more resources are allocated to the team.

In the future, large organizations that are responsible for the country's critical national infrastructure should establish their own CERTs in collaboration with the national CERT.

In some institutions there are teams in charge of information security or are being built. The RCUB CERT exists in the academic sector. However, the remaining sectors do not have a coordinating body responding to incidents.

The working group responsible for the law on information security was formed. The law on information security is in the procedure and it will specify the CERT (will be within AMRES – Academic Network of Serbia, Administration for Joint Services of the Republic Bodies, The Ministry of Trade, Tourism and Telecommunications..).

It is expected that the law on information security to be adopted by the end of the year.

CONCLUSION

Republic of Serbia needs to establish a national CERT, in order to act preventively and coordinate resolution computer security incidents on the Internet.

It is necessary to adopt regulations in the field of information security which will further regulate the standards of information security, as well as the responsibilities and tasks of individual institutions in this area.

It is very important to establish an institution in the field of information security that performs verification and certification methods, software applications, devices and systems, as well as research and development. This institution should monitor and implement standards for information security in government bodies.

It is clear from the findings above, that the setting up of a National CERT acting as a focal point in managing incidents and a coordination centre to manage all the information sharing and information flow within the country pertaining to cyber security is crucial.

One of the most important elements in establishing and sustaining a National CERT is the competency of the personnel. Training and human capacity development programs must be in place to obtain professional local experts.

By forming a CERT, security challenges in cyber space will be reduced, risks will be effectively managed and cyber space will become a safer place for institutions and citizens of the Republic of Serbia.

REFERENCES

1. A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT, European Union Agency for Network and Information Security, 2006. www.enisa.europa.eu
2. Computer Emergency Response Teams (CERTs), An Overview, Global Cyber Security Capacity Centre, University of Oxford, 2014.
3. Haller J., Merrell A.S., Butkovic J.M., Willke J.B., Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Software Engineering Institute, Carnegie Mellon University, Pittsburg, 2010.
4. Information Society Development Strategy in the Republic of Serbia until year 2020, www. digitalnaagenda. gov.rs
5. West-Brown J.M, Stikvoort D. Kossakowski K.P., Handbook for Computer Security Incident Response Teams (CSIRTs), Software Engineering Institute, Carnegie Mellon University, Pittsburg, 2003.

UDC: 343.53:004.738.4
343.85:343.53

DEEPWEB AND DARKNET – POLICE VIEW

Jerzy Kosiński[1]
Police Academy in Szczytno

Abstract: The article presents the main ways how to hide your online identity and how to provide hidden services in The Onion Routing (TOR), Invisible Internet Protocol (I2P) and Freenet. The main ideas that determine the effectiveness of these solutions are shown on presented diagrams. Based on TOR example the article describes official police operations: Torpedo, Onymuos, Darknets as well as putative law enforcement activities that led to closing of the Silk Road, Silk Road 2.0, Freedomhosting and other considered as the largest Internet underground services. The article points mistakes made by offenders that despite using the TOR they may have been disclosed and arrested. It also presents the history of the creation and management of drug-dealing websites: Silk Road by Ross Ulbricht and Silk Road 2.0 by Blake Benthall. The article contains also an example of a very interesting search warrant, issued by the United States District Court for the District of Nebraska, of unspecified computers that were connected to the pedophile website located in onion domain. The article mentioned about an innovative method of TOR users de-anonymization, developed by Alexander Volynkin and Michael McCord from Carnegie Mellon University in 2014 as well as using "network investigative technique" by the FBI for the same purpose.

Keywords: Cybercrime, DarkNet, DeepWeb, tor, i2p, freenet.

DARKNET AND TOR

DarkNet[2] is defined by networks that are anonymous and protected from access by third parties. Another term, but not a synonym, used in this context is called DeepWeb[3]. A characteristic feature of these networks is decentralization, which prevents investigations and intentional or accidental immobilization. From the user's perspective, a significant difference in comparison to the open Internet is a difficulty in reaching the required information and the lack of effective tools for its search. The most common way of searching is to follow links or the usage of the indicated, very complicated links. There are several popular ways to use the DarkNet.

TOR (eng. The Onion Routing) is a virtual network that allows anonymous access to services on the Internet.TOR network, which implements the onion routing, prevents the analysis of network traffic and subsequently, provides users with almost anonymous access to Internet resources. Onion Routing is about multiple data encrypting and transmitting it through a series of randomly selected nodes (servers) called onion routers. Each node decrypts only one layer of the message in order to obtain information about the further package way. This way the proxy server in the transmission knows only node that is directly suited to the encrypted packet and onion router, which immediately gave the message. Proxy node does not know the content of transmitted information, where the package came from (unless it is the input node), or what server is the recipient of data (unless it is the exit node).Additionally before each packet is transferred, first between servers a pair of disposable cryptographic keys used to decrypt the next layer of data is sent. From the point of view of the target computer, incoming traffic comes from the output node of TOR network. This prevents from the disclosure of intermediary nodes, the origin, the recipient and the content of the message.

A simple diagram of the TOR network connection, as shown in Fig. 1 as follows:

user→node 1 (entry node) →node 2→node 3 (exit node) →target server

Packet sent by the user is encrypted with the cipher, and only node 3 has the key to decrypt it. The package includes encrypted address for node 2 and 3.The key to decrypt address of node 2 has node 1 and the key to decrypt address of node 3 has node 2. Node 3 after decryption of the package communicates with the target server. Thus, nodes 1 and 2 don't know the address of the target server. The answer is transmitted in the same way in the other direction, which means that the node 3 does not know the address of the user, because it receives encrypted packet from the target server.

1 kosinski@wspol.edu.pl
2 A computer network with restricted access that is used chiefly for illegal peer-to-peer file sharing. http://www.oxforddictionaries.com/definition/english/darknet, accessed 23.12.2014.
3 The part of the World Wide Web that is not discoverable by means of standard search engines, including password-protected or dynamic pages and encrypted networks http://www.oxforddictionaries.com/definition/english/Deep-Web?q=deep+web, accessed 23.12.2014.

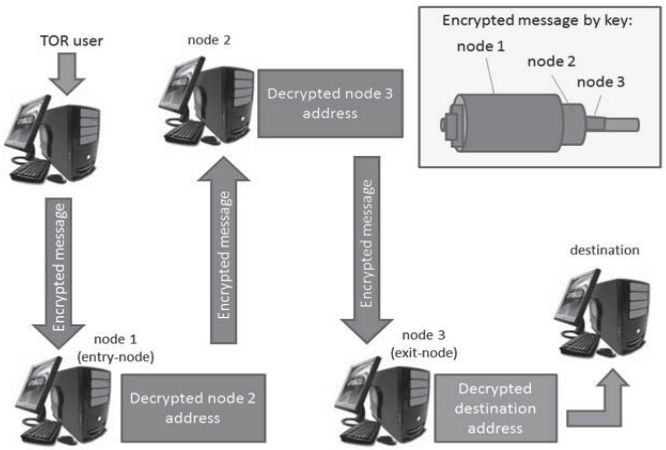


Figure 1 *How TOR connect to Server. Source: own work.*

TOR client program (a specially adapted browser which fulfills the requirements of the TOR network and TOR network addresses as well as supports pseudodomains ".onion"), after downloading the onion routers list, maps, which is determining the pseudo path chosen through a number of servers. Information about the path are encrypted in layers (Fig.1 yellow frame) with a packet sent and transmitted to the first node that proceeds with the onion routing principle described above. To complicate linking of the transferred data, TOR network regularly changes routes, that further transmit data packets. As a result, a user comes to the resource from one location (e.g. Exit-Node IP address may suggest a location in the Netherlands), and already in the next 3 minutes from a different one (e.g. IP address Exit-Node is located in the USA).

Internet user wishing to use the TOR network must have the software client. At the launch of the TOR network client, a current list of nodes from the Internet is collected, which changes over time, as more users of the system switch on and off their servers. Also public keys that will be used to encrypt the transmitted packets are collected. TOR nodes are primarily run by users who wish to support the development of TOR – representing individuals, companies and organizations that care about anonymity on the web.

In addition to the user's IP address anonymization, TOR network allows hidden operation services that do not reveal the IP address of the server, that is: it's location in the network. Access to them can be reached only via the TOR top-level pseudodomains ".onion" (Fig. 2). The domain name server is set automatically when the hidden service is configured. Addresses are not really DNS names (eng. Domain Name System), and the domain ".onion" is not part of ICANN registry and is also not listed in the TLD (eng. Top Level Domain) registry. A visit to the website located at the domain ".onion", e.g. http://vjelr2xdaqsgslzr.onion without use of TOR client software will fail. Through the use of TOR client, browsers and other programs that access the Internet can use the TOR network.

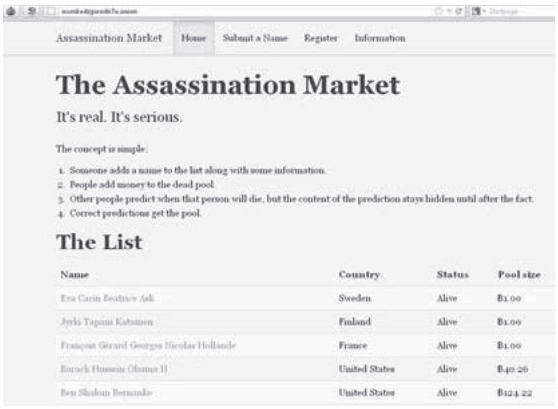


Figure 2 *Example of a service in TOR Network, accessed 23.12.2013. Source: author's archive.*

TOR network users can't be hundred percent sure that applications running in the background, or plugins installed additionally to the Web browser do not communicate parallel to TOR, the normal way via the Internet, destroying the anonymity. This problem concerns applications that don't use the SOCKS protocol.TOR also bypasses all kinds of programs designed to search for resources, e.g. Google Desktop. This problem is partially solved by the query routing mechanism built into the TOR software called Privoxy, a program acting as a server, which assists in controlling the access to the Internet and is equipped with advanced filtering capabilities, privacy and access control as well as the removal of ads and banners.

I2P

There are alternatives to the TOR, fortunately for law enforcement agencies not yet as popular, systems that provide anonymity on the Internet and allow for anonymous Internet services. One of the promising system to be highly used by criminals is I2P network (eng. Invisible Internet Project) that supports the most common Internet activities such as web browsing, using e-mail, file sharing, etc..In contrast to the TOR whose main objective is anonymous access to pages of the "normal" Internet, I2P is more focused on closed DeepWeb, separated from the "normal" internet. Someone who works in I2P can run the anonymous server in the domain ".i2p" (so-called eepsite), which is available only with I2P network (like TOR hidden services in the domain ".onion").For example, the homepage I2P you can access from the I2P network via http: //www.i2p2.i2p. I2P action is based on the absolute separation between software computers participating in the network (router) and the anonymous endpoints (destiny), associated with hosted applications. The fact that someone is working in I2P is usually not a mystery. Information about what the user is doing, if anything at all as well as what router is connected to the end point (destination) is hidden.

Users have usually several local endpoints on your router, e.g. one for the anonymous web servers (eepsite) and another for torrents. Another important term needed to understand I2P is a "tunnel". A tunnel is directed pathway through a clearly selected list of routers. While passing through the routers use the layered encryption is used, which means that each of the routers can only decrypt a single layer. Decrypted information includes the IP address of the next router along with the encrypted information to be transmitted. Each tunnel has a starting point (the first router, also known as the "gate") and an end point. The message can be sent in one direction only. In order to send messages back, you need a different tunnel. There are two types of tunnels: "Outbound" that send a message from the creator of the tunnel and "Inbound" that deliver a message to the originator of the tunnel. The combination of these two tunnels allows you to send messages from the sender to the recipient. In order to connect both tunnels I2P network database (netDb) necessary is needed. This database provides the information necessary to contact a specific router (public keys, transport addresses, etc.) and the data necessary to contact the intended (the gateway, which enables a destination, the lifetime of the tunnel, a public key pair to encrypt messages). Schematic representation of the I2P network is shown in Fig. 3.

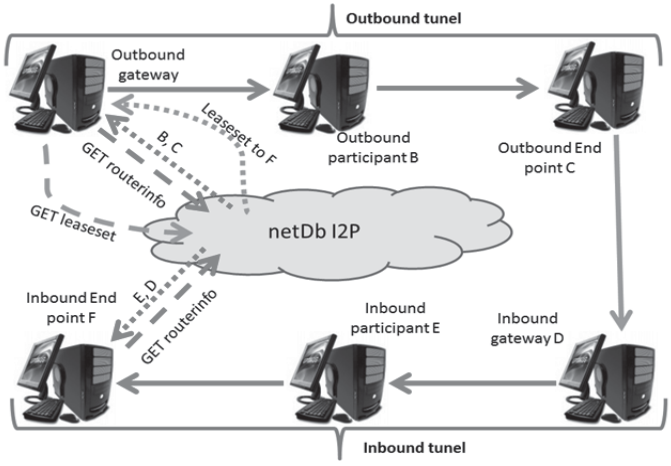


Figure 3 *Simplified diagram of how a I2P network functions. Source: own work, based on http://geti2p.net/en/docs/how/tech-intro.*

FREENET

A different DarkNet network is Freenet, focused on sharing of files (from author's own experience largely infected by malware). Freenet is a distributed repository of data with the characteristics of P2P. Unlike other P2P networks, the user has little or no influence on what is stored in the data warehouse. Files are stored or disposed of, depending on how popular they are. To use Freenet a client software[4] and access data are needed. Each file that exists in Freenet is assigned a key associated with it, which is equivalent to a URL (eg. KSK@sample.txt or SSK@rBjVda8pC-Kq04jUurIAb8IzAGcPAgM).Freenet 0.7 version has 4 kinds of keys[5], most of which are calculated hash values[6]. Freenet users make disk space available on their computers (originally allocated for the data store is a 5% free space on the disk), and links for other participants. Data transfer is not done directly, but through other network nodes. It is usually a chain of several nodes, which makes it unclear whether the user, with whom we are connected to, has the data in its hard disk or just is a middle-man. The Transmission and the stored data are encrypted. Therefore, the user cannot see what data is stored on his disk and he cannot track exchange of data. Freenet does not allow you to browse the Internet, aside from specific sites belonging to Freenet. Materials in Freenet are split into pieces and placed on a large number of nodes. All parts of the files are encrypted and stored in the Freenet installation directory. Users only keep parts of individual files and are directly connected to a small number of other nodes (min. 5). If the user wants to download a file, it sends to a neighboring node it's description. Routing of the request to the neighboring nodes is random. If the asked node has the desired file, then the node forwards the file to the node that made the request, if not, it sends the request further. Each node has only the information from the node directly linked to it, so you cannot determine to who the data is supposed to go (Fig. 4).

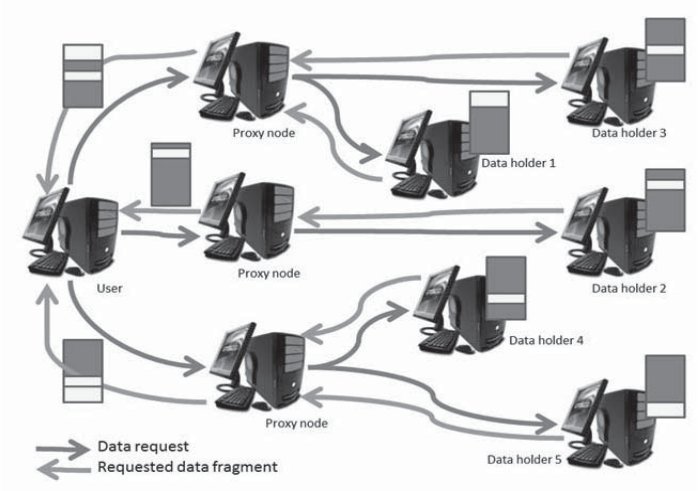


Figure 4 *Acquiring a file in Freenet. Source: own work.*

POLICE LOOK AT TOR

On November 7, 2014, Europol informed about the operation conducted on November 5-6, and coordinated by the Europol's European Cybercrime Centre (EC3), the FBI, the U.S. Immigration and Customs Enforcement's (ICE), Homeland Security Investigations (HSI) and Eurojust, called Onymous[7]. The action aimed to stop the sale, distribution and promotion of illegal and harmful items, including weapons and drugs, which were being sold on online "dark" marketplaces and resulted in 17 arrests of vendors and administrators running these online marketplaces and more than 410 hidden services being taken down. In addition to the takedowns of drug markets Silk Road 2.0, Cloud 9 and Hydra, it's also busted contraband markets like Pandora, Blue Sky, Topix, Flugsvamp, Cannabis Road, and Black Market. Other takedown tar-

4 For download, e.g. from https://freenetproject.org, accessed 01.12.2014.
5 Keys are described at https://freenetproject.org/understand.html, accessed 01.12.2014.
6 The value of a one-way hash function. Hash in a fast and uniquely identifies the digital data, but at the same time there is no concept of hashes semantic proximity. More on the hash function can be read in P. Rodwald, *Kryptograficzne funkcje skrótu*, Zeszyty Naukowe Akademii Marynarki Wojennej, Rok LIV Nr 2 (193) 2013.
7 https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network, accessed 10.11.2014.

gets included money laundering sites like Cash Machine, Cash Flow, Golden Nugget and Fast Cash[8]. And agents have taken from criminal suspects more than $1 million in bitcoin, $250,000 in cash, as well as an assortment of computers, drugs, gold, silver and weapons[9].

One of the primary targets was the Silk Road 2.0 operator since about December 2013– the 26-year old Blake Benthall aka DEFCON (his LinkedIn profile is presented on Fig. 5), coder arrested in San Francisco. Since its launch in November 2013, Silk Road 2.0 has been used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to buyers throughout the world, as well as to launder millions of dollars generated by these unlawful transactions. As of September 2014, Silk Road 2.0 was generating sales of at least approximately $8 million per month and had approximately 150 000 active users[10]. B. Benthall has controlled and overseen all aspects of Silk Road 2.0, including, among other things: the computer infrastructure and programming code underlying the website; the terms of service and commission rates imposed on vendors and customers of the website; the small staff of online administrators and forum moderators who have assisted with the day-to-day operation of the website; and the massive profits generated from the operation of the illegal business.

Officially, an HSI agent acting in an undercover capacity successfully infiltrated the support staff involved in the administration of the Silk Road 2.0 website, and was given access to private, restricted areas of the site reserved for Benthall and his administrative staff. And or about May 2014, FBI identified a server located in a foreign country that was believed to be hosting the Silk Road 2.0 website at the time. On or about May 30, 2014, law enforcement personnel from that country imaged the Silk Road 2.0 Server and conducted a forensic analysis of it.[11]

Unofficially, on January 30, 2014 in the TOR network 115 high-speed servers have appeared. They were run by Alexander Volynkin and Michael McCord – CERT researchers from Carnegie Mellon University. Network managers noticed that, but decided not to intervene, as they considered even having control over approx. 6% of the network input nodes attacker will not be able to threaten the anonymity of its users. Unfortunately, they were wrong. On July 4, network administrators have found that these servers are running a new, previously unknown attack. The attack consisted of clever "determination" of network traffic on a single node and reading the "signature" on another node to the correlation of motion[12].Same type of attack was nothing new – in the same way most of the previous attacks were carried out, but the method of "determination" was innovative. The attacking servers were so fast and stable that they quickly received the network "permission" to perform two roles – hidden catalogs services and input nodes. There was no evidence that servers functioned as exit nodes, which means that the attack was directed only at users accessing the hidden services (domain .onion). Attackers modified nodes serving as hidden directory services that when they were questioned by the customer, they would provide information about the target point in packets with modified headers. These modifications were sent over the network to the client computer and read on the way with the input node, which also was under the control of attackers. This way, the attacker could confirm which client network (knowing its public IP address) asked about specific hidden service in the TOR. Attackers have used an interesting method for the determination of packets. They modified the headers network by sending an appropriate combination of network messages to the client. This combination of cells ("relay" and "relayearly") contained encoded name of hidden service, the customer asked for, and was transferred to the input node, which could be read and linked to the IP address of the client[13]. The attack could undoubtedly lead to the disclosure what the hidden side of the TOR was viewed by users during the period from February to June 2014, together with public IP addresses of users. Worse, such information may have been made available not only to researchers who conducted the attack on live network, but also to anyone who is listening and saving network traffic TOR input nodes. Customer traffic marking attacker could, without being aware of it, make the task easier, for example, the NSA, that could look into their vast archives of motion and read the information stored there. Nodes, substituted by attackers, were removed from the network immediately after detecting the activity (in July 2014). In mid-May at the Black Hat conference an announcement came: "You do not have to be the NSA to break TOR: deanonymizing users on TOR" presented by Alexander Volynkin & Michael McCord[14]. The topic was the gift from the heavens for FBI agents attempting to catch hundreds of criminals operating in the Tor network.

On July 22, presentation on deanonymizing users and Web services in TOR network has been withdrawn from the conference program. About July 30, Defcon – the administrator of SR 2.0, announced that

8 http://www.fbi.gov/news/pressrel/press-releases/more-than-400-.onion-addresses-including-dozens-of-dark-market-sites-targeted-as-part-of-global-enforcement-action-on-tor-network, accessed 10.11.2014.
9 http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/, accessed 10.11.2014.
10 http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court, accessed 10.11.2014.
11 http://www.justice.gov/usao/nys/pressreleases/November14/BlakeBenthallArrestPR/Benthall,%20Blake%20Complaint.pdf, accessed 16.11.2014.
12 https://lists.torproject.org/pipermail/tor-announce/2014-July/000094.html, accessed 16.11.2014.
13 https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack, accessed 5.12.2014.
14 https://web.archive.org/web/20140521040034/https://www.blackhat.com/us-14/briefings.html, accessed 6.12.2014.

in accordance with to the recommendation Tor Project had been moved to a server on a another machine, because the previous IP address could have been disclosed in the attack mention above. However, the FBI probably had already done a backup server. On the server there were found both: the SR 2.0 service and its forum (great idea to keep both services on the same server, but it should give you a taste of the genius administrator) and Defcon chat history, including many of his conversations with the former administrator of SR 2.0.

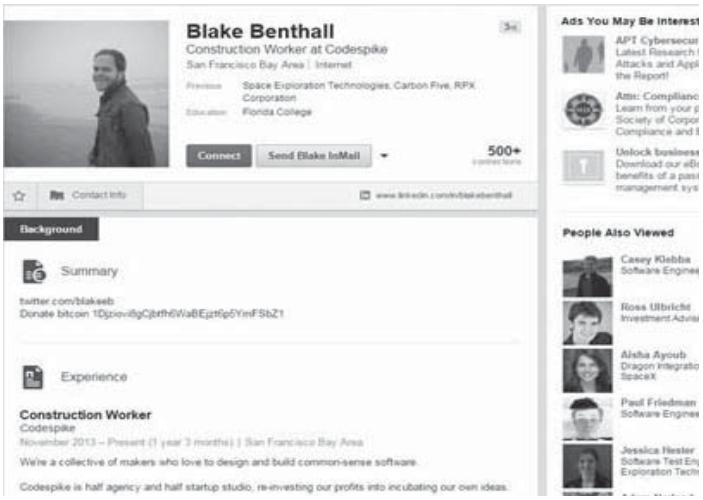


Figure 5 *LinkedIn profile for Blake Benthall. Source:https://www.linkedin.com/in/blakebenthall.*

How the FBI has identified the site owner? ... They asked the hosting company. The server turned out to be purchased using the e-mail address – blake@benthall.net. Post factum it was found that on 05/30/2014, when the FBI was probably doing server image, the owner complained about the unavailability of the machine. He sent in several letters to the hosting company. All letters came from the public IP address. On the same day, from the same IP address, someone signed in 146 times blake@benthall.net mailbox, hosted by Google. On other days service requests were sent from a different IP address belonging to the hotel where Blake Benthall accidentally happened to stop by. As if that were not enough, the FBI found further evidence linking Blake to Defcon. Blake was so smart that in his personal e-mail accounts there were set up on the stock exchanges of BTC and Web services for the direct sale of virtual currency. The FBI received the full history of his accounts and determined that he sold BTCs for more than 300 thousand USD. The history of the e-mail account indicated that at the beginning of 2014 he used 70,000$ for a down payment on a Tesla Model S, a luxury electric car worth approximately 127,000$. Agent operating on SR 2.0 had access to HTTP logs showing that Defcon used an unusual configuration of browser and operating system (Chrome 35.0.1910.3 Beta and OS X version 10.9.0 a few months earlier than the latest available on the market). The same configuration registered intermediary services used in the sale of Blake's BTCs.

There is another unofficial version of the disclosure of the relevant IP address hidden in darkweeb services. It is related to actions, which included the first version of the portal Silk Road (SR). FBI counted that during the less than 3 years of operations (from February 6, 2011 to July 23, 2013) – 9 519 664 BTCs were generated in sales. At today's exchange rate they would be worth approx. 2.57 billion dollars[15]. On the other hand, over the course of SR existence, the administrator – "DreadPirateRoberts" aka "DPR" – earned 614 305 BTCs in the way of "commissions". Who generated such a turnover? The service had 957 079 registered user accounts, which explained the scale of operations. 30% of users as the country of origin marked the USA, 27% did not provide any information on this matter. Other popular countries, according to the declaration of the users were in order of popularity: the United Kingdom, Australia, Germany, Canada, Sweden, France, Russia, Italy and the Netherlands. The scale of the operation of the service may also be confirmed by the fact that during this period the site totaled 1 229 465 transactions, in which 146 946 buyers and 3877 sellers took part. This means that at least 1/7 of the registered users on the site had had an active business. However, from where the FBI had such accurate data? According to the indictment, the FBI has found a quite complex infrastructure of the Silk Road, which servers were spread in a number of countries. One of the servers hosting the website was, on July 23, 2013, taken in by the services of a friendly country that took the image of its hard drive in a way not noticeable by the infrastructure administrator. The image was transferred to the FBI, that had a lot of time on its in-depth analysis.

15 Average bitcoin price 270 USD – source: http://data.bitcoinity.org/, accessed 05.01.2015.

The web server was just one of many machines – the FBI has also managed to attain the server supporting BTC transactions from which the FBI learned the details of the company's turnover. Interestingly, the same investigation had been going on since October 2011, and during that time FBI made more than 100 drug purchase transactions. From the indictment it can be learnt that the site administrators, acting as support, such as forum management and customer service, earned approx. 1000-2000 dollars a week – paid, naturally, in BTCs.

Officially, it has been a joint operation run by the cybercrime squad within the FBI's New York field office. It involved the FBI, DEA, IRS and Homeland Security's investigative unit.

The earliest publicity about SR is a posting dated January 27, 2011, on an online forum hosted at www.shroomery.org, an informational website catering to users of "magic mushrooms" ("Shroomery"). The posting, titled "anonymous market online?" was made by a user identified only by his username, "altoid" (Fig. 6).

Figure 6 *Altoid post on www.shroomery.org.*
Source: http://www.shroomery.org/forums/showflat.php/Number/13860995.

The next reference to SR on the Internet found is a posting made two days later, on January 29, 2011, atbitcointalk.org, an online discussion forum relating to Bitcoins ("Bitcoin Talk"). Also this posting, was made by someone using the username "altoid". The posting appeared in a long-running discussion thread started by other Bitcoin Talk users, concerning the possibility of operating a Bitcoin-based "heroin store".

Approximately eight months after his posting about SR (October 11, 2011), "altoid" stated that he was looking for an "IT pro in the Bitcoin community" to hire in connection with "a venture backed Bitcoin start-up company". The posting directed interested users responses to send to … "rossulbricht at gmail dot com" – indicating that "altoid' uses the e-mail address rossulbricht@gmail.com (Fig. 7). Ulbricht's Google+ profile includes a picture of him, which matches a picture of the LinkedIn profile for "Ross Ulbricht" (Fig. 8).

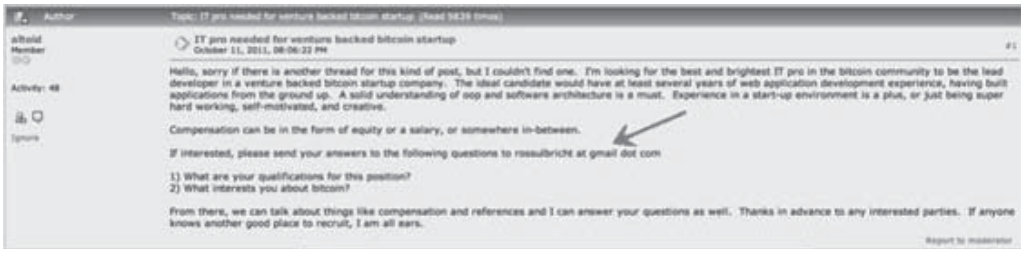


Figure 7 *Altoid post on Bitcoin Forum*
Source:https://bitcointalk.org/index.php?action=profile;u=3905;sa=showPosts

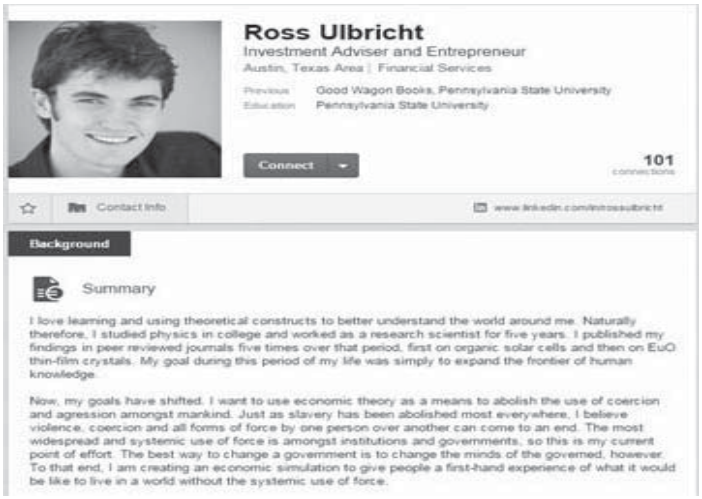


Figure 8 *LinkedIn profile for Ross Ulbricht. Source:https://www.linkedin.com/in/rossulbricht.*

On March 5, 2012, a user established an account on Stack Overflow with the username "Ross Ulbricht". A user provided the Ulbricht Gmail Account as his e-mail address as part of his registration information. On March 16, 2012, a user posted a message on the site, titled, "How can I connect to a Tor hidden service using curl in php?". Less than one minute after posting the message described above, a user changed his username at Stack Overflow from "Ross Ulbricht" to "frosty" (Fig. 9) and several weeks later Gmail Account to frosty@frosty.com (the administrator of Silk Road has a computer named "frosty", on which he maintains a user account also named "frosty", which he uses to log in to the SR Web Server).

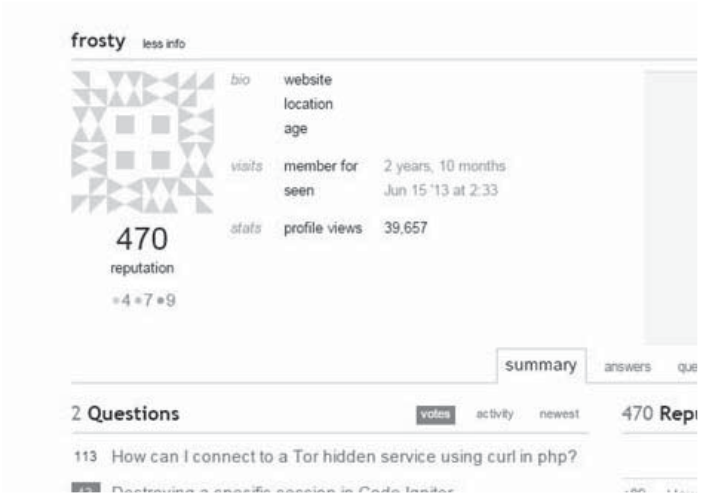


Figure 9 *Stack Overflow profile for Frosty. Source: http://stackoverflow.com/users/1249338/frosty.*

On or about January 29, 2013, DPR communicated with a federal agent in Maryland, acting in an undercover capacity (UC) via the Internet, and agreed to make two payments of 40 000$ each for the murder of the Employee, "half down now and half after the job is done". The UC provided DPR with a bank account number at Capital One Bank in Washington, D.C.to which to wire the money. On or about February 4, 2013, DPR caused approximately 40 000$ to be wired from Techno Cash Limited in Australia to a given bank account, as payment for the murder. After receiving the photograph that purported to depict the Employee's dead body, DPR caused second 40 000$ payment for the murder to be wired.

In March and April 2013 DPR solicited a murder-for-hire of a certain Silk Road user known as "FriendlyChemist", who was attempting to extort money from DPR at the time, based on a threat to release the identities of thousands of Silk Road users. A SR user called "Redandwhite" then proceeded to contact DPR, stating that he was FriendlyChemist's supplier and also the owner of his debt. DPR then solicited Redan-

dwhite to "execute" FriendlyChemist, supplying Redandwhite his full name and address. After having agreed on terms, DPR sent Redandwhite approximately 150 000$ (1 670 BTC) to have FriendlyChemist killed. Redandwhite later provided photographic proof of the alleged murder. Investigators could not find any record of somebody in that region (Canada) being killed around that date or matching that description. This possibly implies that DPR was scammed, but DPR is also quoted as having told Redandwhite the following: "Not long ago, I had a clean hit done for 80k".

On or about July 10, 2013, U.S. Customs and Border Protection intercepted a package from the mail inbound from Canada as part of "a routine" border search. The package was found to contain nine counterfeit identity documents. Each of the counterfeit identification documents was in a different name yet all contained a photograph of the same person – Ross Ulbricht (Fig. 10). The HSI agents showed Ulbricht a photo of one of the seized counterfeit identity documents, which was a Californian driver's license bearing Ulbricht's photo and true date of birth, but bearing a name other than his. Ulbricht generally refused to answer any questions but volunteered that "hypothetically anyone could go onto a website named Silk Road on TOR and purchase any drugs or fake identity documents the person wanted".

Figure 10 *The counterfeit identification documents.*
Source: http://mashable.com/2013/11/21/ross-ulbricht-silk-road-murder-journal/.

Ulbricht was arrested October 1, 2013, following a two year investigation by authorities to unmask the Dread Pirate Roberts and indicted in Maryland on charges of:

- conspiring to have a former administrator of Silk Road murdered in exchange for $80 000,
- distributing and possessing with intend to distribute controlled substances.[16]

The last indictment dated February 4, 2014, done in New York charging Ross Ulbricht on four counts for participation in a narcotics-trafficking conspiracy, a continuing criminal enterprise, a computer hacking conspiracy, and a money laundering conspiracy.[17][18]

However all these clarifications do not explain how the agents located the ST servers in July 2013. It may be helpful to remind that in August 2013, the most popular Web hosting server via TOR, founded in 2008 – Freedom Hosting was blocked. Freedom Hosting hosted servers for the most (in)famous TOR's sites:

- TorMail – long considered the most secure, anonymous e-mail on the Internet,
- HackBB – main hacking forums for various abuse, such as large money-laundering operations,
- Hidden Wiki – Wikipedia of DarkNet,
- Lolita City, Love Zone, and PedoEmpire, etc. – practically the most popular websites with child pornography.

It is estimated that Freedom handled approx. half of all sites in TOR's web[19]. For five years, both law enforcement and hacktivist vigilantes seemed incapable of shutting down the largest child pornography

16 http://www.ice.gov/doclib/news/releases/2013/131002baltimore.pdf, accessed 10.11.2014.
17 http://www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR/US%20v.%20Ross%20Ulbricht%20Indictment.pdf, accessed 10.11.2014.
18 Ross Ulbricht has been found guilty of creating and running the Silk Road. http://www.ft.com/cms/s/0/dd591c6a-ac0a-11e4-a089-00144feab7de.html#slide0, accessed 04.02.2015.
19 http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/, accessed 06.12.2014.

services on the Internet – virtually all of which were Freedom Hosting customers – thanks to the technology provided by TOR. The cause of the loss of anonymity of the servers was caused by unknown Javascripts in the board pages pointing to iframe to a Verizon server on the open web. Iframe contained JavaScript code, that by exploiting a loophole inFirefox' security performed actions on the victim's computer in order to send the collected addresses to the server in Virginia: the real IP, MAC, and host name. These Javascript exploits now widely assumed to have originated from the FBI. Working closely with the French authorities, the FBI acquired control over the FreedomHosting servers run by hosting company in France. Then moved them or cloned in Maryland, where FBI continued the investigation of their owner – Eric Marquesa. It can be assumed that the disclosed FreedomHosting servers provided enough evidence to arrest Marques, and at the same allowed the FBI set up a trap for other Tor users, among them, the manager of the Silk Road.

This suspicion is justified by the FBI activities that were carried out jointly with High Tech Crime Unit (HTCU) – Dutch police, named Operation Torpedo. In August 2011, HTCU agents posted a web crawler, for collecting all the TOR addresses and regularly visited each site with child pornography. Then, with a search warrant issued by the Court in Rotterdam, they tried to determine the physical location of the servers. Agents came onto the "Pedoboard" and found out that the owner had left an administrative account open without a password, logged in and finally found a real web server IP address in Bellevue, Nebraska. The FBI determined that the IP address belonged to a 31-year-old Aaron McGrath, who had managed not one but two sites with child porn at farm servers where he worked, and the third one at home. FBI agents did not shut down servers, but they prepared a legal framework for Torpedo Operation[20] for a year. At the end of November 2012, the FBI took McGrath in and seized his three servers, moving them to the FBI office in Omaha. The federal judge signed three separate search warrants, one for each of the three hidden sites[21]. Orders authorized the FBI to modify the code of the servers in order to install, *network investigative technique* (NIT) on all computers that were connected with these services. The judge also allowed the FBI delayed notification search purposes for 30 days (Fig. 11).


SEALED

UNITED STATES DISTRICT COURT

for the

District of Nebraska

FILED
US DISTRICT COURT
DISTRICT OF NEBRASKA
9 2012
OFFICE OF THE CLERK

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

computers that access the website "Hidden Service A" which is located at oqm56m6lyt6vxk7k.onion

Case No. 8:12MJ340

COPY

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*

See Attachment A, incorporated herein

located in the _____ District of Nebraska and elsewhere , there is now concealed *(identify the*

Figure 11 *Search warrant. Source: http://www.wired.com/2014/08/operation_torpedo.*

The NIT Installed on the servers was developed in order to identify computers that connected to the server. The NIT and from the viewpoint of computer security and privacy is malware. Within two weeks, the FBI has collected IP addresses, MAC addresses and host names of Windows from least 25 site visitors. In April 2013, five months after the implementation of the NIT, the FBI conducted coordinated strikes across the country on home addresses and names of subscribers obtained from ISP. It can be assumed that many of the subsequent arrests described in the article were also the result of this operation.

CONCLUSION

DeepWeb and DarkNet cause law enforcement agencies a lot of trouble. They ensure a large deal of anonymity for internet users and ISPs (Internet Service Provider).Worldwide law enforcement agencies seek tools and methods that will allow them to determine users and places where these services are offered[22]. Some of these methods are becoming more and more like the ones used by criminals.

20 http://reason.com/blog/2014/08/06/fbi-tracking-tor-users, accessed 07.12.2014.
21 http://www.wired.com/2014/08/operation_torpedo/, accessed 07.12.2014.
22 E.g. Russia offers 3,9 million rubles, or about $110,000 for a tool like that, http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008, accessed 30.12.2014.

REFERENCES

1. Rodwald P., Kryptograficzne funkcje skrótu, Zeszyty Naukowe Akademii Marynarki Wojennej, Rok LIV Nr 2 (193) 2013.
2. http://data.bitcoinity.org
3. http://geti2p.net/en/docs/how/tech-intro
4. http://mashable.com/2013/11/21/ross-ulbricht-silk-road-murder-journal
5. http://reason.com/blog/2014/08/06/fbi-tracking-tor-users
6. http://stackoverflow.com/users/1249338/frosty
7. http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest
8. http://www.fbi.gov/news/pressrel/press-releases/more-than-400-.onion-addresses-including-dozens-of-dark-market-sites-targeted-as-part-of-global-enforcement-action-on-tor-network
9. http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court
10. http://www.ice.gov/doclib/news/releases/2013/131002baltimore.pdf http://www.justice.gov/usao/nys/pressreleases/February14/RossUlbrichtIndictmentPR/US%20v.%20Ross%20Ulbricht%20Indictment.pdf
11. http://www.justice.gov/usao/nys/pressreleases/November14/BlakeBenthallArrestPR/Benthall,%20Blake%20Complaint.pdf
12. http://www.oxforddictionaries.com
13. http://www.shroomery.org/forums/showflat.php/Number/13860995
14. http://www.wired.com/2014/08/operation_torpedo
15. http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/
16. http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008
17. https://bitcointalk.org/index.php?action=profile;u=3905;sa=showPosts
18. https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack
19. https://freenetproject.org
20. https://lists.torproject.org/pipermail/tor-announce/2014-July/000094.html
21. https://web.archive.org/web/20140521040034/https://www.blackhat.com/us-14/briefings.html
22. https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network
23. https://www.linkedin.com/in/blakebenthall
24. https://www.linkedin.com/in/rossulbricht

UDC: 343.53:004.738.5(497.7)

CYBERCRIMES – CURRENT STATE AND CHALLENGES
THE CASE OF THE REPUBLIC OF MACEDONIA

Nikola Mickovski[1]
MIT University, Faculty of Law, International Relations and Diplomacy, Skopje
Risto Reckoski[2]
University "Sv. Kliment Ohridski", Faculty of Tourism and Hospitality, Bitola

Abstract: Today we live in a world of global digital connections. In a simple and inexpensive way, with help of modern digital technologies, we can make an ordinary conversation or multimillion monetary transactions with people who are on the other side of the world. The way we spend our leisure time and the way we conduct business relations is changed by the easy access to the computer systems and the internet as well as from the up growing market of new communication devices.

In parallel with these global transformations, the ways criminals commit their criminal acts have changed, too. The universal digital access opens new opportunities for the modern, computer savvy delinquents, who can use this technology and knowledge to cause harm not only to business users but to ordinary users as well. What is worse is the fact that the computers and networks may be even used for coordination and completion of terrorist attacks, which endanger us all. Unfortunately, in many cases, security services lag behind all those delinquents in terms of technical-technological sense, as well as in the personnel training for suppression of this new and up growing threat called computer or cybercrime.

Thus, for the Republic of Macedonia and the rest of the countries it comes as an imperative to recognize the necessity to make a legal base for sanctioning computer crimes and to facilitate adequate capacities that will effectuate the strategy for suppression of this type of crimes. Macedonian experiences in manner of creating and constantly innovating the legal framework, as well as in practical dealings with this type of crimes, may be used as a positive example of successful suppression of cybercrimes.

Keywords: computer, cybercrimes, reforms, suppression, Republic of Macedonia

INTRODUCTION

Starting from an orthodox approach in which, when writing a paper for an international conference, the author attempts (successfully or not) to explain the relevance of the issue which he writes about in the introduction of the work. To accomplish this, an almost axiomatic approach is to join the evolutionary description of the problem with the basic definitions of phenomena in the elaborated topic. Hence, the elaboration and presentation of the problem with proliferation of computer crime, especially the best known and most commonly existing type, cybercrime, and the current situation and challenges regarding its prevention in the Republic of Macedonia, shall here begin in the standard manner: with a historical - evolutionary overview and the definitions of basic concepts and notions.

How old is the phenomenon of cybercrime? It is safe to say that soon after the first computer networks were built, some people were looking for ways to exploit them for their own illegal purposes. By analogy, just as much as an idea of theft is as old as the concept of privately owned property, and an element of almost all societies is dedicated to taking as much as possible of what is not theirs—by whatever means they can. In that way as soon as it was widely recognized that computers store something of value (information), criminals saw an opportunity. But just as it is more difficult to target a robbery victim who stays locked up in his own home every day, the data on closed, standalone systems has been difficult to steal. However, when the data began to move from one computer to another over networks, like the robbery victim who travels from place to place, this data became more vulnerable. Networks provided another advantage: an entry point. Even if the information that was of value was never sent across the wire, the comings and goings of other bits of data opened up a way for intruders to sneak inside the computer, like a robber taking advantage of the victim's housemates who leave the doors unlocked on their way out.[3]

1 nmickovski@gmail.com
2 e-mail: reckoice@t-home.mk
3 Schnider L. D., Scene of the cybercrime, Syngress Publishing, 2002, p. 29.

In July 1961, Leonard Kleinrock from the Massachusetts Institute of Technology (MIT) in the application of his doctoral thesis wrote about the flow of information in large communication networks. It was the first article that introduced theories of packet commutation (packet-switching theory) - a concept in which the information is divided into packets of data, each packet is addressed to the recipient, and is transmitted from point-to-point over a computer network to the receiver where the original message is formed from the received packets. What followed from then on is history.

However, cybercrime did not spring up as a full-blown problem overnight. In the early days of computing and networking, the average criminal did not possess either the necessary hardware or the technical expertise to seize the digital opportunity of the day. Computers were million-dollar mainframe monstrosities, and only a few of them were in existence. An aspiring cybercriminal could hardly go out and buy (or steal) a computer, and even if he did, it is unlikely that he would have known what to do with it. There were no "user-friendly" applications; working with early systems required the ability to "speak" machine language—that is, to communicate in the 1s and 0s of binary calculation that computers understood.

The cybercrime problem emerged and grew as computing became easier and less expensive. Today almost everyone has access to computer technology; children learn to use PCs and tablets in day care, and people who cannot afford computers of their own can use PCs in public libraries, or they can rent computer time at business centres or Internet cafés. Applications are "point and click" or even touch and voice-activated; it no longer requires a computer science degree to perform once-complex tasks such as sending e-mail or downloading files from another machine across the Internet. Furthermore, with the advance of the cell phone technology and the smartphones and tablets, almost each one of us carries a second ready computer, 24/7 connected to the internet in our pockets and these computers are more powerful than the most advanced PCs just a few years ago. Some of today's cybercriminals are talented programmers (the hacker elite), but most are not. Advanced technical abilities make it easier for cybercriminals to "do their thing" and cover their tracks, but these abilities are by no means a job requirement.

Unfortunately this negative global trend did not bypass the Republic of Macedonia. With the widespread ingress of digital technologies in the daily life of the average Macedonian, the opportunity for easy penetration of criminal use of exactly these digital technologies has also been created. What only a few years ago was almost science fiction and a distant phenomenon that occurred there, in western developed countries, has unfortunately been filling police reports and newspapers on a daily basis, becoming a cause of constant concern for the security apparatus, attempting to prevent it. And it is them, the security apparatus and members of judiciary on all levels who necessarily need appropriate education, quality legal framework and adequate ways and methods in conjunction with up-to-date technical means for effective detection, clarification and proving computer crimes.

TOWARDS WORKING DEFINITION OF COMPUTER CRIME

Considering what (in principle) should be the easiest task in the preparation of a scientific paper, the definition of basic concepts that actually outlines the overall covered issues in the article, when it comes to computer related crimes, actually appears as one of the top challenges. The conceptual definition of the computer crime or which criminal behaviours should be framed into this generic term shall condition and further shape the overall approach to this issue, including ways to combat computer related crimes, as well as the actors involved in the process.

To be fair, much of the problem with the definition of computer crime lies in the different approaches related to its terminological determination, the dilemma encountered by the authors themselves in the preparation of this text. Although the term cybercrime is most widely used and recognized, although as somewhat exotic, because of the name from the powerful Hollywood film industry propaganda, the right term for referring to this type of illegal activity would be computer crime. This approach is endorsed primarily because of the limitations of the term cybercrime as a category of computer crime which is done by/with the network connection between computer systems.

Hence, having decided on the terminology dilemma it remains for us to focus on a conceptual definition of computer crime. With relatively peaceful conscience we can move cybercrime in the group of events of which even closely involved actors do not know the exact and complete definition, but about which even the uninitiated believe that they will recognize it once they see it. But is it that simple and what complicates the process of extraction of precise and comprehensive definition of cybercrime?

One of the reasons lies in the phenomenological features of this group of crimes - namely the computer and the network may be involved in crime in several ways:[4]

1) A computer or network may be a means for committing the crime, or used to commit the crime

4 Ibid, p. 45

2) The computer or network may be the target of the crime ("victim")

3) The computer or network may be otherwise associated with crime (e.g. storage of illegal drug trafficking data).

On the other hand, in many cases, a series of crimes are conditionally categorised as computer crimes, although they basically represent a form of so-called classic crimes only now computer systems and networks are included in their execution. This is the case when one uses the Internet to run, for example, a pyramid scam (Ponzi scheme), or to find customers for illegal activities associated with prostitution, illegal betting, etc. All these actions are illegal in most national legislations and can be executed without the use of computer systems and networks. In this context the term "computer" is not a necessary element of the substantial definition of the crime, it is only one way to carry out the illegal activities. In fact, computer systems and networks give criminals new ways to carry out the classic forms of crimes; therefore, in these cases the same legal provisions can be used to sanction such cases when a crime is committed with or without a computer. However, some crimes are necessarily connected with the invention of the computer and establishment of the Internet as a global network, and therefore bring up the need for a clear definition of computer crimes as a necessary condition for the creation of legal provisions that penalize such behaviour.

Hence the only possible solution is that the definition for the computer crimes should be based on four main pillars:[5]

1) Unlawful conduct that constitutes a breach or violation of important individual and social goods that the law provides criminal sanction for,

2) Specific manner, means and purpose of the crime - the use of computer systems and networks,

3) The special object of protection - the safety of computer systems and networks, streaming of stored computer data as a whole or a particular section,

4) The objective of the perpetrator to obtain unlawful gain (tangible or intangible) or to cause harm to others.

Given this, we define computer crimes as any illegal conduct which violates important individual and social goods; is executed or in connection with the computer system or networks, and directed against the security of computer systems and the data processed by them including such crimes as illegal possession, offering and/or distribution of information through a computer system or network, committed in order for the perpetrator himself or for others to obtain unlawful gains or to cause someone harm.

COUNCIL OF EUROPE

Although we believe that this kind of comprehensive definition of computer crime meets the basic theoretical and practical needs related to the efficient suppression of computer crimes, still, due to the rapid evolution of emergent forms of crimes that belong in this group we consider that it is necessary as a correction to use an approach based on enumeration list of groups of similar and homogeneous crimes that fit in the group of computer crimes.

On the other hand, primarily due to the phenomenological picture of computer crimes as a group of crimes due to its inherent features almost necessarily incorporate international element, there is unquestionably a need for complementary existence of international instruments which will appear as a kind of focal point of international efforts to prevent this type of crimes. The result of such efforts to internationalize the action to prevent computer crime was the adoption of the Council of Europe's Convention on Cybercrime.[6]

The Convention on Cybercrime is an international treaty that seeks to harmonize national laws on cybercrime, improve national capabilities for investigating such crimes, and increase cooperation on investigations. The Convention was drafted by the Council of Europe (COE) in Strasbourg, France. In addition to COE Member states, Canada, Japan, South Africa, and the United States participated in the negotiation of the Convention as observers[7] and later, signed and ratified the Convention, raising the total number of 53 countries that signed the Convention and 44 countries that have ratified it.[8]

The origins of the Convention date back to November 1996, when the European Committee on Crime Problems (CDPC) recommended that the COE set up an expert committee on cybercrime.[9] From the

5 I. Marcella, Albert J. II. Greenfield, Robert, Cyber Forensics, CRC Press, 2005, p. 48

6 The adequacy of the Convention of the Council of Europe as a global instrument and the need and the possibility of adopting a "global" Convention see more in Harley, B., A Global Convention on Cybercrime?, The Columbia Science and Law Review, 2010

7 Vatis, M.A., The Council of Europe Convention on Cybercrime, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.html

8 Status as of: 12/2/2015, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

9 See Convention on Cybercrime, Explanatory Report, p. 7.

beginning, the CDPC recognized that "the trans-border character of cyber-space offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."[10] Accordingly, the CDPC opined then, "a concerted international effort is needed to deal with such crimes", and "only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena."[11]

Following the CDPC's advice, the COE Committee of Ministers, in February 1997, established "the Committee of Experts on Crime in Cyber-space." The Committee of Experts' role was to examine the following subjects and to draft a "binding legal instrument" addressing them[12]:

- cyber-space offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions, offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors;
- other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation such as definitions, sanctions and responsibility of the actors in cyber-space, including Internet service providers;
- the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. interception of telecommunications and electronic surveillance of information networks, e.g. via the Internet, search and seizure in information-processing systems (including Internet sites), rendering illegal material inaccessible and requiring service providers to comply with special obligations, taking into account the problems caused by particular measures of information security, e.g. encryption;
- the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (*locus delicti*) and which law should accordingly apply, including the problem of *non bis in idem* in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts; and
- questions of international co-operation in the investigation of cyber-space offences.

The Committee of Experts negotiated and drafted the text of the Convention (and its Explanatory Report) over the next four years, culminating in the final draft that was approved by the CDPC in June 2001 and then adopted by the COE's Committee of Ministers on November 8, 2001, and after ratification of 5 countries, including 3 COE member states, it came into force in July 2004. On November 7, 2002, the Committee of Ministers adopted the Additional Protocol to the Convention on Cybercrime. The Additional Protocol requires ratifying Member States to pass laws criminalizing "acts of racist or xenophobic nature committed through computer networks." This includes the dissemination of racist or xenophobic material, the making of racist or xenophobic threats or insults, and the denial of the Holocaust and other genocides. It also commits ratifying nations to extend to these crimes the investigative capabilities and procedures created pursuant to the main Convention.

Provisionally, the Convention can be viewed as a document consisting of three parts and the Preamble. The first part upholds the substantive definitions of cybercrime offences that member countries are supposed to adopt; the second part is reserved for the investigative procedures that are required and the third part is dedicated for mechanisms aimed at bolstering international cooperation at fighting cybercrimes.

In the Preamble, the Convention states its goals that arise from the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation. In it, member states, conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks and concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks, state their determinations to resolve this situation by facilitating detection, investigation and prosecution of computer related crimes at both the domestic and international levels by adoption of powers sufficient for effectively suppressing such criminal offences and by providing arrangements for fast and reliable international co-operation.

In the first part, as previously mentioned, the Convention stipulates the substantive definitions of criminal offences that form the generic term computer crime. In this direction, the Convention, at first differentiates four major groups of computer crimes, comprised of:

- Offences against the confidentiality, integrity and availability of computer data and systems
- Computer-related offences
- Content-related offences

10 See Convention on Cybercrime, Explanatory Report, p. 8.
11 Ibid, p. 9
12 Ibid., p.10

- Offences related to infringements of copyright and related rights
- The first group of offences incorporates the following types of crimes:
- Illegal access (to the whole or any part of a computer system)
- Illegal interception (made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data)
- Data interference (damaging, deletion, deterioration, alteration or suppression of computer data)
- System interference (serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data)
- Misuse of a device which incorporates the production, sale, procurement for use, import, distribution or otherwise making available of a device or a item, including a computer program, designed or adapted primarily for the purpose of committing any of the offences mentioned before; a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the mentioned crimes.

The second group of offences consist of the computer-related forgery and computer-related fraud, where the third group of offences, the content-related offences, are consisted of the crimes related to child pornography (producing, offering or making available, distributing or transmitting, procuring and possessing).

The fourth group of computer of offences is connected with the protection of copyright and related rights and is consisted of crimes committed by infringement of the aforementioned rights.

Also in the first part of the Convention provisions are found aimed at answering the open questions about substantive criminal law institutes like, attempt and aiding or abetting and corporate liability and provisions concerning sanctions and measures as may be necessary to ensure that the criminal offences are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

The second part of the Convention turns its focus on establishing such investigative procedures that are adequate for accomplishing the purpose of specific criminal investigations or proceedings in the case of criminal offences established in accordance this Convention, other criminal offences committed by means of a computer system and the collection of any evidence in electronic form of a criminal offence. In this part, the Convention also provides safeguards when the usage of such investigative procedures is in collision with the adequate protection of human rights and liberties, including rights arising pursuant to obligations undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments. The safeguards provide, inter alia, for the principle of proportionality in provisioning of investigative procedures, judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

Having in mind these restrictions, the Convention stipulates the following investigative procedures and powers:

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order to submit specified computer data which is stored in a computer system or a computer-data storage medium and a subscriber information in service provider's possession or control
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data

Concerning the last part, international co-operation, the Convention, in accordance with the provisions of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, regulates the extradition and mutual assistance as a form of international cooperation.[13] The Convention is predominantly specific about regulating mutual assistance and its emerging forms and applicable procedures like sharing spontaneous information, mutual assistance regarding provisional measures, mutual assistance regarding investigative powers, procedures pertaining to mutual assistance requests, confidentiality and limitation on use, etc.

13 More about newest trends in international cooperation in criminal mater, especially concerning republic of Macedonia, see Buzarovska L. G., Mickovski N., International cooperation in criminal matters in the Republic of Macedonia, Proceedings of International Conference Rule of Law and Democracy, Law faculty, State University of Tetovo

When it comes to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, the purpose of this amendment was to expand the scope of the Convention to cover the criminalisation of the dissemination of racist and xenophobic material through computer networks. Hence the Convention discerns four types of such crimes: offences (directed against computer systems and their content); computer-related crimes (computer system is instrument); intellectual property crimes; and content-related crimes (computer system is the environment of the crime), and dissemination of racist and xenophobic expressions fits in the latter category.[14]

The Protocol concentrates on conduct that relates to the electronic environment of computer systems and networks. The protocol defines four independent offences, but the Articles are preceded by a definition of what is called 'racist and xenophobic material'. In the next articles either this material is the object of the criminalised conduct or elements of the definition are used to qualify conduct or circumstances. Thus, Art. 3 criminalises the distributing or otherwise making available to the public through a computer system of material as defined by the additional Protocol. Art. 4 deals with racist- and xenophobia-motivated threats against individuals or groups of individuals. The threat must involve the commission of a serious crime and it is left to the implementing Party to define a serious crime.

Art. 5 deals with racist- and xenophobia-motivated insults through a computer system. Within the frame of this article, insulting denotes causing prejudice to the honour or dignity of a person. The expression therefore needs to be offensive, contemptuous or invective.

Art. 6 deals with the denial or gross minimisation of acts of genocide or crimes against humanity as defined in the relevant UN-instruments. This behaviour is assumed to be deeply insulting to victims, their relatives or other survivors of such crimes. State Parties that included such a provision in their law do not yet refer to the general notions of genocide or crimes against humanity but to the holocaust. Given the fact that genocide and crimes against humanity motivated by racism and xenophobia have and are being committed after W.W. II, the provision therefore was given a more general structure.

As a last remark on the Protocol: according to Article 7 of the Protocol, State Parties can include the intentional aiding and abetting to the crimes defined in article 3-6; namely, individual member states may determine that attempts to commit one of the offences is also punishable, thus, service providers may be liable for the hosting of criminal content if they would intentionally aid or abet the crime.[15]

THE CASE OF THE REPUBLIC OF MACEDONIA

Having in mind the threat to national security and to the security of everyday life of ordinary people and their numerous interactions and transactions, and influenced by international obligation accepted and accumulated by accession to international instruments whose field of regulation are the efforts to combat computer related crimes, the Republic of Macedonia in its Criminal Code[16] (CC) starting from its original form has a numerous provisions concerning sanctioning of computer crimes. Also, the Law on Criminal Procedure[17] (LCP) holds a number of provisions concerning handling digital evidence and special investigative techniques and procedures when computer crime is involved.

The interesting thing about both legislations is that there is a clear evolutionary line in the prospect of achieving more comprehensive coverage of the different phenomenological forms in which computer related crimes can be manifested and to answer the ever evolving structure of this type of offences.

What as a general assessment can be drawn on the legal scope of computer crimes in the Macedonian criminal law is that it is an approach which for now means a maximum legal provisions for the possible forms of this type of criminal behaviour, but also relatively timely adjustment of the provisions to match the rapidly evolving and fluctuating phenomenological picture of computer related offences.

To say simply, the legislator in the Criminal Code, at least for now, provides a wide range of provisions intended to legally cover current forms of computer crime. On the other hand there is visible tendency of the legislator through relatively frequent changes of existing and prediction of new provisions to keep up with rapid changes in the emergent forms of computer crime, thus offering an effective legal framework, which is certainly a necessary condition in effective suppression of this type of offences.

This situation can be easily illustrated with the fact that the original legal solution in terms of provisions for computer offences was only limited to unauthorized access and damage to the computer system, and

14 .Kaspersen, Henrik W.K, Cyber Racism and the Council of Europe's reply, Computer/Law Institute, Vrije Universiteit Amsterdam the Netherlands, p.7

15 Ibid, p. 9

16 Official gazette of Republic of Macedonia, No. 37/96, 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 115/14, 132/14 and 160/14)

17 Official gazette of Republic of Macedonia, No. 150/2010 и 100/2012

later through continuous renewal and introduction of new legislation in effort to reach the present situation of almost maximum coverage of all possible aspects of computer crime. In this way, we can classify the Macedonian CC as a modern, appropriate and effective legal basis which adequately meets the challenges of the preventive and repressive suppression of cybercrime.

The CC, even in Article 122, which contains the meaning of the terms used in the text, with the primary goal of providing clear definitions of certain terms in order to avoid certain vagueness and ambiguity about their exact meaning, a computer system is defined as any device or group of interconnected devices that one or more of them performs automatic data processing according to a program; while computer data is defined as presentation of facts, information or concepts in a form suitable for processing by a computer system, including programs such as operating systems that put computer system into operation.

As regards the basic forms of computer crime, the Code envisages three offences: Article 251 - Damage and unauthorized access into computer system, Article 251a - Creating and infiltrating computer viruses and Article 251b - Computer fraud.

Article 251 - Damage and unauthorized access into computer system, represents a "classical" form of computer offence which is found in criminal codes of almost all countries in the world. From the substantial definition of the crime it becomes clearly visible that the intention of the legislator is to sanction the unauthorised malicious intrusions in someone else's computers, i.e. those unauthorized intrusions aimed to damage and/or use of the data or programs to which access is gained with the purpose of making illegal profit.

With this legal approach of the normative determination of the scope of the crime unfortunately remains uncovered part of the so-called "benign" unauthorized intrusions into computer systems and networks, i.e. the situation when offenders attempt or carry out unlawful access in order to demonstrate their ability to perform this intrusion, for fun, boredom and curiosity. Unfortunately this youthful "games" often occur as a starting point for much heavier similar offenses, so that one can only regret the lost opportunity for potential preventive effect of sanctioning this type of unauthorized intrusion into a computer system/network.

However, it must be admitted that this legal definition of unauthorized intrusion and attack on a computer system/network is a legal provision that the relatively adequately sanction common (in frequency and damages) intrusions and attacks, and by using of extensive descriptions legislator attempts to cover most of the existing and possible future forms of unauthorized intrusion and damage to computer systems and networks.

In this sense the legislator further continues and as a severe form of the offence envisages unauthorized intrusion and damage to the computer system, data or programs that are protected by special measures of protection or used in the operation of state entities, public enterprises and public institutions or international communications or participation in an organized group created to perform such acts, but as a separate form of this offence sanctions unauthorized manufacture, acquisition, sale, possession or making available other special devices, tools, computer programs or computer data intended or suitable for damaging or gaining unauthorized access into another computer system.

Correspondingly, Article 149, starting primarily from the significance and the impact of IT infrastructure in contemporary social trends, stipulates sanctioning of unauthorized access into a computer information system containing personal data wherein the perpetrator strives, using the accessed data for himself or for others, to achieve a benefit or to inflict some damage.

Similar motivational background rests behind the legal solution in Article 251-a, creation and infiltration of computer viruses. But in this case, unlike in the case of unauthorized intrusion and damage, legislator's normative scope moves ahead by sanctioning even the creation of computer virus with the intention of infiltrating into another's computer or computer network (paragraph 1), not only the use of a computer virus that will cause actual damage to someone else's computer system, data or program (paragraph 2). This normative approach clearly demonstrates the intention of the legislator to legally cover real life situations in which the ordinary user has the largest "chance" to appear in the role of victims of computer crime - the misuses of malicious computer programs specifically designed to damage the program and/or mechanical part of computer systems or their regular functioning.

Although the legislator uses only the term "computer virus" in the legal definition, that in real life situations is manly used for only a portion of malicious computer programs, hence, legally the term should be interpreted in the broadest sense, or as a term that in despite of the importance of the viruses covers and other types of malicious computer programs such as worms and Trojan horses (Trojans).

The legislator in paragraph 3 of this Article as an aggravated form outlaws the case when the use of malicious computer program caused severe damage and the last paragraph of this Article criminalises the attempted use of a computer virus.

Third primary cybercrime that the Macedonian Criminal Code criminalizes is the offense under Article 251-B Computer fraud. In the substantial definition of this offence the act of committing this crime is defined as the act of the perpetrator who, with intent to obtain unlawful gains for himself or for others by entering into a computer system untrue information data, not registering the factual data, changing, deleting or concealing the computer data, falsification of electronic signature or otherwise causing false results from the electronic processing and transmission of data.

From the chosen way of defining the substantial definition of this offence it is evident that an attempt has been made by the legislature to incriminate a wide range of ways of committing this crime, which of course is aimed as an adequate response to a potentially rich modus operandi of the perpetrators of this crime.

On this occasion must be emphasized the separate legal provision that sanction the unauthorized manufacture, acquisition, sale, possession or making available of special devices, tools, computer programs or computer data intended for perpetrating computer fraud, for which the legislator provides fine or imprisonment up to one year.

Also in the group of basic forms of computer crimes that Macedonian CC has provisions for is the offence from Article 149-a, Preventing access to public information system. Defined as unauthorized action preventing or limiting other access to public information system, the offence is directed primarily to legally sanction the so-called DoS attacks, which mainly represent automated indirect attacks aimed at overloading the victim's network servers with requests and as a result of that servers actually become unusable for legitimate users.

Besides these basic forms of computer offences, Macedonian legislator imposes a series of computer crimes that are directly related to computer systems and networks, whether their role is limited to instrumentum operandi or the target of the criminal act.

Thus, in Article 147, which penalizes the violation of the secrecy of correspondence and other consignments, as a guarantee of confidentiality of communication, in paragraph 1, in the ways of carrying out this offence, the Code provides for the violation of the confidentiality of the secured e-mail, which stipulates fine or imprisonment for up to 6 months.

The role of computer systems as an auxiliary tool in the production or distribution of child pornography Criminal Code of the Republic of Macedonia sanctioned as aggravated circumstance around the main provision under Article 193-A, Production and distribution of child pornography. Namely, if the production, distribution or otherwise making available child pornography, or if its supply or possession is done through a computer system or other means of mass communication, the Code stipulates for the perpetrator to be sentenced to imprisonment of at least eight years.

Possession and use of computer systems, components and programs is an aggravating circumstance in the case of Article 271, Making, acquisition or sale of counterfeit money. In this Article, in paragraph 2 criminal liability is stipulated for unauthorized persons who manufactures, purchases, hold, sell or use instruments, tools, computer programs and other safety components which serve to protect against counterfeiting, as well as means of unauthorized acquisition of bank data for making counterfeit money or masking the real money or other payment instruments, securities or false payment cards.

Article 379-a incriminates situations of creating the so-called computer forgery or criminal responsibility of the person with the intention of using them as genuine without authorization develops, introduces, amends, deletes or makes unusable computer data or programs that are specific or adequate to serve as evidence of facts which have value for the legal relations. The same paragraph provides responsibility for the person who uses such data or programs as genuine and shall be punished by a fine or imprisonment up to three years.

If such work or computer forgery is committed against the computer data or programs used in the operation of state entities, public institutions, companies or other legal entities and individuals who are working in the public interest or in the legal traffic abroad or if their use has caused significant damage, shall be punished with imprisonment of one to five years.

In connection with the logistical basis and tools for the creation of computer forgery, the law provides for liability of the person that manufactures, sells, keeps or makes them available to others: special devices, tools, computer programs or computer data intended or suitable to perform the computer forgery.

In addition to these legally regulated offences that are belonging in the narrow sense of to the group of computer crime, the Macedonian CC has provisions for several criminal acts that are only conditionally placed in this group. Mainly, in this group we place offences that are related to the creation and use of false credit cards. The first offence is unauthorized manufacture, acquisition, holding, selling or giving for usage instruments, articles, computer programs and other components for security or protection which serve to protect against counterfeiting as well as tools for unauthorized gathering bank data for making forged payment cards in addition to their encasing on banking devices in order for making forged payment cards or their usage in any other way in order to obtain data from a real bank payment cards and data for holders

of such cards. This legal provision primarily regulates the misuse of devices for collection and the misuse of electronic data from credit cards. Such devices are also known as skimmers and they contain dedicated prepared part of which is built-in camera to capture PIN codes and additional part "data reader" from the magnetic tape, which also mounts on the ATM.

Also sanctioned is manufacture itself, acquisition and use of false credit card and other ways of obtaining data from a real bank payment cards and data for holders of these cards in order to use them for fabrication and use of forged payment card or such collected data is given to someone else with such intention.

Finally, as the latest amendment to the Code provides criminal liability for misuse of computer systems as a medium for the dissemination of racist and xenophobic material. Namely, it incriminates the usage of computer system to spread racist and xenophobic written material, picture or other representation of an idea or theory that helps, promotes or incites hatred, discrimination or violence against any person or group on the basis of race, colour, national or ethnic origin, or religious beliefs in public. For this offence the legislator provides imprisonment of one to five years, and if the offense is committed with abuse of power or authority or this offence provokes riots and violence against people or property damage to a large extent, the provisioned prison sentence is one to ten years.

According to this legal structure and substantial definitions of computer crime in the Criminal Code and its role in standardization of conditions and content of the right of the state to impose criminal sanctions on the perpetrators of criminal acts on the one hand, and on the other hand given the role of criminal procedural law to define the conditions and actions for the implementation of substantive criminal law, or the necessity of complementary and functional unity of the two legal disciplines in achieving the goals of the criminal policy, imposes the need for separate procedural solutions that arise in the role of the necessary preconditions to the correct, fair and full implementation of the norms of substantive law.

Without going into this point in to the details of the particularity of detection, prosecution and proving the computer crimes but we will address several specific solutions that are included in the new Macedonian Law on Criminal Procedure[18], and have a direct impact in the offences from the scope of computer crime.

Thus with Article 184 of the new LCP, in the part referring to the procedural rules regarding measures for finding and securing persons and objects, to be more precise concerning the provisions on the search of the homes, the LCP regulates the procedure for performing a search of a computer system and computer data. Regarding it, the legislator firstly in Article 181 paragraph 2, stipulates that the search of the computer system is to be done only with the prior existence of a written and reasoned court order (warrant), obtained at the request of the public prosecutor, and in cases where it is likely to delay the proceedings, at the request of the judicial police. Hence, Article 184 stipulates the obligation of the person using the computer or having access to it or to another device or data carrier to allow access to them and to provide the necessary information to the enforcement agent of the aforementioned court order to guarantee the smooth achieve the goal of the search.

Also, in paragraph 2 of this article is provided for the duty of the person - the user of the computer system, or the person who has access to it or to another device or data carrier, to immediately take measures to prevent the destruction or alteration of data. From this solution is evident intention of the legislator, at least legally, to regulate the preservation of key information with potentially unstable character like the data stored in the so called RAM (Random Access Memory).

The sanction for failing to respond to the mentioned legal provisions for the person using the computer or have access to it or to another device or data carrier is provided as a fine of 200 to 1,200 euros, with the possibility that the amount may increase tenfold if, despite the imposed fine, the person still does not act on the court order.

The Criminal Procedure Code contains provisions that address the specifics of temporary seizure of computer data. It is the data stored in the computer and similar devices for automated or electronic data processing, devices which are used for collection and transmission of data, data carriers and subscriber information available to the service provider and data that according to the Criminal Code must be seized or which may serve as evidence in criminal proceedings. Seized data is given for storage to the public prosecutor or authority designated by a special law or otherwise provides their storage. The judge of the previous procedure on the proposal of the public prosecutor with special decision can determine protection and storage of computer data until it is needed, at a maximum of six months. After this period, the data will

18 The new Macedonian LPC establishes a new type of procedure, which is based on principles set out in the Strategy for the reform of criminal law, such as the expansion of the application of the principle of opportunity in crime persecution, extrajudicial settlements, plea bargaining and simplified procedures. Also, the new LCP is based on making distance from the judicial paternalism and placing the burden of proof on the interested parties; providing an active and leading role of public prosecution in the pre-trial proceedings with effective control of police; abolition of the judicial investigation, providing major role in the investigation for the public prosecutor; introduction of the preclusion of certain procedural actions and measures against the abuse of procedural powers by the parties; strict deadlines; rationalization of the system of legal remedies; implementation of the recommendations of the European Union and the Council of Europe on the criminal proceedings; creating more efficient public prosecution through the establishment of a new operative management bodies as well as leadership and cooperation with the police and other agencies involved in law enforcement

be returned, unless if that data is involved in committing the following crimes: Damage and unauthorized access into a computer system under Article 251, Computer Fraud under Article 251-B and Computer forgery under Article 379. Also, seized data won't be returned if the data is included in the commission of another (different) criminal act committed with the help of a computer or if it serves as evidence of a crime.

As for the practical application of this legal framework for incrimination of computer crime, as illustrative, both in terms of numbers and dynamics, and in terms of efficiency in tackling, we present the results of Skopje Basic Public Prosecution Office regarding Unauthorized access into a computer system under Article 251 of the Criminal Code of the Republic of Macedonia which is probably the most typical offence for computer crimes.

Volume of cases that were brought before the Basic Public Prosecution Office – Skopje, concerning Art. 251 of the Criminal Code of the Republic of Macedonia

Year	2010	2011	2012	2013
Total criminal charges	10	7	12	10
Request for additional information to Ministry of interior	1			
Indictment	3	2	4	3
Rejected criminal charges	2	1	4	4
Waiver of prosecution			2	
Investigation	2	1		3
Termination of investigation	1			
Verdict	1 (probation)	3 (probation)	2 (probation) 1 fine 1 imprisonment	4 (probation) 2 imprisonment

It is visible from the presented table that the relative stability of the number of criminal charges for which acted Skopje public Prosecution Office, and the relatively small size of the incidence of such crime in the overall operation of this prosecution. Also, from the relatively large number of dropped charges, the obvious conclusion is relatively low quality and reliability of the charges, which is an indication of the need for intensive training of competent authorities for better handling in dealing with this type of crimes. However, one of the arguments justifying this low number of criminal charges for computer crimes lies in the fact that a great number of the cases are basically criminal acts with a foreign element and were solved using the institutes of international legal assistance and cooperation.

Another obvious fact of this relatively modest research on the dynamics and the prevalence of cybercrime are relatively mild judicial penalties that the convicted perpetrators of this crime received, which is partly explained by the relative youth of the perpetrators and the fact that in almost all cases they were first time offenders and previously had absolutely no conflicts with criminal or tort law, but on the contrary, were considered promising and valued members of the community.

CONCLUSION

Cybercrime is one of the newest and one of the most dangerous forms with greatest potential to threaten the quality of human life and safety. One of its features is that it carries and practically demonstrates potentially devastating effects primarily due to our vulnerability arising from our reliance on the use of digital devices in everyday life and communication.

Hence the question of finding appropriate and effective ways to deal with this threat stands out as a priority. The first step in this direction is the establishment of adequate legislative basis that will outline the legal limits of possible responses to the threat of computer crime. In the process of establishing such a legislative solution it must be taken into account that, on one side, the legal basis must be wide enough to cover all potential forms of computer crime (which in itself is a challenge mainly because of extremely rich

phenomenological picture of this type of crime), and on the other side to be flexible enough to cover new forms of computer crimes that appear every day. Finally this legislative framework must be balanced in such a way so as not to limit the legitimate use of computer and network technology in everyday stations.

On the other hand, it is important to work on the internationalization of efforts to deal with this kind of offences primarily because of its international nature. Partial approach is doomed to failure from start. The European Convention together with the Additional Protocol is the first, but insufficient step, yet it traces the possible solutions for the establishment of unified universal approach in dealing with computer crime. In places an emphasis on a comprehensive approach, which incorporates substantial definitions of computer offences and procedural prerequisites for the prosecution of these cases accompanied by the principles and conditions that determine the international assistance and cooperation in dealing with the computer criminal acts.

The case of the Republic of Macedonia is representative of relatively firmly set legal basis for prosecution of computer related offences. Substantive legislation is packed with a wide range of incriminations that include most forms of computer crime, and it is in accordance with the requirements of the European Convention. On the other hand, frequent changes of criminal legislation enabling timely innovation and customization of incriminations contained in the Criminal Code allow this relatively comprehensive system to adequately respond to the new challenges. What is missing is a greater staffing and greater competence of the involved actors to deal with these crimes which would enable timely detection, clarification, proving and crime prevention.

REFERENCES

1. Buzarovska L. G., Mickovski N., International cooperation in criminal matters in the Republic of Macedonia, Proceedings of International Conference Rule of Law and Democracy, Law faculty, State University of Tetovo
2. David R. Johnson &David G. Post, *Law and Borders-The Rise of Law in Cyberspace,* 48 STAN. L. REv. 1367 (1996)
3. Desante Anthony F., *Evidentiary Consideration for Collecting and Examining Hard- Drive Media,* The George Washington University, 28.11. 2001, Forensic Sciences 262
4. I. Marcella, Albert J. II. Greenfield, Robert, Cyber Forensics, CRC Press
5. Icove, D., Segar, K., and VonStorch, W., *Computer Crime, A Crimefighter's Handbook,* O'Reilly & Associates, 1999
6. Harley, B., A Global Convention on Cybercrime?, The Columbia Science and law Review, 2010
7. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors,* 66 U. CIN. L. REv. 177, 179 (1997).
8. Kaspersen, Henrik W.K, Cyber Racism and the Council of Europe's reply, Computer/Law Institute, Vrije Universiteit Amsterdam the Netherlands
9. Krsul I, *Authorship Analysis: Identifying the Author of a Program,* Department of Computer Sciences, Purdue University, M.S. Thesis, CSDTR-94-030, 1994.
10. Pettinari Dave, *Handling Digital Evidence from Seizure to Court Presentation*, IOCE conference, June 2000
11. Pollit Mark M., *Report on Digital Evidence,* (FBI CART report, DC Washington, USA), Interpol Forensic Science Symposium, Lyon, France, 16-19.10.2001
12. Rosenblatt, K. S., High Technology Crime — Investigating Cases Involving Computers, KSK Publications, San Jose, CA, 1995.
13. Schnider L. D., Scene of the cybercrime, Syngress Publishing, 2002,
14. Vatis, M.A., The Council of Europe Convention on Cybercrime, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/catalog/12997.html
15. Weber, Amalie M., The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal, Volume 18 | Issue 1, January, 2003
16. Whitcomb C. M., *A Historical perspective of Digital Evidence*: *A Forensic Scientists View,* International Journal of Digital Evidence, 2002, vol.1, issue 1.

UDC: 004.738.5.056

PRIVACY ENHANCING TECHNOLOGIES

Brankica M. Popovic[1]
The Academy of Criminalistic and Police Studies, Belgrade
Milos Bandjur[2]
Djoko Bandjur[3]
University of Priština, Faculty of Technical Sciences, Kosovska Mitrovica

Abstract: Concept of privacy involves, but is not limited to, cultural, social, legal, political, economic and technical aspects, and although recognized as a fundamental human right, has never been more endangered than today due to the proliferation and advancement of innovative information and communication technologies (ICT). ICTs have become so essential to the modern society that they are taken for granted, without full awareness and understanding of new problems and risks they introduce. They are providing unseen possibilities to collect, store, process and distribute personal data, with recognized issues relating to privacy vs. security, free expression vs. censorship, intellectual property and alike. One solution to privacy problems is the adoption of appropriate privacy enhancing technologies (PET) which constitute a wide array of technical means including, but not limited to, encryption, policy, filtering and anonymity tools. They, on the one hand, can assist data controllers' compliance with data protection principles, and on the other hand provide individuals a control over personal information (how and when these information will be disclosed to and used by third parties), especially on the Internet. This is essential since the available information about a person can be cross-referenced and used for many purposes, lawful and not. The aim of this paper is to give an insight to recent developments of different PET solutions and their acceptances among the Internet users.

Keywords: Privacy, Security, Internet, Privacy Enhancing Technologies PET.

INTRODUCTION

> '*There are many unique challenges we face in this age of information. They stem from the nature of information itself.... The ethical issues involved are many and varied, however, it is helpful to focus on just four. These may be summarized by means of an acronym* **PAPA. P***rivacy: What information about one's self or one's associations must a person reveal to others, under what conditions and with what safeguards?* **A***ccuracy: Who is responsible for the authenticity, fidelity and accuracy of information?* **P***roperty: Who owns information?* **A***ccessibility: What information does a person or an organization have a right or a privilege to obtain, under what conditions and with what safeguards? ... Two forces threaten our privacy. One is the growth of information technology, with its enhanced capacity for surveillance, communication, computation, storage, and retrieval. A second, and more insidious threat, is the increased value of information in decision-making. Information is increasingly valuable to policy makers; they covet it even if acquiring it invades another's privacy*' (Mason, 1986).

Although written back in 1986, the subject is even more in focus today with striking remark that after so many years we are no closer to finding an adequate response to those questions. It seems that the development of modern technology further emphasized the scale of the problem and challenges faced by society during their deployment. Modern society relies on almost unlimited access to information (from anywhere at any time) and is virtually dependent on the use of the Internet and modern technologies in a network environment (for gathering, storage, retrieval and dissemination/transmission of information). This access to information, unfortunately, comes with a considerable risk since it is enabled to everyone (criminals, terrorists, industrial competitors and government agencies as well), or even injustice denied, irrespective of their actual intentions (Britz, 1996; Verizon White Paper, 2010; Young, 2011).

1 brankica.popovic@kpa.edu.rs
2 milos.bandjur@yahoo.com
3 djoko.bandjur@pr.ac.rs

Thus, modern technologies introduce new problems that previously did not exist, which, despite of increased data security threats, are often related to the moral principles (e.g. the dilemmas of privacy vs. security, freedom of expression vs. censorship, intellectual property and alike) (Popovic, Banđur & Raičević 2014). For example, the main privacy and confidentiality concerns in Cloud Computing is the possibility to disclose private information (accidentally or deliberately), or use them for unauthorized purposes. Ethical and legal issues related to privacy issues are especially emphasized in the case of large-scale data analysis (data mining, big data analytics) and processing of information obtained from sensor networks and other distributed data sources (including social media). All available information about a person can be cross-referenced, and the resulting dossier (so called *dossier effect*) ends up being used for many purposes, lawful and not (Goldberg, Wagner & Brewer, 1997). Privacy on social networking sites can be undermined by many factors: from disclosing of personal information by users themselves, to more frequently network management practices to incorporate location aware services and use personal information for consumer tracking and behavioural marketing through data mining (Michael & Miller, 2013). And although it seems like a great idea to share our activities with our friends, making the sensitive information like locations public is potentially dangerous. The "PleaseRobMe.com" website, for example, collects information about when people are away based on public status information and can be used by burglars to pick their victims.[4] Not to mention arising privacy concerns about possible fusion of social media data with biometric data and traditional surveillance techniques. Moreover, our Internet activity is not only monitored, but is also archived in a way that can never be forgotten or erased, regardless of our wishes.

All these are challenges with no adequate response yet, and should be seriously dealt with before the application of modern technology (non-selective and without precise regulation) make every effort to ensure information security and the protection of individual privacy pointless. One of the possible solutions is the development and utilization of privacy enhancing technologies (PET), which will be further discussed in the following sections, as well as the concept of privacy itself.

CONCEPT OF PRIVACY

Despite its importance, the concept of privacy is difficult to fully describe since it is a truly multi-dimensional notion which involves, but is not limited to, cultural, social, legal, political, economic and technical aspects. Since privacy has been studied for decades, many different definitions of privacy have been proposed.[5] One of them was proposed by the Council of Europe Parliamentary Assembly[6] in 1970:

'The right to privacy consists essentially in the right to live one's own life with a minimum of interference. It contains private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially. Those who, by their own actions, have encouraged indiscreet revelations about which they complain later on cannot avail themselves of the right to privacy'.

When talking about personal data, according to the EU Data Protection Law (EU, 2014):

- Data are personal data if they relate to an identified or at least identifiable person, the data subject.
- A person is identifiable if additional information can be obtained without unreasonable effort, allowing the identification of the data subject.
- Data are anonymised if they no longer contain any identifiers; they are pseudonymised if the identifiers are encrypted.
- In contrast to anonymised data, pseudonymised data are personal data.

In the context of modern (ICT) technology utilization, it is also important to understand what Personally Identifiable Information (PII) refers to. It is 'information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.'[7]

There are a number of Privacy laws and regulations, dealing with organizational and technical requirements for ensuring personal data protection. The most used super-national guidelines are the European Union privacy-related directives (EU, 1995, 2002), privacy guidelines of the Organization of Economic Co-Operation and Development (OECD, 1980), Association for Computing Machinery (ACM) Recom-

4 The Register. Burglars used social network status updates to select victims, 2010. http://www.theregister.co.uk/2010/09/13/social_network_burglary_gang/

5 http://www.privileged.group.shef.ac.uk/projstages/stage1/introduction/definitioncounter/

6 Council of Europe, Parliamentary Assembly, Resolution 428 of 23 Jan 1970 http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta70/ERES428.htm

7 US General Services Administration: Rules and Policies - Protecting PII - Privacy Act. http://www.gsa.gov/portal/content/104256

mendations on Privacy (USACM, 2006) and Federal Trade Commission Reports and Principles (FTC, 2000).

According to them, a core set of privacy principles can be summarized as (Wang, 2009):

1) Notice/Awareness (upon collection) (USACM, 2006)
2) Data minimization (USACM, 2006)
3) Purpose specification (OECD, 1980)
4) Collection limitation (OECD, 1980)
5) Use limitation (OECD, 1980)
6) Onward transfer (EU, 1995; FTC, 2000)
7) Choice/Consent. The two widely adopted mechanisms are (FTC, 2000): Opt-in and Opt-out
8) Access/Participation. An individual should have right to: know whether a data controller has data relating to her (OECD, 1980), inspect and make corrections to her stored data (USACM, 2006)
9) Integrity/accuracy (USACM, 2006)
10) Security (OECD, 1980)
11) Enforcement/Redress (FTC, 2000).

Wang also summarized anonymity-related principles are as: '*Anonymity* (means that users cannot be identified nor be tracked online); *Pseudonymity* (also means that users cannot be identified, but they can still be tracked using a so called alias or persona); *Unobservability* (a data controller cannot recognize that a system/website is being used or visited by a given user); *Unlinkability* (a data controller cannot link two interaction steps of the same user) and *Deniability* (means that users are able to deny some of their characteristics or actions and that others cannot verify the veracity of this claim)' (Wang, 2009).

In the context of information systems, the growing importance of **privacy by design** is recognized. The goal of privacy by design is to take privacy requirements into account from the conception of a new IT system up to its realisation, suggesting that privacy protection is a system requirement that must be treated like any other functional requirement (Hoepman, 2013). Regarding this, the International Organisation for Standardisation (ISO) issued the ISO 29100 Privacy framework[8] which collects organisational, technical and procedural aspects of privacy protection, with the intention to enhance the existing security standards. Also, the proposal for a new European data protection regulation explicitly requires data protection by design (EU, 2012).

With understanding how significant privacy is, there is no surprise that the idea of development of privacy enhancing technologies is widely adopted giving a rise to numerous project and researches in that area.[9] The suitability of the different PET options primarily depends on the characteristics of the information system, the required level of protection and the sensitivity of the personal data concerned (KPMG, 2004).

PRIVACY ENHANCING TECHNOLOGIES

"Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system." (Blarkom, Borking & Verhaar, 2003)

This definition was later adopted by the European Commission (COM, 2007), suggesting that privacy enhancing technologies are slightly more high-level than those that are typically studied.

In order to help individuals to protect their personal information, a wide range of PET are developed (ICAEW, 2011), with a number of published PET reviews (Goldberg et. al., 1997, Goldberg, 2002, 2007; Blarkom et. al., 2003; Wang, 2009). With the aim to prevent identification and protect unlawful processing of personal data, PETs are based on:

- tools to help individuals to manage their personal information and are therefore focused on transparency and control; and
- tools intended to prevent other to collect other people's personal information including:
- anonymity or pseudoanomity products that remove an individual's identity from the rest of the data;
- encryption tools that prevents unauthorized parties to access information
- filters and blockers that prevent third parties from reaching the individual and devices for wiping records and traces which can be traced

8 ISO/IEC 29100. Information technology – Security techniques – Privacy framework. Technical report, ISO JTC 1/SC 27
9 European Union EU. MEMO/07/159: Privacy enhancing technologies (PETs), Brussels, 2 May 2007

Having that in mind we can say that different PET implementation offers different functionalities which can be grouped in four main types (KPMG, 2004):

1) General PET controls - relatively simple to implement and are most widely accepted (e.g. encryption and logical access security controls);
2) Separations of data - identifying personal data are detached from the other personal data through utilization of identity protector;
3) Privacy management systems - systems that can ensure automated enforcement of the privacy policy, and
4) Anonymisation of personal data involves software that does not register the identifying personal data at all, or destroys it as soon as the data is no longer required – preferably immediately after collection and verification.

In the following sections, the following major privacy-enhancing technologies: privacy management systems, authentication and identity management, authorization and access control and anonymity techniques, will be briefly described. Additionally the necessary utilization of encryption tools is emphasized.

PRIVACY MANAGEMENT SYSTEMS

Privacy management systems are systems that can ensure automated enforcement of the privacy policy.[10] Privacy policies enable users (and other entities) to specify how they would like their personal data to be treated by other parties while limiting access to unauthorised persons. These policies can be taken into account before disclosure of PII, and can direct the way in which PII is treated (Shen & Pearson, 2011).

Privacy policy languages are intended to be machine-readable and can be roughly divided into two types: external policy languages and internal ones. The first one describes website public privacy policies or users privacy preferences, and is declarative without enforcement mechanism (e.g. - *P3P*[11], *APPEL*[12], *XPref*[13]) (Cranor et.al, 2002, 2006, Agrawal et.al, 2003). One of the most widely used, P3P,[14] for example contains the following information:

- who collects, processes and stores the data;
- what data are collected and the reason for their processing;
- whether there are *opt-in* and *opt-out* alternatives;
- whom the data are supplied to;
- which data the responsible person has access to;
- the default storage period for the relevant personal data;
- how conflicts about the privacy policies of the processing organisation are resolved or settled, and
- where the privacy policy can be found on the website.

Internal policy languages, on the other hand, specify internal rules for privacy practices of company or website, and are normative with support for enforcement (e.g. *EPAL-Enterprise Privacy Authorization Language*[15]). There has been a great deal of work done on defining access control privacy polices (Platform for Enterprise Privacy Practices (E-P3P), trust management policies, RBAC - role based access control privacy policies, privacy access control in shared social networks etc.) (Shen, 2011).

To summarize, the use of policy tools is in the following: users declare their privacy policy on their browsers, websites register their policy with security agencies, the website policy is compared with user policy and the browser makes automated decisions. The obvious benefit is that they might help in uncovering privacy gaps for websites, block cookies or prevent access to some sites. Today they are built into many web browsers, but not all websites have policy tools.

10 A higher degree of integration of data and software that, in fact, forms a shell around the Personally Identifiable Information (PII) and that automatically tests all transactions involving these data against the privacy regulations
11 The **P**latform for **P**rivacy **P**references - P3P
12 APPEL - *A P3P Preference Exchange Language* was designed to complement P3P by allowing users to express their privacy preferences in terms of rules that specify certain conditions under which user information may be collected and used
13 XPref is preference language for P3P which outweighs APPEL in that it can specify what is acceptable as well as what is unacceptable, and combinations of both
14 http://www.w3.org/P3P/
15 A formal language developed by IBM and ZeroKnowledge that allows enterprises to write their internal privacy policies, so that those can be enforced across IT applications and systems in an automated manner.

AUTHENTICATION AND IDENTITY MANAGEMENT

Authentication aim is to ensure that a user is actually the person who she/he claims to be. Authentication is performed by something user knows (username in combination with a password, PIN...), has (identity token e.g., a bank ATM card) or is (biometrics). Additionally, the combinations of two or even three factors can be used to strengthen authentication. A digital identity[16] is an online or networked identity adopted or claimed in cyberspace by an individual, organization or electronic device. These users may also project more than one digital identity through multiple communities.

Identity management deals with the authentication of the individuals and controlling access to resources in a system. PETs associated with identity management aim to perform authentication with minimum identity disclosure, thus providing protection against identity theft. This is different to anonymity since some PII and even sensitive information may be revealed in order to have access to wanted resource. There are different researches and projects focusing on privacy issues for identity management (e.g. EU funded PRIME[17], FIDIS[18], PrimeLife[19]).

One of the goals of the emerging identity management systems is to allow users to have more than one digital identity and be able to freely choose which identity to use. PET incorporated systems use Identity Protectors to divide systems into identity, pseudo-identity and anonymity domains. There are several major approaches in this area (e.g. Kantara initiative[20], OpenID[21] authentication, etc.).

AUTHORIZATION AND ACCESS CONTROL

Authorization involves granting or denying specific access rights. It can be achieved via an access matrix,[22] roles[23] or directories[24] (Wang, 2009). From a privacy point of view, PETs for identity management should provide (or need to be able to provide) authentication and authorisation without identification. One way to separate *authorization* from *authentication* is to use private credentials. They allow users to prove that they are authorized to access a certain service or gain a certain benefit (a proof of entitlement), by providing only the necessary PII, while revealing no unnecessary personal information such as their identities (Shen, 2011).

Authorization schemes allow much more privacy-friendly mechanisms for solving a variety of problems, since it can be anonymous or pseudonymous. For example, both IBM's 'Idemix' and Microsoft's 'u-prove' are privacy enhancing technologies implementing the (implicit) design pattern *anonymous credentials* (Hoepman, 2013).

ANONYMITY TECHNIQUES

Anonymity, as 'the quality or state of being unknown or unacknowledged',[25] is privacy of identity providing that user cannot be identified (connected with their offline identities) nor tracked online. It is a reasonable request from users concerned about political or economic retribution, harassment, or even threats to their lives.[26] Instead of using their true names to communicate, users choose to speak using pseudonyms (assumed names or 'nym') or anonymously (no name at all). The main difference is in linkability: with a nym, one may send a number of messages that are all linked together but cannot be linked to the sender's true name; by using one-time anonymity for each message, none of the messages can be linked to each other or to the user's physical identity.[27] Both, in certain contexts, can be provided by PETs (Shen, 2011).

16 http://www.techopedia.com/definition/23915/digital-identity
17 https://www.prime-project.eu/
18 http://www.fidis.net/
19 http://www.primelife.eu/
20 https://kantarainitiative.org/
21 Current version is OpenID Connect. More on http://openid.net/
22 In classic access control model it specifies what permissions each subject has on the resources the system retains.
23 In a role based access control model, permissions are assigned to roles instead of subjects directly (subjects can take on multiple roles, and multiple subjects can take on the same role).
24 In a directory-based access control model, subjects are managed and organized in directories (e.g., in an LDAP server), and permissions are granted based on these different directories.
25 http://www.thefreedictionary.com/anonymity
26 https://www.eff.org/issues/anonymity
27 More can be found in a link containing a list of selected papers regarding anonymity: http://freehaven.net/anonbib/full/date.html

Several different anonymous communication techniques have been used:

- trusted infomediaries that remove PII, (e.g. 'strip identifying headers and resend' approach which has been used in anonymous email remailers and anonymous web browsing tools like Anonymizer[28]),
- mix networks to obfuscate the source of a communication (e.g. 'onion routing'),
- addition of additional traffic or data to make the 'real' data more difficult to mine, etc.

All of them are supposed to hide the correlation between input and output data in order to protect the identity of the data subject.

Email anonymity and pseudonymity systems

The oldest and simplest email anonymity systems - type-0 remailers[29] were developed back in 1990s. They worked in a way that a user sends email to the remailer, which strips off the user's identifying information and re-mails the message to its intended recipient. The remailer assigns a random pseudonym to the sender and keeps a master list matching those pseudonyms to real email addresses, allowing messages replies to the original sender. Since then, there have been three newer classes of remailers. The *type-I*, or *cypherpunk remailers* were developed in order to better protect the privacy of email users. Some of improvements included: *chaining,*[30] *encryption*[31]and *mixing*[32] but in order to use this type of remailers, users had to have sophistication technical skills. Still some vulnerability remained, which were addressed in *type-II* or *Mixmaster remailers*. For the deployment of this type of remailer users need specially customized software in order to send anonymous mail. *Type-III* or *Mixminion remailers* improve privacy protection in a number of ways and have several new features to prevent different forms of attack, and to aid in the management of the network (Danezis, Dingledine, Hopwood & Mathewson, 2003).

Internet browsing anonymity

There have been a number of systems that have been implemented to provide anonymity to users of interactive Internet applications.

Anonymizer, as the global leader in online privacy and anonymity (18-year history), allows the consumers and organizations to remain safe, secure, and anonymous each time they go online. Anonymizer Universal's[33] personal VPN routes all of users' Internet traffic through an encrypted tunnel to Anonymizer's secure and hardened servers, and then masks users' real IP address to ensure complete and continuous anonymity online. This system is supposed to be incapable of tracking online activities, viewing or keeping logs of users' website activities.[34] It is user friendly, requiring absolutely no technical knowledge to install and use. Tool like this is almost a must, when using public Wi-Fi networks which are often unsecured and therefore a natural target of eavesdroppers and criminals. It is also a great help in data theft protection.

Onion Routing, originally the US Naval Research Lab's[35] project was developed in 1996. It is an infrastructure for private communication over a public network, providing anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. Onion Routing operates by dynamically building anonymous connections within a network of real-time Onion Routing Proxy servers (mixes). An application, instead of making a (socket) connection directly to a destination machine, makes a socket connection to a mix node which builds an anonymous connection through several other mix nodes to the destination. A message or packet is encrypted to each mix node using public key cryptography where the resulting encryption is like a layered 'onion' with the original message in the innermost layer. As the message traverse over the network, each mix node strips off its own layer of encryption to reveal where to send the message next. Each mix can only identify adjacent one along the route (Syverson, Reed & Goldschlag, 2000). This layering occurs in the reverse order for data moving back to the initiator. When the connection is broken, all information about the connection is cleared at each mix node. Unless all mix nodes are compromised, intractability can be achieved. Access to an onion routing network can be configured in a variety of ways depending on the needs, policies, and facilities of those connecting. A few modifications

28 A web proxy that strips off identifying headers and source addresses from the web browser
29 The best known being anon.penet.fi.
30 A message is sent through a chain of remailers
31 When first remailer decrypts an encrypted message it receives, only the address of the second remailer and another encrypted message is found. The first remailer sends that message to the second remailer, which decrypts it to find the address of the third remailer and another encrypted message and so on. Finally, only the last remailer decrypts message and sends it to the final recipient.
32 Incoming messages to any remailer are batched together and randomly reordered before being sent out.
33 https://anonymizer.com/anonymizer_universal.html
34 Erases cookies and log files, pop-up blocker, kills Spyware, unlisted IP
35 http://www.onion-router.net/

of the described concept were proposed until 2002, when Tor, a second generation of Onion Routing was introduced.

Tor[36], is the most successful (in terms of number of users) interactive anonymity tool to date. In order to address the limitations in the original Onion routing design, Tor adds perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points (Shen, 2011). Tor nodes are run by volunteers and all of the software is free and open-source. In addition to protecting the users of TCP/IP-based Internet services, Tor also contains a facility to protect *providers* of such services. The most common such *hidden services* are web servers; a user runs a web server somewhere in the world which is only accessible through Tor which protects the identities of both the user and the provider of the service. In this way, Tor provides a *censorship-resistant publishing* service, which has been used by whistleblowers,[37] to distribute information of public importance (Goldberg, 2007). Although a formal proof of security for the Tor authentication protocol was presented in 2006 (Weis, 2006), a recent development when some servers used for illegal activities were found and shut down put that fact in question.[38]

Freenet[39] is decentralized, censorship-resistant distributed data store which aims to provide freedom of speech through a peer-to-peer network with strong protection of anonymity. Freenet works by pooling the contributed bandwidth and storage space of member computers to allow users to anonymously publish or retrieve various kinds of information. If used in 'darknet' mode, where users only connect to their friends, it is very difficult to detect. Communications by Freenet nodes are encrypted and are routed through other nodes to make it extremely difficult to determine who is requesting the information and what its content is.

The **Invisible Internet Project** (I2P)[40] is an anonymous network, exposing a simple layer that applications can use to anonymously and securely send messages to each other. It is similar to Tor, with primary difference related to the out-proxy design. While Tor takes the directory-based approach, providing a centralized point to manage the overall 'view' of the network as well as gather and report statistics, opposed to it I2P's proposes distributed network database and peer selection.

ENCRYPTION TOOLS UTILIZATION

Today, *Encryption Tools,* although not sufficient by themselves, are necessary for privacy protection. They are seen as a security tool to prevent unauthorized access to communications, files, and computers with downside that both parties need to use the same software. Their importance in establishing anonymous connection was already described in Onion Routing/Tor case. Also the role in securing data in cloud storage is considered as irreplaceable. Below, some other well known PETs based on encryption tools will be described.

TLS/SSL: At this point we have to point out the role of secure protocols in enhancing privacy on the Internet. Secure Sockets Layer (SSL) was a protocol proposed by Netscape in the mid-1990s, meant for protecting HTTP (web) connections, general, and could be used to protect any TCP-based connection. SSL went through a few revisions, and was eventually standardized into the protocol known as Transport Layer Security (TLS). TLS/SSL is the single most widely used PET to date. Their success stems from the fact that every major web browser comes with support for these technologies built right in and that their use is largely invisible to the user. That is, no special installation or configuration needs to be done by end users before they can benefit from these technologies. A web browser will automatically encrypt web requests when communicating with a TLS/SSL web server, and the server will automatically encrypt its responses; no user intervention is needed at all.

However, the discovery that the United States National Security Agency (NSA), for the purposes of espionage activities, intentionally[41] incorporated vulnerability in a widely used encryption algorithm (Elliptic Curve Dual Deterministic Random Bit Generation Dual DRBG EC) approved by NIST[42] greatly disturbed the public leaving them clueless to what extent is the US government willing to go in their attempt to have control over people.[43]

36 The name is an acronym derived from the original software project name **T**he **O**nion **R**outer, thttps://www.torproject.org/
37 E.g. Wikileaks project
38 See 'Anonymity is dead and other lessons from the Silk Road trial' http://www.engadget.com/2015/02/08/silk-road-trial-lessons/ and https://blog.torproject.org/blog/tor-and-silk-road-takedown
39 https://freenetproject.org/whatis.html
40 https://geti2p.net/en/about/intro
41 Perlroth N, Larson J and Shane S. 'N.S.A. Able to Foil Basic Safeguards of Privacy on Web', September 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=1&
42 National Institute of Standards and Technology, which establishes the standards for data protection in all devices that are used in government agencies
43 Lily Hay Newman, Can You Trust NIST? Revelations that the NSA undermined the U.S. standards agency leave cryptographers feeling queasy, 9 Oct 2013, http://spectrum.ieee.org/telecom/security/can-you-trust-nist/?utm_source=techalert&utm_medium=e-

Another, well known email privacy enhancing tool is **Pretty Good Privacy** (PGP).[44] Beside many other features, its fundamental purpose is to encrypt and/or digitally sign email (and to decrypt it and verify the signatures at the other end, of course). Today, many email programs, have incorporated PGP support, greatly improving its ease of use.

Off-the-Record Messaging (OTR)[45] is a technology that allows users to have private conversations over instant messaging by communicating in an encrypted and authenticated manner. OTR provides: *confidentiality* (with encryption no one else can read your instant messages), *authentication* (you are assured the correspondent is who you think it is), *perfect forward secrecy* (if you lose control of your private keys, no previous conversation is compromised), *deniability* (the messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured the messages he sees are authentic and unmodified). There are three ways that users can integrate OTR into their instant messaging: by using a proxy, by using a plugin or to have OTR functionality built directly in to the user's client (the best option, since, like SSL/TLS, the user does not have to install or configure anything special in order to gain some benefit from OTR).

CONCLUSION

In the above sections we tried to put a light to a number of PETs that are available or are being developed. Today, both citizens and organizations are interested in deploying PETs. Citizens rely on PETs to protect themselves from predators in online ambient and organizations see them as a help to meet their legal and regulatory responsibilities.

Although effective, PETs cannot resolve all privacy concerns, mostly due to the lack of regulatory powers and lack of user awareness of privacy risks. Not to mention rapid development of new technologies introducing new privacy threats. Nevertheless, a great deal of researches in PET area, give some promising solutions to the complex privacy requirements in a global (online) environment. Their utilization is in focus of some regulations with aim not only to be some sort of recommendation, but rather an obligation in a form of law and other legal documents.

ACKNOWLEDGEMENTS

This paper is the result of the research on the project 'Forensic methods in criminalistics', which is financed by the Academy of Criminalistic and Police Studies. The work was partly supported by a grant from the Ministry of Education and Science, Republic of Serbia [Project number TR34019].

REFERENCES

1. Agrawal, R., Kiernan, J., Srikant, R. & Xu, Y. (2003). An XPath-based Preference Language for P3P. *In proceedings of the 12th Int'l World Wide Web Conference*, Budapest, Hungary, pp. 629 - 639.
2. Blarkom, G. W. v., Borking, J. J. & Verhaar, P. (2003). PET. In G. W. v. Blarkom, J. J. Borking & J. G. E. Olk (Eds.), *Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents*: College bescherming persoonsgegevens. The Hague, The Netherlands, chapter 3, pages 33–54.
3. Britz, J.J. (1996). Technology as a Threat to Privacy: Ethical Challenges and Guidelines for the Information Professionals. *Microcomputers for Information Management*, 13(3-4): 175-93.
4. COM (2007) Communication COM 228 from the Commission to the European Parliament and the Council. *On Promoting Data Protection by Privacy Enhancing Technologies (PETs),* May 2nd 2007.
5. Cranor, L., Langheinrich, M. & Marchiori, M. (2002). *A P3P Preference Exchange Language 1.0 (APPEL1.0)*: W3C Working Draft 15 April 2002.
6. Cranor, L. et al. (2006). *The Platform for Privacy Preferences 1.1 (P3P1.1) Specification*. W3C Working Group Note 13 November 2006, http://www.w3.org/TR/P3P11/
7. Danezis, G., Dingledine, R., Hopwood, D. & Mathewson, N. (2003). Mixminion: Design of a Type III Anonymous Remailer Protocol. *In Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pp.2-15.

mail&utm_campaign=101013
44 http://www.pgpi.org/
45 https://otr.cypherpunks.ca/

8. EU. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ C L*, 281:0031 – 0050, November 23 1995

9. EU. (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ L* 201, July 31 2002

10. EU. (2012). Proposal for a Regulation of the European Parliament and of the Council. On the protection of individuals with regard to the processing of personal data and on the free movement of such data. *OJ C*, 102:24, April 5 2012.

11. EU. (2014).European Union Agency for Fundamental Rights. *Handbook on European data protection law*, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

12. FTC. (2000). Federal Trade Commission. *Privacy online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*, http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission

13. Goldberg, I., Wagner, D., & Brewer, E. (1997). Privacy-Enhancing Technologies for the Internet. *In proceedings of the 42nd IEEE COMPCON San Jose, CA*, pp-103-109, http://www.cypherpunks.ca/~iang/pubs/privacy-compcon97.pdf

14. Goldberg, I. (2002). Privacy-Enhancing Technologies for the Internet, II: Five Years Later. *Lecture Notes in Computer Science* 2482:1-12, http://freehaven.net/anonbib/papers/petfive.pdf

15. Goldberg, I. (2007). Privacy Enhancing Technologies for the Internet III: Ten Years Later, in Acquisiti A., Gritzalis S., Lambrinoudakis C.& Vimercati S. Eds, *Digital Privacy: Theory, Technologies, and Practices*, Chapter 1, pp. 3-18, http://www.cypherpunks.ca/~iang/pubs/pet3.pdf

16. Hoepman JH. (2013). Privacy Design Strategies, arXiv preprint:1210.6621v2, 6th May 2013, http://arxiv.org/pdf/1210.6621v2.pdf

17. ICAEW (2011): *Building trust in the digital age: rethinking privacy, property and security, making information systems work initiative,* http://www.icaew.com/~/media/archive/files/technical/information-technology/business-systems- and-software-selection/making-information-systems-work/building-trust-in-the-digital-age-report.pdf

18. KPMG (2004). *Privacy- enhancing technologies, White paper for decision-makers*. Duch Ministry of the Interior and Kindgom Relations, the Netherlands, DIIOS, December 2004. http://is.muni.cz/el/1433/podzim2005/PV080/um/PrivacyEnhancingTechnologies_KPMGstudy.pdf?lang=en

19. Mason, RO. (1986). Four Ethical Issues of the Information Age. *Management Information Systems Quarterly*, 10(1), http://www.gdrc.org/info-design/4-ethics.html

20. Michael, K. & Miller, W. (2013). Big Data: New Opportunities and New Challenges. *Computer*, 46(6), pp. 22-24.

21. OECD. (1980). Organization of Economic Co-Operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

22. Popović, B., Banđur, M. & Raičević, A. (2014). Security challenges of modern technologies utilization. *In thematic conference proceedings of international significance, 'Archibald Reiss Days'*, Belgrade, 3-4 march 2014, pp. 95-105.

23. Shen Y. & Pearson S. (2011), *Privacy Enhancing Technologies: A Review*, HP Laboratories, HPL-2011-113, 6 August, 2011, http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf

24. Syverson P.F., Reed M.G., Goldschlag D.M. (2000). Onion Routing Access Configurations. *In DISCEX 2000: Proceedings of the DARPA Information Survivability Conference and Exposition*, Hilton Head, SC, IEEE CS Press, 2000, pp.34-40, http://www.onion-router.net/Publications/DISCEX-2000.pdf

25. USACM. (2006). USACM Policy Recommendations on Privacy. http://usacm.acm.org/privsec/category.cfm?cat=7&Privacy%20and%20Security

26. Verizon White Paper (2010): Security in the new information age: Striking a balance between risk and opportunity, http://www.verizonenterprise.com/resources/whitepapers/wp_security-in-the-new-information-age_en_xg.pdf

27. Wang, Y. (2009). Privacy-Enhancing Technologies. In Gupta, M. & Sharman, R. (Eds.) *Handbook of Research on Social and Organizational Liabilities in Information Security,* Hershey, pp. 203-227, doi:10.4018/978-1-60566-132-2.ch013, http://www.cs.cmu.edu/afs/cs/Web/People/yangwan1/papers/2008-Handbook-LiabSec-AuthorCopy.pdf

28. Weis S.A. (2006). Privacy-Enhancing Technologies, *IEEE Securitye&Privacy*, pp.59, http://pascal.computer.org/csdl/mags/sp/2006/05/j5059.pdf

29. Young, M.D. (2011). Electronic surveillance in an era of modern technology and evolving threats to national security. *The Free Library (January,1)*, http://www.thefreelibrary.com/Electronic surveillance in an era of modern technology and evolving...-a0261729763

UDC: 343.53:004
343.98:004.9
343.98:004.832

THE IMPORTANCE OF DATA MINING TECHNOLOGIES AND THE ROLE OF INTELLIGENT AGENTS IN CYBERCRIME

Kristijan Kuk
The Academy of Criminology and Police Studies, Belgrade
Ahmet Mehic
University of Paderborn, Heinz Nixdorf Institute
Stefan Kartunov
Technical University of Gabrovo, Faculty of Mechanical and Precision Engineering

Abstract: Social networking sites are online venues where members can create and post content to profiles (i.e., lists of demographic information and personal interests constructed by completing forms within the site) and can form personal networks that connect them to others using tools embedded in the social software. Electronic surveillance or e-surveillance can be defined as system investigation or motion monitoring / communication of one or more persons on the Internet, aiming to gather information on them, their activities and inter-connection. Police analysis of data gathered by intelligent agents (software robot - bot) could be successfully exploited in the field of the cybercrime. Factors that help in evaluation of the application relevance of data mining techniques in crime combat fluctuate within the range of activities data collection resulted from, to their quality (degree of uncertainty, accuracy and completeness). This paper will be most useful to behavioral researchers who wish to use social Web to unobtrusively study text data on the Internet for the purpose of crime combat. This paper describes the use of social media that can be used productively in behavioral research on the Internet.

Keyword: cybercrime; crime data mining; intelligent agents; personal data collection techniques.

INTRODUCTION

Every day, news providers broadcast events happening all over the world (mostly in forms of text, some in forms of photo or video) on the Web; Millions of internet users share their opinions and experience by posting to blogs or microblogs (e.g., Twitter). The abundance of information has become more overwhelming than ever, which also brought up research opportunities to analyze and discover patterns within the large scale data sets. Although these online text data are free-form text, they also carry spatial and temporal footprints.

Digital communities not only bring people closer together but also, inadvertently, provide criminals with new ways to access potential victims online. Digital personas play a key role in criminal tactics in online social media. One criminal may hide behind multiple digital personas or a single persona may be shared by a criminal group when engaging with potential victims. Examples of such criminal exploitation of digital personas include [1]:

- Child sex offenders masquerading as young persons to gain the trust of their victims. An offender may use multiple personas over the course of an interaction (introducing himself/herself as a young person and then introducing another persona, e.g., that of an older relative). Alternatively, a single persona may be shared by an offender group so that a victim is groomed by multiple people over a period of time [2].
- Romance scam operators using digital personas with appropriate age and gender to engage with multiple victims in online dating sites, gaining their trust and exploiting them for financial gain [3].
- Radicalisation of youth in online forums through persuasive messaging [4]. Multiple digital personas are used as a tactic at times. For instance, one persona is used to vigorously support a radical cause, followed by silence for a few days and then a different persona is used to claim that the original protagonist has left to fight for the cause.

As the Web has become an inseparable part of modern life, it has become the platform for large scale information exchange. Public user profile information is a common feature of modern websites. These profiles can provide a valuable resource for investigators tracing digital artefacts of crime. Users of the modern web are no longer visible only to the owners of the websites with which they interact. Web services do not

just collect information about users, they publicly reveal some portion of this information on a user's profile page within their website. Identifying details which could once be found on a web user's personal homepage are now replicated across a number of websites, and visibly linked to public logs of their activities on that site. An investigator aiming to searching for extra information in order to facilitate an arrest for online harassment, may find information items - attributes of greater value due to their ubiquity. The combination of usernames and linguistic fingerprints with temporal data and network graphs can be considered highly identifiable on a broad range of services [5]. Clear leaders in information content are Google and Facebook, as would be expected.

PROFILING CYBER CRIMINALS AND VICTIMS

The various analysis techniques discussed above combine to form a key feature of the toolkit – the ability to generate identity profiles of specific digital personas. The toolkit is able to automatically create profiles for a specified digital persona, drawing upon the conversations in which it has participated to produce an overall analysis of its online activity, language and identity characteristics. These profiles can provide investigators with additional intelligence about trends and characteristics not immediately apparent to the human eye. The generated profile is built from a number of elements, including:

a) Language usage. A model of the persona's language use within conversations highlighting characteristics such as people/place names, dates/times, frequently used words/phrases, aggressive/sexual content, email addresses/URLs, as well as non-dictionary words which may indicate an attempt at disguising what is being discussed or represent unique jargon used within that domain (of which an investigator may or may not be aware).

b) Age/Gender analysis. Utilising the decision tree to provide an inferred estimation of the age and gender of the person behind the persona. By default investigators are provided with a summary view which presents the strongest path through the tree, but they are also able to view the full tree allowing them to examine the decisions the toolkit made at all points should the certainty of the decision not be clear cut.

c) Online activity. An analysis of the persona's overall online activity, highlighting when it has appeared online within relevant conversations. This analysis can take many forms including indicating when a persona is most likely to be online over a 24 hour window and on which days during the week.

User model dimensions in case of cyber criminals

To define a user model for the domain of the Social Web, we first have to understand the demands of social web applications on user models. After collecting all the information (Figure 1), the first step is to determine the user model dimensions that our user model has to cover.

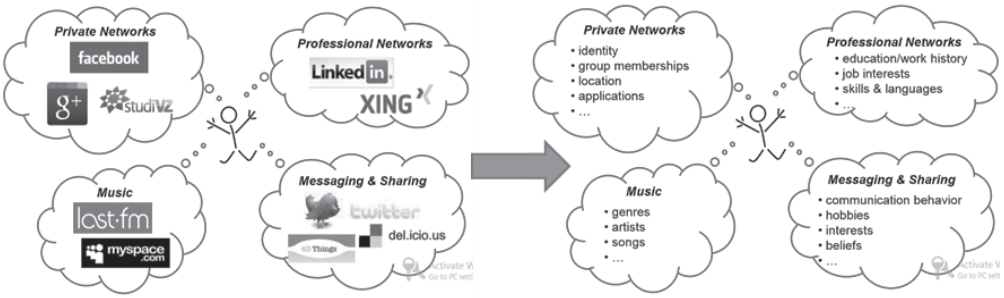


Figure 1 *Collecting data from social networking Web*

A lot of dimensions exist, but not all of them are required in the context of the Social Web. Several dimension are mentioned and discussed in the literature. Authors in work [6] present a consolidated taxonomy and build the basis for the selection of the dimensions needed for their model:

- *Personal Characteristics* (or Demographics) range from basic information like gender or age to more social ones like relationship status. – Interests and Preferences in an adaptive system usually describe the users interest in certain items. Items can be e.g. products, news or documents.
- *Needs and Goals*: When using computer systems, users usually have a goal they want to achieve. Such goals can be to satisfy an information need or to buy a product. The plan to reach such goals is for

example to support users by changing navigation paths or reducing the amount of information to a more relevant subset.

- *Mental and Physical State* describe individual characteristics of a user like physical limitations (ability to see, ability to walk, heartbeat, blood pressure, etc.) or mental states (under pressure, cognitive load).
- *Knowledge and Background* describe the users knowledge about a topic or system. It is used in educational systems to adapt the learning material to the knowledge of a student, display personalized help texts or tailor descriptions to the technical background of a user. The knowledge and background is a long-term attribute on the one hand but can differ and change from session to session depending on the topic. Knowledge and background about certain topics can increase or decrease over time [7].
- *User Behavior*: The observation and analysis of user behavior is usually a preliminary stage to infer information for one of the previous mentioned dimensions. It can also serve for direct adaptation like using interaction history to adapt the user interface to common usage patterns of the user.
- *Context*: In computer science context generally refers to ”any information that can be used to characterize the situation of an entity” [8], but the discussion about what context actually is, is still ongoing[5]. In the area of user modeling, the term context focuses on the user's environment (e.g. Location or Time, or devices the user interacts with) and human characteristics. Human characteristics describe Social Context, Personal Context and overlap with the Mental and Physical State dimension).
- *Individual Traits* refer to a broad range of user features that define the user as an individual. Such features can be user characteristics like introvert or extrovert or cognitive style and learning style.

User data collected by social network

In recent years, online social networks have gained great popularity amongst internet users. These networks serve different purposes and communities, for instance, socializing on Facebook or Google+, establishing professional networks in LinkedIn1 or communicate via short messages called “tweets”. Their popularity led to a huge amount of collected data, and, hence, attracts the interest for exploitation by commercial and non-commercial applications such as recommender applications. Since (1) users (2) are (3) often members of several social networks, integrated profiles from multiple networks are desired to achieve a comprehensive view on users, which would, for instance, increase the quality of personalized recommendations [9] in business intelligence (BI). In a recent report from BI Intelligence, we take a close look at the kinds of information each of the biggest social networks collects on its users, and how those data fit into the overall strategy of each network, shown in Figure 2.

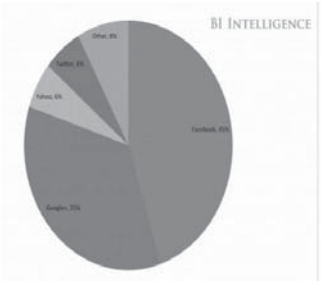


Figure 2 *Social network account credentials people use to login to other sites across the web*[1]

INTELLIGENT AGENTS AND USER DATA COLLECTED

Intelligent agents can be very useful in accomplishing the so-called e-surveillance. Electronic surveillance or e-surveillance can be defined as system investigation or motion monitoring / communication of one or more persons on the Internet, aiming to gather information on them, their activities and inter-connection. Independently, intelligent agents on the Internet (1) could conduct (2) search activities (3) very successfully on behalf of and for the needs of various users.

Due to the efficient gathering, manipulating and management of the data, this software could be of great interest from the intelligent data analysis point of view in various fields of the police forces activities. Police analysis of data gathered by intelligent agents (software robot - bot) could be successfully exploited

1 http://www.businessinsider.com/types-of-user-data-collected-by-social-networks-2014-7

in the field of the cybercrime. It is necessary to take a closer look into the existing techniques of artificial intelligence used for making a conclusion in intelligent agents in order to effectively utilised gathering and analysis of data from criminal activities.

Automated data collection on the Internet is nothing new, and scrapers continually access and repost data for other websites. This information is often highly valuable to the businesses that collect it, and they go to great lengths to protect it. Search engines, PageRank[2] and advertising all use bots to collect information stored by others. Web services can gather information from data hosts—websites that store or house target data—primarily by parsing or scraping data. Parsing generally refers to the collection of information from the data host directly[3]. Parsing accesses a website's underlying data structures through a series of formalized data requests, often through application programming interfaces ("APIs").

Computer vision APIs such as *Diffbot* must turn the web contents into your database. The article API[4] is used to extract clean article text and related data from news articles and blog posts. Retrieve complete text, normalized HTML, related images and videos, author, date, tags—all automatically, from any article on any site.

Extract schema information from instance data

User profile integration from multiple social networks is indispensable for gaining a comprehensive view on users. Although current social networks provide access to user profile data via dedicated APIs, they fail to provide accurate schema information, which aggravates the integration of user profiles, and not least the adaptation of applications in the face of schema evolution.

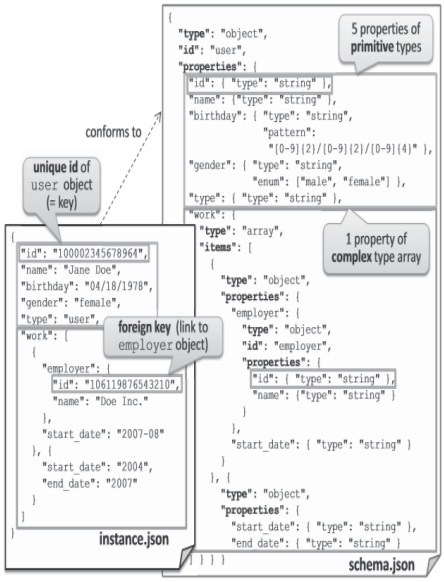


Figure 3 *JSON data and extracted JSON Schema*

However, up to now the systematic integration of the gathered data is hampered, because the underlying data stores of social networks are built with a focus on extension and flexibility, and thus, they often use the so-called *NOSQL* databases [10]. Such databases may store data in large tables without a traditional schema (e.g., HBase in Hadoop, used by Facebook and LinkedIn), or in schema-less multidimensional maps (e.g., Cassandra, used by Twitter). Since JSON (JavaScript Object Notation) is the leading format for data interchange supported by many APIs of social networks, we derive schema information expressed in the JSON schema language. In the data extraction phase), instance data is extracted from social networks through their corresponding APIs. These extracted data fragments are each expressed in a generic markup language Lx, i.e., JSON in the case of most social networks. To integrate user profiles from different social networks, the proposed process consists of four major phases [11]:

2 https://support.google.com/toolbar/answer/79837?hl=en
3 http://www.techopedia.com/definition/3853/parse
4 http://techcrunch.com/2013/07/31/diffbot-releases-product-pages-api-uses-robot-learning-to-supercharge-shopping-and-collecting-sites/

1) data extraction,

2) schema extraction,

3) transformation and

4) integration.

In the data extraction phase, instance data is extracted from social networks through their corresponding APIs. These extracted data fragments are each expressed in a generic markup language Lx, i.e., JSON in the case of most social networks. A short JSON example from a Facebook user is shown on the left hand side of Figure 3. The object of type user (as indicated by property type) provides information about the user's name (string value), birthday (string, possibly following a particular pattern), gender (string, possibly with restrictions concerning allowed values), and work experience (array of objects) [12]. Note that, in order to enable fine-grained access to user profile information guarded with authorization techniques, APIs require multiple requests to retrieve complementing data fragments (e.g., an additional request using the employer id would be needed to retrieve detailed employer information, which was not provided within the original response).

DATA MINING THEOLOGIES IN IDENTIFYING CRIME CHARACTERISTICS

Data mining essentially relies on several mathematical disciplines, include partially ordered sets, combinatorics, general topology, metric spaces, linear spaces and graph theory. A significant number of applications of these mathematical tools are included ranging from association rules, clustering algorithms, classification, data constraints, logical data analysis, etc. Many classic data mining techniques have been successful for crime analysis generally, such as association rule mining [13], classification [14], and clustering [15].

Data mining is defined as the discovery of interesting structure in data, where structure designates patterns, statistical or predictive models of the data, and relationships among parts of the data [16]. Data mining in the framework of crime and intelligence analysis for national security is still a young field. The following describes our applications of different techniques in crime data mining. Preprocessing has been used to keep the data set ready for the process. Entity extraction has been used to automatically identify person, address, vehicle, and personal properties from police narrative reports [17]. Clustering techniques have been used to cluster the city crime data mining depends on the crimes. Classification has been used to detect criminal data from the city crime data base. Social network analysis has been used to analyze criminals' roles and associations among entities in a criminal network [18].

Identifying crime characteristics is the first step for developing further analysis. The knowledge that is gained from data mining approaches is a very useful tool which can help and support police forces. A crime analysis should be able to identify crime patterns quickly and in an efficient manner for future crime pattern detection and action. Crime information that has to be stored and analyzed. Criminals often develop networks in which they form groups or teams to carry out various illegal activities.

Data mining task consisted of identifying subgroups and key members in such networks and then studying interaction patterns to develop effective strategies for disrupting the networks. Data is used with a concept to extract criminal relations from the incident summaries and create a likely network of suspects [19].

Graph mining

How can we localize the source of diffusion in a complex network? Because of the tremendous size of many real networks—such as the internet or the human social graph—it is usually unfeasible to observe the state of all nodes in a network. More recently, the controllability of complex networks was considered in [20], using appropriately selected driver nodes. A Portuguese researcher at the Ecole Polytechnique Federale de Lausanne (EPFL) has developed a mathematical system to identify the source of information circulating on a network[5], an epidemic or a terrorist attack. The researcher Petro Pinto developed a system "that could prove a valuable ally" for those who must conduct criminal investigations or seeking the origin of information on the Web. With this method, we can trace the source of all types of information flowing through a network and that by not listening to a small number of members. For example, when locating a spammer who is sending undesired emails over the internet, where it is clearly impossible to monitor all the nodes. Thus, the main difficulty is to develop tractable estimators that can be efficiently implemented (i.e., with subexponential complexity), and that perform well on multiple topologies.

5 http://www.semanticweb.rs/Article.aspx?iddoc=32&id=142&lang=2

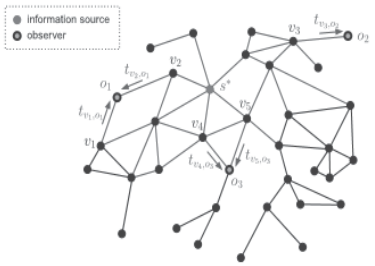


Figure 4 *An algorithm to trace the source of crimes on Internet*

Figure 4 show source estimation on an arbitrary graph $G\{V,E\}$, where the vertex set V has N nodes, and the edge set E has L edges. At the unknown time $t = t^*$, the information source $s^* \in G$ is the vertex that originates the information and initiates the diffusion. In this example, there are three observers, which measure from which neighbors and at what time they received the information. The goal is to estimate, from these observations, which node in G is the information source.

Similarity metric

Similarity metric is the basic measurement and used by a number of data mining algorithms. It measures the similarity or dissimilarity between two data objects which have one or multiple attributes. One of the major goals in criminology is the etiology (cause) of crime, because of this, criminologist studies are concerned with the relationship between two or more variables. Considering different data type with a number of attributes, it is important to use the appropriate similarity metric to well measure the proximity between two objects. Correlation for two binary variables will be identical to a Pearson correlation coefficient for two binary variables [21]. It is often used in recommender systems based on Collaborative Filtering - CF.

In general, collaborative filtering is a technique of suggesting particularly interesting items or patterns based on past evaluations of a large group of users. In a typical CF scenario, there is a list of m users $\{u_1, u_2, \cdots, u_m\}$ and a list of n items $\{i_1, i_2, \cdots, i_n\}$, and each user u_i has a list of items (i.e., Iu_i), which the user has rated, or about which their preferences have been inferred through their behaviors [22]. Generally speaking, the basic procedure of CF-based recommendation or prediction can be summarized in the following two steps [23]:

1) Look for users sharing the similar interests or rating patterns with a given user (called active user),
2) Use the information from those like-minded users found in step (1) to calculate a prediction for the active user. At present, Pearson correlation coefficient has been introduced for computing similarity between users or items according to the user-item data as in Figure 5, which is usually called user-item matrix. For two given users a and u, their similarity can be computed as follows.

$$Sim(a,u) = \frac{\sum_{i\in 1}\left(r_{a,i} - \bar{r_a}\right)\left(r_{u,i} - \bar{r_u}\right)}{\sqrt{\sum_{i\in 1}\left(r_{a,i} - \bar{r_a}\right)^2}\sqrt{\sum_{i\in 1}\left(r_{u,i} - \bar{r_u}\right)^2}}$$

where $I = I_a \cap I_u$ is the subset of items which both use a and u have invoked previously, $r_{a,i}$ is a vector of item i observed (or rated) by user a, and $\bar{r_a}$ and $\bar{r_u}$ represent average values of different items observed (or rated) by user a and u, respectively.

	Item1	Item2	Item3	Item4	...	Target	Pearson
Alice	5	3	4	1	...	?	
User1	3	1	2	5	...	5	-0.54
User2	4	3	3	3	...	2	0.68
User3	3	3	1	5	...	4	-0.72
User4	1	5	5	2	...	1	-0.02

<- User2 most similar to Alice

Figure 5 *Pearson correlation as similarity measure*

The prediction method based on two users' similarity is referred as user-based CF. Similarly, CF can also be conducted through the similarity computation between two items, that is, item-based CF. According to

the studies from other researchers, item-based CF can outperform user-based CF in most conditions, and has been treated as a preferred choice for prediction or recommendation problems. Similarity measures are an important factor which helps to find unsolved crimes in crime pattern.

*Crime-crime similarity*Authors Tong Wang et al. in work [24] propose a pattern detection algorithm called *Series Finder*, that grows a pattern of discovered crimes from within a database, starting from a "seed" of a few crimes. The pairwise similarity γ measures how similar crimes C_i and C_k are in a pattern set $\hat{P}$. Their model is in the following form:

$$\gamma_{\hat{p}}(C_i, C_k) = \frac{1}{\Gamma_{\hat{p}}} \sum_{j=1}^{J} \lambda_j \, \eta_{\hat{p},j} S_j(C_i, C_k)$$

where two types of coefficients are introduced:

1. λ_j – pattern-general weights. These weights consider the general importance of each attribute. They are trained on past patterns of crime that were previously labeled by crime analysts.

2. $\eta_{\hat{p},j}$ – pattern-specific weights. These weights capture characteristics of a specific pattern. All crimes in pattern $\hat{P}$ are used to decide $\eta_{\hat{p},j}$, and further, the defining characteristics of $\hat{P}$ are assigned higher values. Specifically:

$$\eta_{\hat{p},j} = \sum_{i=1}^{|\hat{p}|} \sum_{i=k}^{|\hat{p}|} S_j(C_i, C_k)$$

$\Gamma_{\hat{p}}$ is the normalizing factor $\Gamma_{\hat{p}} = \sum_{j=1}^{J} \lambda_j \, \eta_{\hat{p},j}$. Two crimes have a high γP^ if they are similar along attributes that are important specifically to that crime pattern, and generally to all patterns.

Text mining

Text mining is an interdisciplinary method used in different fields like machine learning, information retrieval, statistics, and computational linguistics. Web mining is a sub discipline of text mining used to mine the semi structured web data in form of web content mining, Web Structure mining and web usage mining. Opinion mining also called sentiment analysis is a process of finding users opinion about particular topic or a product or problem. Figure 6 has the hierarchy of data mining and the categories of how opinion mining is formed under the branch [25].

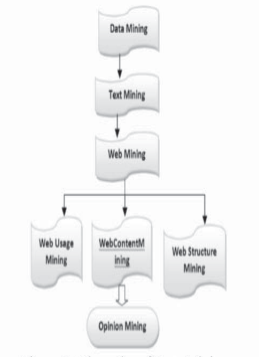


Figure 6 *Hierarchy of data mining*

Opinion mining

Opinion mining is the area of research that attempts to make automatic systems to determine human opinion from text written in natural language. It aims to extract opinions from information sources such as reviews and present them to the user in a user friendly manner [26]. Opinion mining draws on computational linguistic, information retrieval, text mining, natural language processing, machine learning, statistics and predictive analysis. Textual information in the world can be broadly classified into two main categories, facts and opinions. Facts are objective statements about entities and events in the world. Opin-

ions are subjective statements that reflect people's sentiments or perceptions about the entities and events. Much of the existing research on text information processing has been focused on mining and retrieval of factual information [27].

There are two significantly different models for representing emotions: the categorical model and the dimensional model. Each type of model helps to convey a unique aspect of human emotion and both of them can provide insight into how emotions are represented and interpreted within the human mind. A fundamental technology in many current opinion-mining and sentiment-analysis applications is classification. Categorical classification is the basis of the categorical model. Likewise, a dimensional model is the foundation of practical dimensional estimation. Categorical classification method utilises *WordNet-Affect* as a linguistic resource and vector space model for measuring the similarity between input text and emotion category. Dimension reduction methods enable hidden semantic meaning behind the text to become more evident in the categorical emotion classification. Dimensional estimation method also takes advantage of a lexical repository the Affective Norms for English Words – ANEW [28] (a set of normative emotional ratings for a collection of English words) but this method relies on the coordinates in the VAD space to find the closest emotion to input text.

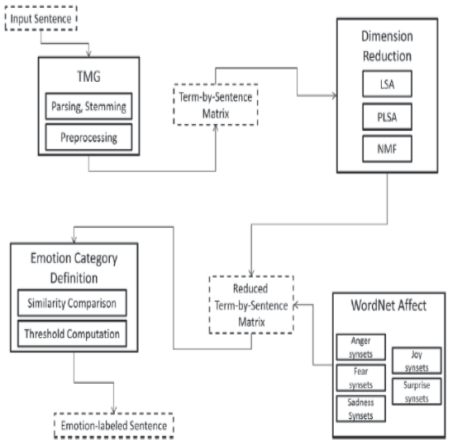


Figure 7 *A system flow overview of categorical classification*

Both methods go through pre-processing steps: stopwords listing and stemming. These steps help the significant linguistic components of text to be focused and considered by removing unimportant features. Most languages are full of structural words that provide little meaning to text. Figure 6 gives a system flow overview of categorical classification [29].

There are words such as "fear" and "cheerful" which refer directly to emotional states. These words are called direct affective words. On the other hand, indirect affective words have an indirect reference that depends on the context (e.g. "monster", "cry"). *WordNet-Affect* is an affective lexical resource that is essential for affective computing, computational humour, text analysis, etc. and it particularly has a lexical repository of direct affective words. *WordNet-Affect* is an extension of *WordNet* by means of selecting and labelling of synsets representing affective concepts. Besides, *WordNet-Affect* has an emotional hierarchy of affective domain labels with which the synsets representing affective concepts are annotated.

Sometimes, the blog users comment on each other. The identification of such overlapped comments on a given topic is crucial for detecting emotion. The module created of author Dipankar Das [30] aims to track a single user's comments on the same topic as well as on different topics to analyze the changes in emotion with respect to topic and time. Tracking of mass emotions on certain subject / topic / event over time will also be taken up in the proposed research.

CONCLUSION

Gathering of miscellaneous information on citizens and its distribution to corresponding databases represents reality of the modern society. Although, computer gathering, search and comparison is widely applied in the business administration and economy, it has not been sufficiently exploited in crime science and forensics so far. Regardless of its application purpose, automatic gathering, search and comparison of

data in the present time is based on the one hand on the application of software capable to independently gather information and on the other hand on the databases to accommodate certain gathered information.

On the Internet, an intelligent agent (or simply an agent) could be successfully exploited in the field of the cybercrime. A web browser intelligent - methods of artificial intelligence should be used in finding data in intelligent data analysis – data mining that widely applied in the fields of business administration, economy, mechanics, medicine, genetics, traffic and similar.

Factors that help in evaluation of the application relevance of data mining techniques in crime combat fluctuate within the range of activities data collection resulted from, to their quality (degree of uncertainty, accuracy and completeness). Researchers have developed a variety of automated data mining techniques – and for the purpose of crime combat, both in the field of local police affairs, and national level. Specific understanding of the relationship between analysis capabilities and characteristics of a particular type of criminal offence can be helpful to the investigators to apply these techniques more efficiently in order to identify trends and patterns, locate problem areas, and even anticipate criminal offense.

REFERENCES

1. Rashid, A., et al., Who Am I? Analyzing Digital Personas in Cybercrime Investigations. *Computer*, 2013. 46(4): p. 54-61.
2. Awais Rashid et al. *Technological Solutions to Offending*, pages 228–243. Willan, 2012.
3. M. T. Whitty and T. Buchanan. The online dating romance scam: A serious crime. *CyberPsychology, Behavior, and Social Networking*, 15(3):181–183, 2012.
4. Gabriel Weimann and Katharina Von Knop. *Applying the notion of noise to countering online terrorism. Studies in Conflict and Terrorism*, 31(10), 2008.
5. Edwards, M.J.; Rashid, A.; Rayson, P., "*A Service-Indepenent Model for Linking Online User Profile Information*" Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint , vol., no., pp.280,283, 24-26.
6. Plumbaum T, Wu S, De Luca EW, Albayrak S (2011), *User modeling for the social semantic web*. In: SPIM, pp 78–89.
7. Brusilovsky, P., Millan, E.: *User models for adaptive hypermedia and adaptive educational systems*. In: Brusilovsky, P., Kobsa, A., Nejdl, W. (eds.) The Adaptive Web: Methods and Strategies of Web Personalization, chap. 1, pp. 3–53. SpringerVerlag,Berlin Heidelberg New York (2007).
8. Dey, A.K.: Understanding and using context. *Personal and Ubiquitous Computing*, 5, 4–7 (2001).
9. M. Wischenbart, S. Mitsch, E. Kapsammer, A. Kusel, S. Lechner, B. Pröll, J. Schönböck, W. Schwinger, M. Wimmer:"*Automatic Data Transformation: Breaching the Walled Gardens of Social Network Platforms*";Vortrag: 9th Asia-Pacific Conference on Conceptual Modelling (APCMM 2013), Australia; 29.01.2013 - 01.02.2013; in:"Proceedings of the 9th Asia-Pacific Conference on Conceptual Modelling (APCMM 2013)", ACM (2013), 89 - 98.
10. Ito H, Potekhin M and Wenaus T 2012. *Development of noSQL data storage for the ATLAS PanDA Monitoring System,* CHEP 2012, New York, NY, May 2012.
11. Rahm, E., Do, H. H.: *Data Cleaning: Problems and Current Approaches*. IEEE Bulletin on Data Engineering 23:4, 2000.
12. Martin Wischenbart , Stefan Mitsch , Elisabeth Kapsammer , Angelika Kusel , Birgit Pröll , Werner Retschitzegger , Wieland Schwinger , Johannes Schönböck , Manuel Wimmer , Stephan Lechner, *User profile integration made easy: model-driven extraction and transformation of social network schemas*, Proceedings of the 21st international conference companion on World Wide Web, April 16-20, 2012, Lyon, France.
13. Ng, V.; Chan, S.; Lau, D.; and Ying, C. M. 2007. *Incremental mining for temporal association rules for crime pattern discoveries*. In Proc. of the 18th Australasian Database Conference, volume 63, 123–132.
14. Wang, G., Chen, H., Atabakhsh, H.: *Automatically detecting deceptive criminal identities*. Communications of the ACM 47(3) (2004) 70–76.
15. Wagstaff, K., Cardie, C., Rogers, S., Schr¨odl, S.: *Constrained k-means clustering with background knowledge*. In: Int'l Conf on Machine Learning. (2001) 577–584.
16. Hsinchun Chen, Wingyan Chung, Yi Qin, Michael Chau, Jennifer Jie Xu, Gang Wang, Rong Zheng, Homa Atabakhsh, "Crime Data Mining: A General Framework and Some Examples", *IEEE Computer Society,* April 2004.

17. Chau, M., Xu, J., & Chen, H. (2002). *Extracting meaningful entities from police narrative reports*. In: Proceedings of the National Conference for Digital Government Research (dg.o 2002), Los Angeles,-California, USA.

18. Mohammad Reza Keyvanpour, Mostafa Javideh, Mohammad Reza Ebrahimi, Detecting and investigating crime by means of data mining: a general crime matching framework, *Procedia Computer Science,* Volume 3, 2011, Pages 872-880.

19. A. Milani Fard and M. Ester, "*Collaborative mining in multiple social networks data for criminal group discovery*" in Proc. SocialCom 2009, pp. 582-587.

20. Pinto, P. C., Thiran, P. & Vetterli, M. Locating the source of diffusion in large-scale networks. *Phys. Rev. Lett*. 109, 068702 (2012).

21. Consonni, V., Todeschini, T., *New Similarity Coefficients for Binary Data,Communications in mathematical and in computer chemistry,* Vol. 68, No. 2, 2012, 581-592.

22. X. Su and T. M. Khoshgoftaar, (2009). A Survey of Collaborative Filtering Techniques, *Advances in Artificial Intelligence*, Hindawi Publishing Corporation,pp. 1–19.

23. Chengying Mao and Jifu Chen, QoS Prediction for Web Services Based on Similarity-Aware Slope One Collaborative Filtering, *Informatica*, 37 (2013) 139–148.

24. T. Wang, C. Rudin, D. Wagner, and R. Sevieri. *Learning to detect patterns of crime*. In Machine Learning and Knowledge Discovery in Databases, pages 515--530. Springer, 2013.

25. G.Angulakshmi, Dr.R.ManickaChezian," An Analysis on Opinion Mining: Techniques and Tools", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, Issue 7, July 2014, 2319-5940.

26. Dipali V. Talele ME[CSE],GHRIEM, Chandrashekhar D. Badgujar Asst. Prof. in Dept. of CSE, GHRIEM "*The Art of Opinion Mining and Its Application Domains: -A Survey*" at International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS -2012).

27. B. Pang and L. Lee, Opinion mining and sentiment analysis. *Foundations and Trends in Information Retrieval*, 2 (1-2): 1,135, 2008.

28. Bradley, M. M. & Lang, P. J. (1999a). *Affective norms for English words (ANEW): Instruction manual and affective ratings*. Technical Report C-1, The Center for Research in Psychophysiology, University of Florida.

29. CHANDRAN, Soumya; BAIRAVEL, S.. Intelligent System for the Prediction of Emotions via Text Mining. *Automation and Autonomous System*, [S.l.], v. 6, n. 3, p. 85-90, May. 2014.

30. Dipankar Das, "*Analysis and Tracking of Emotions in English and Bengali Texts: A Computational Approach*", Proceedings of the International World Wide Web Conference (WWW 2011), 2011, pp. 343-347.

UDC: 343.53:004(4-672EU)
343.85:343.53(4-672EU)

STRATEGIC RESPONSE OF EU INSTITUTIONS ON CYBERCRIME IN THE POST-LISBON PERIOD[1]

Sladjana Mladenovic[2]
Institute for Political Studies, Belgrade

Abstract: In this paper the author presents the strategic response of the European Union institutions on the problem of cybercrime in the period from the entering into force of the Treaty of Lisbon (2009) until the end of 2014. Strategic response of the EU institutions will be examined twofold.

On the one hand, the author explores the EU institutional setting for dealing with cybercrime, on three different levels: 1) the main EU institutions proclaimed in the Treaty of Lisbon, both intergovernmental (European Council – EC and Council of the European Union – Council) and supranational (European Commission – Commission, European Parliament – EP and the Court of Justice of the EU – CJEU); 2) EU bodies, offices and agencies within the Area of Freedom, Security and Justice (AFSJ) involved in the fight against cybercrime, namely Europol (hosting the European Cybercrime Centre), Eurojust and CEPOL; and 3) various groups, networks and other EU bodies, offices and agencies which according to their respective mandates have the auxiliary role in combating cybercrime, achieved mainly through cooperation with the first two levels actors. The division of tasks and mutual cooperation of these actors are envisioned in EU strategic documents such as the Stockholm Programme (SP), Internal Security Strategy (ISS) and Cybersecurity Strategy (CSS), as well as in other relevant legislative and programmatic documents.

On the other hand, the author will present the functioning of EU institutions on cybercrime within European Multidisciplinary Platform against Criminal Threats – EMPACT, a multi-annual EU Policy Cycle with the aim of ensuring the effective cooperation of all interested actors, and delivering the operational action against the criminal threats facing the EU, having cybercrime as one of its priorities.

Keywords: cybercrime, European Union, EU institutions, EU agencies, Europol, European Cybercrime Centre, Eurojust, CEPOL, EU Policy Cycle, EMPACT, Area of Freedom, Security and Justice.

EUROPEAN UNION INSTITUTIONAL SETTING FOR COMBATING CYBERCRIME

The fight against cybercrime in the European Union gradually evolved as an important EU internal security issue. Although embedded in the wider aspect of cyber security, it eventually became one of primary concerns in combating serious and organised international crime within the AFSJ. However, the incorporation of cyber security issues, and thus also cybercrime into the institutional structure of EU remains an open question due to the dual character of governance in this area: 1) emphasised role of Member States and 2) plurality of actors.[3]

The European Council has adopted the five-year Stockholm Programme in 2009, shortly after the Treaty of Lisbon entered into force, with the aim of bringing strategic guidelines into the AFSJ. The SP emphasised the fight against crime with typically cross-border dimension as the prime objective of EU law enforcement cooperation. The primary responsibility has been given to Europol, which should serve as a hub for information exchange between national law enforcement authorities (LEAs), a service provider and a platform for law enforcement services. Together with Eurojust it has significant role in using Joint Investigation Teams (JITs).[4] One of the areas of serious and organised crime singled out was cybercrime. Apart from the need for Member States (MSs) to ratify the 2001 Council of Europe (CoE) Convention on Cybercrime, EC asked the Commission to enhance the public-private partnership and make proposals for clarifying the legal framework of investigations in EU cyber space. On the other hand, Europol was seen as

1 This paper represents the result of research within the project No. 179009, financed by the Ministry for Education, Science and Technological Development of the Republic of Serbia.
2 sladjana.mladenovic83@gmail.com
3 A. Bendiek, "European Cyber Security Policy", *SWPR Research Paper*, RP 13, German Institute for International and Security Affairs, Berlin, 2012, p. 12.
4 European Council, The Stockholm Programme – an Open and Secure Europe Serving and Protecting Citizens, OJ EU, No. C 115, 4 May 2010, p. 20.

a European resource centre (by creating the European platform for identifying offences), with the task of stepping up strategic analysis on cybercrime.[5]

EC proclaimed that "the Council should, in principle, have a leading role in the evaluation process, and in particular in its follow-up".[6] The Commission was given the task of producing the action plan for implementation of SP. Both the Commission and the EP have followed their own agendas in the aftermath of the SP, rather than observing its stipulations. It was provoked by the EC's Council-dominant focus, while suggesting the Commission its tasks and ignoring the EP's new position. The Commission responded by not strictly following the prescribed agenda and instead pursuing its own, insisting on the right of legislative initiative and not carrying out detailed evaluation of the SP implementation. By developing its policy priorities and recommendations, the EP became a co-owner and a policy agenda-setter in AFSJ.[7] Another supranational actor, the CJEU, was given significant role in creating the "uniform European fundamental and human rights system" based on the CoE European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the Charter of Fundamental Rights of the European Union (CFR).[8]

The Commission emphasised that the implementation of Action Plan for SP (ASP) depended on the political commitment of all concerned actors: "the Commission as its driving force, the European Parliament and the Council when debating and enacting proposals, national parliaments in their scrutiny of subsidiarity and proportionality", thus putting itself in the foreground.[9] As far as cybercrime, it was linked with network and information security, and outlining: 1) creation of a cybercrime alert platform at European level; 2) developing a European model agreement on public-private partnerships in the fight against cybercrime; and 3) adopting measures, including legislative proposals to establish rules on jurisdiction on cyberspace at European and international levels. The first measure was to be achieved by joint effort of Europol and the Commission, while the others were only envisioned as tasks of the Commission.[10] The Council in its Conclusions on the Action Plan urged the Commission to take forward those matters which were in conformity with SP and criticised the Commission for inconsistencies between SP and ASP.[11]

According to the mandate of the EC in SP, the Council adopted Draft Internal Security Strategy which identified cybercrime within common threats, i.e. the challenges for the EU internal security.[12] However, it was not until the adoption of the Commission Communication on Internal Security Strategy that specific actions were envisioned. The Commission put the fight against cybercrime in the broader context of raising levels of security for citizens and businesses in cyber space. The main problem perceived by the Commission was the fact that although Internet knows no boundaries, the jurisdiction for prosecuting cybercrime stops at national borders. It was also noticed that the coordinating role for law enforcement of the High Tech Crime Centre at Europol was not enough. Therefore, the Commission envisioned three actions: 1) building capacity in law enforcement and the judiciary; 2) working with industry to empower and protect citizens; and 3) improving capability for dealing with cyber attacks.[13] As can be concluded, all three actions included dealing with cybercrime, albeit each in different manner and with different actors.

Building capacity in law enforcement and the judiciary was to be achieved primarily by establishing a cybercrime centre within existing structures by 2013, as a focal point in Europe's fight against cybercrime. The cybercrime centre should cooperate with the European Network and Information Security Agency (ENISA) and interact with a network of national Computer Emergency Response Teams (CERTs). Eurojust, CEPOL and Europol were given the tasks of helping MSs to develop national cybercrime awareness and training capabilities, and establish centres of excellence on national or international level. The Commission kept for itself the primary role in working with industry by establishing, if appropriate, the European cybercrime alert platform (for reporting cybercrime incidents), central pool of shared resources and best practices among MSs and the industry, and European Public-Private Partnership for Resilience (EP3R). It

5 *Ibid*., pp. 22-23.
6 *Ibid*., p. 6.
7 S. Carrera, E. Guild, "The European Council's Guidelines for the Area of Freedom, Security and Justice 2020: Subverting the 'Lisbonisation' of Justice and Home Affairs?", *CEPS Essay*, No.13/14, Centre for European Policy Studies, Brussels, July 2014, pp. 4-5.
8 European Council, The Stockholm Programme – an Open and Secure Europe Serving and Protecting Citizens, *op.cit*., p. 8. With the adoption of the Lisbon Treaty, CFR became binding legal instrument which had major impact on CJEU rulings in AFSJ even prior to the end of transitional five-year period (expired on 1 December 2014) after which the CJEU assumed additional authority in this area.
9 The European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm Programme, COM(2010) 171 final, Brussels, 20 April 2010, p. 9.
10 *Ibid*., pp. 36-37.
11 House of Lords, European Union Committee, "Strategic Guidelines for the next Justice and Home Affairs programme: steady as she goes", *HL Paper 173*, London, 2014, p. 11.
12 Council of the European Union, Draft Internal Security Strategy for the European Union: "Towards a European Security Model", 7120/10, Brussels, 8 March 2010, p. 6.
13 The European Commission, Communication from the Commission to the European Parliament and the Council. The EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe, COM(2010) 673 final, Brussels, 22 November 2010, pp. 9-10.

also decided to promote the use of an internet-based Contact Initiative against Cybercrime for Industry and Law Enforcement. Dealing with cyber attacks is a subject of concern both at national and European levels, which is why the Commission urged the establishment of CERTs within MSs and European institutions, in order to develop (by engaging with ENISA) a European Information Sharing and Alert System (EISAS).[14]

Prior to adopting the next strategic document in AFSJ, this area saw the establishment of a European Cybercrime Centre (EC3) within Europol in a growing effort to communitarise AFSJ agencies.[15] In its Communication on establishing EC3, the Commission singled out major strands in order for EC3 to provide added value. These are: 1) cybercrime committed by organised crime groups (particularly OCGs which are generating large profits as in online fraud); 2) cybercrime which causes serious harm to victims (as online child sexual exploitation); and 3) cybercrime affecting critical infrastructure and information systems in EU (including cyber attacks).[16] The core functions of EC3 are to: 1) be European cybercrime information focal point (by collecting information from public, private and open sources); 2) pool expertise in supporting MSs in capacity building by assisting in expertise and training; 3) provide support to MSs' cybercrime investigations (especially by encouraging the establishment of JITs and exchanging of operational information during investigations); and 4) become collective voice of European cybercrime investigators in both law enforcement and judiciary.[17]

The question of precise tasks of EC3 was raised soon after the Commission Communication, by two different stakeholders. The Council called upon the Commission (in consultation with Europol) to "further elaborate the scope of specific tasks" of EC3.[18] The European Data Protection Supervisor criticised the Commission on several grounds, one of them referring to competences of EC3, with primary concern of data protection due to the expected new Europol legal regime.[19] He also emphasised that if EC3 had been involved in operational and investigative activities, there should be clear procedure for such involvement as well as respect for individual rights and procedural guaranties for evidence collection.[20]

Immediately after establishing EC3 in January 2013, the Commission adopted the EU Cybersecurity Strategy in February the same year. One of the strategic priorities therein is to drastically reduce cybercrime. That priority has three aspects: 1) strong and effective legislation; 2) enhanced operational capability to combat cybercrime; and 3) improved coordination at EU level. The Commission's tasks include: commitment to ensure transposition and implementation of cybercrime related directives; urging MSs to ratify and implement the CoE Convention on Cybercrime; financial support and finding best practices and techniques in the fight against cybercrime; support to Europol/EC3 and Eurojust in aligning policy approaches and best practices; and involvement in the fight against cybercrime outside EU.[21] Europol/EC3 was asked to focus on MS's cybercrime investigations and produce strategic and operational reports on trends and threats related to cybercrime. It should cooperate with CEPOL in designing and planning of training courses to LEA, and with Eurojust in order to increase effectiveness in combating cybercrime. Eurojust should focus on identifying the obstacles to judicial cooperation on cybercrime investigations and coordinate between MSs and with third countries in supporting investigation and prosecution on cybercrime.[22]

CSS made a link between internal security and crime issues and EU internal market and defence areas. Therefore, actors within law enforcement such as Europol/EC3, Eurojust and CEPOL were given the responsibility to interact with entities outside AFSJ, on both European and national levels. Those entities have their respective mandates that are not directly pointed to combating cybercrime, but cybercrime can

14 *Ibid*.

15 E. Fahey, "The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation*, No. 1, 2014, pp. 52-53. The author of the cited paper calls EC3 "quasi-institution". In the feasibility study ordered by the Commission, and conducted prior to establishing EC3, RAND concluded that the risks associated with the new Centre were related to its visibility and institutional complexity. Therefore, the focus of EC3 should be put on "measurable benefits for law enforcement rather than trying to tackle the much broader aspect of cybersecurity", especially due to the range of partners within and outside Europe. N. Robinson et al., *Feasibility Study for a European Cybercrime Centre*, Final Report, TR-1218-EC, RAND Europe, Cambridge, 2012, p. 4.

16 The European Commission, Communication from the Commission to the Council and the European Parliament. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final, Brussels, 28 March 2012, p. 4.

17 *Ibid*., pp. 4-5.

18 The Council of the European Union, Council conclusions on the establishment of a European Cybercrime Centre, Luxembourg, 7 and 8 June 2012, p. 3.

19 European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre, Brussels, 29 June 2012, pp. 3-5. In the dilemma of data protection within AFSJ policies, CJEU took substantial role. In CJEU ruling of 8 April 2014, the Directive 2006/24/EC (Data Retention Directive) was declared invalid. Court ruled that the interference with fundamental rights went beyond what was strictly necessary and was not in accordance with the principle of proportionality. However, the Court acknowledged the fight against serious crime as an objective of general interest. The Court of Justice of the European Union, Press Release No. 54/14, Judgment in Joined Cases C-293/12 and C-594/12, Luxembourg, 8 April 2014, p. 2.

20 European Data Protection Supervisor, *op.cit*., p. 7.

21 The European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, Brussels, 7 February 2013, pp. 9-10.

22 *Ibid*., pp. 10-11.

fall within the scope of their activities. Due to different legal frameworks and jurisdictions as well as many actors, the EU should clarify the roles and responsibilities of each of them. Instead of centralised European supervision, MSs are designated to prevent and respond to cyber incidents/attacks and contact with private sector and general public, while EU should be involved with national response due to borderless nature of the risks.[23]

In the Commission report concerning implementation of CSS, within the strategic priority of drastically reducing cybercrime, all three aspects mentioned in CSS were tackled. Within strong and effective legislation, the EU institutions adopted two directives: Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and Directive 2013/40/EU of 12 August 2013 on attacks against information systems, both of them replacing previous Council framework decisions.[24] Enhanced operational capability to combat cybercrime included several institutional engagements: 1) revised agreement between EC3, CEPOL and ECTEG (European Cybercrime Training and Education Group) with the aim of updating training curricula; 2) establishment of European Law Enforcement Training Scheme (LETS); 3) funding of 10 Cybercrime Centres of Excellence in Research and Training in MSs; 4) funding of European Academy of Law (ERA) training courses on legal and technical aspects of cybercrime; 5) cooperation of the Commission's Joint Research Centre (JRC) and EC3; 6) the Commission support to MSs' mutual assessment of cybercrime within the Council Working Party on General Matters including Evaluations (GENVAL); and 7) cooperation within EMPACT.[25] Improved coordination at the EU level, next to the already mentioned actions and regular activities, includes plans for future funding of Europol and EMPACT from the Internal Security Fund "Police", and proposed (but rejected for the current work programme) funding for research purposes to Europol from the Horizon 2020 budget.[26]

The EC in its Conclusions in June 2014 considered the future steps in a number of areas, the first being AFSJ. One of the priorities in the next five-year term is prevention and combating crime and terrorism, among which is the fight against cybercrime.[27] The reinforced coordination role of Europol and Eurojust include, *inter alia*, review and update of the ISS by mid 2015; improvement of cross-border information exchange, including on criminal records; and "the further development of a comprehensive approach to cyber security and cybercrime".[28] The EU institutions and MSs are called to ensure follow-up to EC guidelines and to hold a mid-term review in 2017.[29]

Bearing in mind the announced adoption of a renewed Internal Security Strategy in 2015, the Council adopted draft conclusions thereof. Cybercrime was one of areas of serious and organised crime. Along with cyber security, cybercrime has to be tackled by taking into consideration that Internet represents fundamental tool for EU growth, and that it needs to be kept open and free and secured from illicit exploitation.[30] As far as engagement of institutions, the Council marked its Standing Committee on Operational Cooperation on Internal Security (COSI) as an actor responsible for implementing and monitoring ISS, while at the same time facilitating the operational cooperation among MSs. The Commission was called upon to submit annual reports on actions within ISS to the Council and EP, based on which the Council should consider appropriate measures for the achievement of goals. The Council emphasised that the AFSJ would be developed in compliance with EC's Strategic Guidelines set in June 2014.[31] As regards particular area of cybercrime, the Council Friends of Presidency Group on Cyber Issues will continue to coordinate cyber-related work in various policy areas and contribute to closer cooperation between EU agencies in cyber domain. One of pending issues refers to new legal base for both Europol and CEPOL.[32]

EU CRIME POLICY CYCLES

The first policy cycle for combating crime within AFSJ was a European Criminal Intelligence Model (ECIM), a pre-Lisbon, intergovernmental, Member States-driven policy cycle. It was enshrined in the British-inspired law enforcement theory of intelligence-led policing. It presupposed the cooperation of national

23 *Ibid*., p. 17.
24 The European Commission, Working document, Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", JOIN (2013) 1, Brussels, 28 February 2014, p. 5.
25 *Ibid*., pp. 7-10.
26 *Ibid*., pp. 10-15.
27 The European Council, Conclusions, Brussels, 27 June 2014, p. 19.
28 *Ibid*., p. 5.
29 *Ibid*., p. 6.
30 The Council of the European Union, Draft Council conclusions on the development of a renewed European Union Internal Security Strategy, 14186/6/14, Brussels, 13 November 2014, pp. 6-7.
31 *Ibid*., p. 13.
32 *Ibid*., p. 53. In 2013 the Commission presented ambitious legislative packages on a new legal framework for all three agencies relevant in combating cybercrime – Europol, CEPOL and Eurojust. The first two of them should have been merged, but both EP and Council rejected such a possibility. The proposed regulation on turning Eurojust into a fully-fledged EU agency was also not adopted.

LEAs, Europol and European Police Chiefs Task Force (PCTF) at the European level.[33] On the other hand, the Netherlands presented its proposal regarding the European police cooperation – the Comprehensive Operational Strategic Plan for the Police (COSPOL). The Council stressed out that it should not be seen as a new tool or structure, but purely as methodology for strengthening police cooperation.[34]

In 2010 the Council established a new four-year EU policy cycle for serious international and organised crime, the European Multidisciplinary Platform Against Criminal Threats (EMPACT). It was based on the experiences from COSPOL approach and the success of its projects. The more important was that it was grounded in a post-Lisbon context.[35] Its key features are: intelligence-led approach (in context of ECIM); integrated character (using multidisciplinary and multi-agency actors); "integral", "broad" or "holistic" approach; and project approach.[36]

The need for a new policy cycle stemmed from the adoption of the ISS, which led the ministers to ask the COSI to develop a new methodology of tackling security issues within Europe with special attention to threats and challenges.[37] EMPACT consists of four steps: 1) policy development with picturing criminal threats on EU on the basis of EU Serious and Organised Crime Threat Assessment (SOCTA) produced by Europol; 2) definition of priorities by the Council, with each priority having a Multi-Annual Strategic Plan (MASP); 3) development of annual Operational Action Plans (OAP) in line with strategic goals defined by MASP upon the COSPOL framework; and 4) evaluation at the end of the cycle as an input for the next cycle. The Council made the decision that an initial cycle was to be a reduced one, and consist of a two-year cycle 2011-2013 based on Europol Organised Crime Threat Assessment (OCTA) produced in 2011. The results of such reduced cycle were to be used for the fully-fledged four-year term policy cycle 2013-2017 on the basis of SOCTA 2013.[38] In 2011 the Council adopted conclusions on setting the priorities for the fight against organised crime in 2011-2013 on the basis of OCTA 2011. One of eight priorities was stepping up the fight against cybercrime and the criminal misuse of Internet by OCGs.[39]

The Council set the roles of various entities participating in a serious and organised crime policy cycle. COSI was given the coordination role, and its assignments consist in endorsing the customer requirements for EU SOCTA, submitting the conclusions to the Council for the latter to decide on priorities and adopting, coordinating and monitoring the implementation of MASPs and OAPs. The role of the Commission consists in: 1) the development of MASPs (together with experts of EU Agencies and MSs); 2) development on independent mechanism of evaluating the implementation of MASP and OAPs; 3) reporting yearly on implementation of activities and horizontal crosscutting issues related to OAPs to COSI; 4) carrying an overall evaluation of the implementation of MASP at the end of a policy cycle and transmitting the results thereof to Council via COSI; and 5) considering the setting up the Internal Security Fund to support the activities within the policy cycle. When it comes to the EU Agencies, the Council highlighted the role of Europol due to its responsibility for delivering EU SOCTA, and CEPOL which was given the assignment of contributing to raising awareness about the EU policy cycle, in particular by providing training packages. All the relevant agencies were tasked to develop OAPs with the experts of Member States, and to integrate the actions within the policy cycles into their respective yearly working programmes.[40]

Europol provided inaugural edition of SOCTA in 2013.[41] It defined three aspects within cybercrime which need to be tackled: 1) profit-driven cybercrime and hacktivism; 2) online child sexual exploitation (CSE); and 3) payment card fraud.[42] In 2014 Europol/EC3 adopted Internet Organised Crime Threat Assesment (iOCTA) for the 2014 EMPACT cycle. The three areas within cybercrime were defined in a slightly different way than in SOCTA 2013: 1) cyber attacks, 2) online child sexual exploitation and 3) payment fraud. The aim of iOCTA is to "inform priority setting for the EMPACT Operational Action Plan for 2015 in the three sub-areas of the cybercrime priority".[43] The focus is put on the crime areas within the scope of EC3, investigated by Europol Focal Points Cyborg (Internet-enabled crime), Twins (CSE) and Terminal

33 H. Brady, "Europol and the European Criminal Intelligence Model: a Non-state Response to Organized Crime", *Policing*, Vol. 2, No.1, Oxford University Press, 2008, pp. 106-107.
34 The Council of the European Union, Conclusions on the 10th meeting of the Police Chiefs Task Force - 11 and 12 October 2004, 14094/04, Brussels, 29 October 2004, p. 2. One of the targets within COSPOL was cybercrime, but only the aspect of child pornography, placing Sweden at the fore as a leading country.
35 The Council of the European Union, Amending the COSPOL framework into EMPACT, 15386/1/11, Brussels, 3 November 2011, p. 3.
36 *Ibid*., pp. 4-5.
37 The Council of the European Union, the Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime, Brussels, 8 and 9 November 2010, p. 2.
38 *Ibid*., p. 3.
39 Council of the European Union, Council conclusions on setting the EU's priorities for the fight against organised crime between 2011 and 2013, Luxembourg, 9 and 10 June 2011, p. 3.
40 Council of the European Union, Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime, *op.cit.*, p. 4.
41 Europol, SOCTA 2013, The Hague, 2013, p. 5.
42 *Ibid*., pp. 30-32.
43 Europol, The Internet Organised Crime Threat Assessment (iOCTA), The Hague, 2014, p. 15.

(payment card fraud).[44] The contribution was also given by Member States, the EUCTF (European Cybercrime Task Force), Cyber Intelligence team, Serious Organised Crime Strategic Analysis team and the Data Protection Office, as well as private sector, EC3 advisory groups and academia. These contributions were combined with open source research and analysis.[45] Europol shall prepare an interim SOCTA in 2015, in order to evaluate, monitor and perhaps adjust the existing efforts in fulfillment of tasks.[46]

CONCLUSIONS

Despite being a global problem by its borderless nature, cybercrime can also be seen as an EU problem on the internal plane. The subject of this paper was precisely the fight against cybercrime at the EU level, primarily focusing on the institutional aspect of the matter. Although combating cybercrime was proclaimed as a priority in a number of EU documents, it is still virtually at the beginning. In the observed period 2009-2014 it came down to setting the institutional framework which was put into operation at the end of the period and could only show results in the years to come.

The strategic response on cybercrime involves actors from various levels, but the primary role was taken by the main EU institutions, which are setting the pace in the strategic documents in AFSJ and cybercrime domains. Since the SP initiated by EC, through ISS adopted by the Council and operationalised by the Commission, until CSS adopted by the Commission, the author presented the expanding role of the Commission, positioning of EP as a policy agenda-setter and co-owner in AFSJ, growing concern of the EC/Council over these developments and recently exercised "exploitation" of the binding nature of CFR by the CJEU ruling on Data Retention Directive. At the same time, the EC/Council and the Commission are engaging other actors in the operationalisation of the fight against cybercrime, but still without tangible outcomes. The EU agencies Europol, CEPOL and Eurojust are awaiting for the change in their respective legal frameworks. The groups, networks, bodies, offices and agencies originating from MSs on the one hand, and from the EU environment on the other should, according to the Commission's plans, be focused on the cooperation with the supposed EU focal point for the fight against cybercrime, Europol-based EC3. So far its share of the strategic EU response on cybercrime has been expressed in adoption of iOCTA, a basis for setting OAP for cybercrime in 2015. The latter means that the institutional setting is only commencing to put the proclaimed priorities in combating cybercrime into practice. The period 2009-2014 served for the establishment of EMPACT Policy Cycle, but the first results of this model can be expected upon adopting an interim report of its progress in 2015. The results will largely depend upon MSs, due to their dominant operational role. It remains to be seen whether the EU institutional setting with its strategy-oriented approach will be able to handle MSs roles effectively.

REFERENCES

1. Bendiek, A., "European Cyber Security Policy", *SWPR Research Paper*, RP 13, German Institute for International and Security Affairs, Berlin, 2012;
2. Brady, H., "Europol and the European Criminal Intelligence Model: a Non-state Response to Organized Crime", *Policing*, Vol. 2, No.1, Oxford University Press, 2008;
3. Carrera, S., Guild, E., "The European Council's Guidelines for the Area of Freedom, Security and Justice 2020: Subverting the 'Lisbonisation' of Justice and Home Affairs?", *CEPS Essay*, No.13/14, Centre for European Policy Studies, Brussels, July 2014;
4. The Council of the European Union, Amending the COSPOL framework into EMPACT, 15386/1/11, Brussels, 3 November 2011;
5. The Council of the European Union, Conclusions on the 10th meeting of the Police Chiefs Task Force – 11 and 12 October 2004, 14094/04, Brussels, 29 October 2004;
6. The Council of the European Union, the Council conclusions on setting the EU's priorities for the fight against organised crime between 2011 and 2013, Luxembourg, 9 and 10 June 2011;
7. The Council of the European Union, the Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime, Brussels, 8 and 9 November 2010;
8. The Council of the European Union, the Council conclusions on the establishment of a European Cybercrime Centre, Luxembourg, 7 and 8 June 2012;

44 *Ibid*., p. 15.
45 *Ibid*., p. 16.
46 Europol, SOCTA 2013, *op.cit*., p. 6.

9. The Council of the European Union, Draft Council conclusions on the development of a renewed European Union Internal Security Strategy, 14186/6/14, Brussels, 13 November 2014;
10. The Council of the European Union, Draft Internal Security Strategy for the European Union: "Towards a European Security Model", 7120/10, Brussels, 8 March 2010;
11. The Court of Justice of the European Union, Press Release No. 54/14, Judgment in Joined Cases C-293/12 and C-594/12, Luxembourg, 8 April 2014;
12. The European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm Programme, COM(2010) 171 final, Brussels, 20 April 2010;
13. The European Commission, Communication from the Commission to the Council and the European Parliament. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final, Brussels, 28 March 2012;
14. The European Commission, Communication from the Commission to the European Parliament and the Council. The EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe, COM(2010) 673 final, Brussels, 22 November 2010;
15. The European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, Brussels, 7 February 2013;
16. The European Commission, Working document, Table on the Implementation of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", JOIN (2013) 1, Brussels, 28 February 2014;
17. The European Council, Conclusions, Brussels, 27 June 2014;
18. The European Council, The Stockholm Programme – an Open and Secure Europe Serving and Protecting Citizens, OJ EU, No. C 115, 4 May 2010, p. 1;
19. European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre, Brussels, 29 June 2012;
20. Europol, SOCTA 2013, The Hague, 2013;
21. Europol, The Internet Organised Crime Threat Assessment (iOCTA), The Hague, 2014;
22. Fahey, E., "The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation*, No. 1, 2014;
23. The House of Lords, the European Union Committee, "Strategic Guidelines for the next Justice and Home Affairs programme: steady as she goes", *HL Paper 173*, London, 2014;
24. Robinson, N. et al., *Feasibility Study for a European Cybercrime Centre*, Final Report, TR-1218-EC, RAND Europe, Cambridge, 2012.

UDC: 343.53:004
343.983:004
004.6

CHALLENGES OF RECOVERING AND ANALYZING VOLATILE DATA

Milana Pisaric[1]
University of Novi Sad, Faculty of Law

Abstract: In early years of computer forensics there was one rule whenever an investigator found a running system during a search and seizure process: Pull the plug! In times where the amount of volatile data in memory, remote connections and the usage of encryption software grow bigger and bigger, this old rule became outdated many years ago. The acquisition and analysis of volatile data is of high importance as it might be of high evidential value. That is why Live Data Forensics plays an important part in search and seizure situations nowadays. As traditional digital forensic analysis is in some cases becoming impractical and examiners must often rely on an in-situ investigation of the live computing environment, the special attention should be paid to live forensics. Live forensics is performed on a running computer system and may capture all running processes and all volatile data such as the current configuration of the machine and the data in its RAM memory, data that would be lost as soon as the machine is powered down. Volatile data may contain many pieces of information relevant to a forensic investigation and having the knowledge and tools needed to recover and analyze that data is essential and is becoming increasingly more relevant. Live Data Forensics deals with situations where it is necessary to capture data from devices before they are turned off or disconnected from networks or power supplies and it requires a higher level of specialism than the procedure in the search and seizure of dead boxes. There are many relatively new tools available that have been developed in order to recover and dissect the information that can be gleaned from volatile memory. This paper will cover the theory behind volatile memory analysis, including why it is important, what kinds of data can be recovered, which tools and techniques developed for this purpose can be used and which technical and legal issues represent the challenges for forensically sound acquisition of volatile data from live computer systems.

Keywords: digital evidence, digital forensics, volatile data, love data forensics.

INTRODUCTION

There is a variety of standard operating procedures for the purpose of storing and processing electronic evidence. These standards should be general enough to represent the basic steps in routine forensic examination as a sort of instruction but should leave room for flexibility of reaction to unforeseen situations. Whichever standard procedure is chosen or prescribed as obligatory, it basically comes to these phases: 1. Collection of data: a. identification of data; b. preservation of data c. extraction of data; d. packaging, transport and storage of data; 2. Analysis of data (to provide the data that can be used as evidence in court). First, it is necessary to determine which data are available and where they are (i.e. who is the source of electronic evidence) in a thorough manner with respect to the circumstances of concrete case, which determines the future course of action to be taken. As computer data are by their very nature prone to modifications, damage or loss, in order to protect and preserve the integrity and reliability of electronic evidence, a clone of device on which they are stored is created (imaging), which is then safely packed and transported to the laboratory for analysis (dead box). However, in certain cases it is necessary to conduct an analysis of the "live" computer system (live forensics).

DIGITAL CRIME SCENE EXAMINATION

The standard methodology in conjunction with an electronic evidence during the 90s meant that the computer which was supposed to contain relevant data was excluded from the power source, packed and sent from the crime scene to the laboratory where forensic scientist made a copy of the hard disk bit by bit and on that copy search and analysis was done about the report which was made in the end. Digital forensics was engaged in the research, development and application of appropriate techniques, tools and

1 mpisaric@pf.uns.ac.rs

methods for collecting, storing and preserving exempted from the computer system[2]. Given the nature of electronic evidence and principals and standards relating to the collection and storage of computer data, all actions that may cause modification, damage or loss of data may lead to non-acceptance of evidence in court[3]. However, in exceptional circumstances, it is sometimes necessary to take action in a computer system before being switched off and transported to the laboratory. In these circumstances that computer may be considered as digital crime scene and it was necessary to develop procedure for digital crime scene examination.

There are, therefore, two methodological correct scenarios: a search and seizure in "dead box" scenario and search and seizure in "live data" scenario. In the first situation, the tools and equipment are deducted from the crime scene and then transferred to the laboratory in which the review and exclusion of relevant computer data is done afterwards. The second refers to the situation when it is necessary to review devices and equipment to extract data on the crime scene before being disconnected from the network or from the electronic power supply (as a sort of situational *in situ* expertise), which requires a higher degree of specialization and can be performed only by highly trained staff. Decision on what scenario is the best solution in a concrete case: to approach seizure of devices and equipment from the crime scene and their search in laboratory or to search them on the crime scene or to apply a combination of both approaches, depends on the circumstances of the case. However, still in the planning stage it is necessary to collect as much information as possible regarding the information system and potential sources of electronic evidence, and as well about: computer hardware, operating system, software, applications, networks, and related information pertaining to communication (ISP, phone, fax, modem, LAN network equipment, etc.); that person is responsible for computer system and/ or network (for example, if a network managed by a local administrator or an external company); how much equipment is expected to be present at the scene and how the data will be confiscated etc.

SEARCH AND SEIZURE IN LIVE DATA SCENARIOS

From the early years of computer forensics as one of the most important rules was that the researcher whenever the computer was found during the search and seizure at crime scene was supposed to unplug it from the power supply. This traditional methodology for the collection of electronic evidence is still widely used in the treatment of the competent authority as the seizure of computer system and the implementation of a forensic examination at a later stage (in the laboratory) is still considered as the appropriate method which ensures the integrity of the evidence and it can be assumed that this will be the standard for many years to come. However, there are exceptions to the rule. Specifically, certain circumstances require testing of the current system in an ever-increasing number of cases and for several reasons. One of the circumstances relates to the increasing prevalence of small wired or wireless computer networks in the home or business premises where a computer that is the subject of the search is. In addition, this rule is completely inappropriate given the increasing prevalence of 1. volatile data in memory, 2. remote connections and 3. use of encryption software. As the collection and analysis of volatile data is of great importance because data as they may have a great probative value, which cannot be ensured by applying the rules relating to the packaging and transport of devices to a laboratory for analysis but it takes an expert and careful handling of data in "live systems ", Live Data Forensics is becoming an increasingly important role.

In certain situations it is necessary to find and exclude data from the device before being shut down or disconnected from the network or source of supply. In this case, the risk of change, damage or loss of data is very high, so much higher level of specialization of staff is required compared to "dead box" scenario. In addition, investigators should be aware of the fact that they change the data in the computer of the suspect. They must be qualified and competent to carry out the necessary steps and must use techniques that cause minimal impact on the system. It is also necessary to leave detailed audit trial as a record of all actions undertaken as well of the time they were taken.

Forensic examination of the "live" systems requires special training, practical experience and proven set of forensic tools. If the presence of specialized forensic experts could not be secured, the prompt support of the specialized units should be sought, and if this cannot be provided, the more proper decision is to plug out than manipulate volatile data which can result in contamination of evidence and the impossibility of its use in court[4].

2 First Responders Guide to Computer Forensics(CERT Training and Education Handbook, http://www.sei.cmu.edu/reports/05hb001.pdf

3 Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (Washington, DC: July 2001) https://www.ncjrs.gov/pdffiles1/nij/219941.pdf Овај водич је саставила и одобрила Техничка радна група за увиђај лица места за електронски криминал (Technical Working Group for Electronic Crime Scene Investigation).

4 https://www.ncjrs.gov/pdffiles1/nij/219941.pdf стр.25

Although the proper practices in case of running on a computer network is to call for help from experts, the number of persons trained in computer and network forensics is insufficient to secure the adequate on-site professional support in an ever-growing amount of small computer networks. For this reason it is essential that people who take action in first operation to be trained to collect potential evidence instituted by the computer system at crime scene.

VOLATILE DATA

Volatile data are those data that are stored digitally in a way that it is a very high probability that the content is deleted, overwritten or changed in a short period of time and as a result either of human activity or automated actions in the computer system. Volatile data are stored in RAM memory which is a main memory in the computer used by the operating system and applications running while the computer is on. Data on all active processes in the computer are stored in this memory but are lost the moment the computer is shut down and cannot be recovered any longer. There are various types of volatile data:

– volatile data in the computer, such as data on open network connections or running applications;
– interim volatile data that are not volatile by their nature, but are available or can be accessed only on the site (for example, encrypted data or data that are stored on remote resources) so their contents may become unavailable, altered or lost if the investigator does not collect them at the right time because it may become impossible to access them later.

The RAM memory contains very useful information, such as, for example: information about processes (currently running, hidden, and the recently completed processes), about open files and registers used by process, operating system information, the decoded data or applications (which is useful if the device has installed software for data encryption / application encryption), passwords and cryptographic keys to decrypt the encrypted content and information about other security mechanisms installed in the computer by the user, the data on registered users, information about network connections, information about how to start system, open instant messaging, hidden data...

As the memory capacity is growing, it is not uncommon that RAM memory contains several gigabytes of data, and the authorities of the proceedings should not afford to lose 12 GB or 16 GB of data (which could be around 55,000 images with an average size of 300 KB) by simply turning off the device. Volatile data can without any doubt be useful for the case, however, as they are very "fragile", which means that it can easily be lost or altered if not handled in responder manner, it is necessary to devote attention to create the proper methodology of how to access them, that is, to save them quickly and correctly. All these data would be irretrievably lost if the traditional procedure were respected: that the device is disconnected from the power supply, so it is a better solution first to collect volatile data and then power off the device.

Analysis of RAM can contribute to investigative purpose which is the collection of relevant data, because it goes beyond a few limitations of traditional forensic analysis as well as problems that are caused by new technologies, such as encryption, which occur during the described method.

Traditional forensic analysis is limited in several ways.

A. The investigator cannot access to encrypted contents unless user password or key by which the data is encrypted is reached. Passwords and keys are rarely stored on the hard disk so search of hard disk will often not give results in this regard. However, when the user at the keyboard types passwords or when the data are decrypted, then the passwords and keys are stored at that moment in RAM, and they may be reached by analyzing the RAM memory on a live system.

B. Furthermore, the physical disk does not show data about the processes that were started in the computer's memory, and the analysis of the hard drive cannot explain how the applications were used in the system at the time of execution of actions.

C. Also, there is a possibility that the suspect is hiding data in RAM memory and is not keeping them on the hard disk.

D. It is common to produce viruses, Trojans and worms that reside in memory and are not stored on a hard disk of the computer they attack so the analysis of the hard drive does not reveal the malicious code or the way which the attack took place.

METHODOLOGY OF COLLECTING VOLATILE DATA FROM "LIVE" SYSTEMS

There are two methods to collect volatile data:

1) The method based on the use of hardware;

2) The method based on the use of software.

The first method to collect volatile data is carried out by using special hardware which suspends the processor and uses direct access to memory in order to create a copy of the memory that is then analyzed[5]. Such actions are considered to be more reliable because even if the operating system and software systems are compromised by the user, this way an identical copy of memory is acquired because its creation does not rely on the aforementioned components of a computer system. However, the lack of access is the price of this special hardware. Therefore, it is more common to use method of collecting volatile data based on specialized software designed for this purpose. There are a number of forensic tools that are used to collect volatile computer data. Bearing in mind the speed of technological development, there is a risk that currently applicable techniques and tools may become obsolete in the near future. For this reason it is necessary to pay attention to the development and respect for a certain methodology that would be technologically neutral and in accordance with established principles of handling electronic evidence.

When selecting forensic tools to collect volatile data, the investigator should keep in mind the following:

– give preference to a tool that has the least possible impact on the system. For example, for the collection of data in RAM, the better solution is to use a tool like *Dumpit* rather than required graphical tools such as FTK Imager;

– the tool should be able to have its own automatic execution so it may be run without the use of unverified binar commands from the system from which the data is collected;

– investigator should use only those tools whose operation can be explained in the court;

– tool should be automated and not require a lot of interaction with users given that the investigator will not remember all of the options for all commands and will not be able to observe at all times the processing of data in a situation where there is more than one device which is to be engaged;

– tool should be configured to collect volatile data only and not the data that are normally available on hard-disk drive (which subsequently can certainly be collected via usual procedures).

Although there are certain configured Live Forensics DVD with a wide range of tools, it is recommended that the investigator themselves assemble a compilation of tools for their own needs, as opposed to cases in which the needs are encountered in accordance with the national regulations (all activities that may be applied by these tools may not be allowed in all countries)[6].

This methodology should be applied regardless of the used forensic tools and techniques for analyzing computer memory. It is important to note that all the tools that are used produce some changes in the computer but these changes apply only to the operating system files and do not change the content stored in RAM memory. Namely, when the data is collected on the "live" devices it is inevitable that the use of forensic tools results in changes in the computer system that is active, for example, in Windows Registry, cache files or computer memory. While it is desirable that an investigator collect and preserve as much volatile data, it must be done in a way to leave as little trace of their actions in the system as possible.

The order in which the data are to be collected can also be crucial to the investigation and investigator should take this also into account. Although each individual case should be approached taking into account the circumstances of this case, it is desirable to comply with a prescribed methodology to collect volatile data according to a certain order of instability, i.e. volatility.

When the investigators collect the data from the active system, they will proceed properly if the collected data are not kept in the data storage device of this computer system but in the previously prepared external storage device that connects to a PC: USB sticks with a high capacity memory, external hard-drives with as many possibilities for connecting to a computer (USB/eSATA/FW), DVD with write protection which ensures the protection of recorded data or external hard-drive with a virtual DVD.

After direct access to the RAM and data stored within is achieved in described manner, a static forensic image of RAM memory is created that absolutely fits its condition at the time of collection or external forensic memory analysis is applied in the real-time. For the analysis of the image of computer RAM memory various software tools are used which allow obtaining the information on the status, configuration, and anomalies of the computer system. A particularly useful feature is that this kind of analysis detects malware that has infected the system. The analytical ability of the aforementioned tools is becoming more and more

5 For example: Tribble card which is PCI card that is being installed in the system.

6 Kristine Amari, Techniques and Tools for Recovering and Analyzing Data from Volatile Memory, 2009, 40-50.

used for various purposes: to analyze the distance[7], for the classification of malware even for self-healing of the compromised computers[8].

Volatile data collection techniques carry a unique evidentiary challenges because they inevitably bring changes on a live computer system. In certain jurisdictions the search order contains the power for an initial search and subsequent forensic analysis, whereas in other systems two search orders for these two phases need to be issued.

As the collection of volatile data is limited in coverage and purposes (that is to provide the data that could be lost forever if turning off the computer) we consider that special authorization is not required in addition to power to search the computer, except when circumstances of collecting volatile data require additional time or extends the scope of execution of originally approved order. This procedure does not apply to the collection of real-time communications content via a computer network. The actual collection of volatile data by applying this methodology should be regarded as one of the stages in search of a computer system as previously described steps apply only to the collection, security and registration of electronic evidence already present in computer (similar to collecting clues at the crime scene) that could be permanently lost, in case the proper steps were not undertaken. For this reason it is justified in an order that authorise the search of the computer to indicate the following:

– Document in electronic form and preserve the state of computer networks and electronic storage devices, and
– Conduct a review of computer memory in order to check whether there are hidden contents using the software for data recovery.

Certainly this can be done only by trained personnel, but it is necessary that these skills be also available to the staff who first come on the scene. The defense may call into question the accuracy and reliability of each method of gathering evidence and used tools. In order to ensure the admissibility of evidence gathered in this way, the police and the prosecution must, in case of need to perform forensic analysis of live systems, have proper knowledge and skills as well as proof of the validity of the tools used.

CONCLUSION

Traditional forensic approach, according to which the device is switched off and then a copy/ clone of hard disk is created in which the data is stored before any further analysis, is becoming unacceptable and impractical in some cases and considering the changes in the nature of computer systems investigator must rely on *in situ* search and review of a live working computer environment. Although this new approach enables collection of computer data that would otherwise be permanently and irreversibly lost and therefore unavailable for later analysis (especially information on the operating state of the computer at the time when it was approached), the legitimacy of live digital forensics can be brought into question. It carries a challenge in terms of whether the evidence collected in this way may lose credibility as they are not in compliance with the main principles of digital forensics which are supposed to secure evidence integrity and chain of custody. Although in the literature research on standardizing techniques of collecting volatile data from live systems may be found, a prevailing attitude is that the data collected in this way cannot be accepted as evidence in the court. As data and information obtained by this approach may represent a significant contribution to the investigation with great probative value, it is necessary to pay further attention to the effects and accuracy of these data collection techniques.

REFERENCES

3. Cohen M, Bilby D, Caronni G., „Distributed forensics and incident response in the enterprise", Digital Investigation 8/2011, 101–10.
4. Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (Washington, DC: July 2001) https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
5. First Responders Guide to Computer Forensics(CERT Training and Education Handbook, http://www.sei.cmu.edu/reports/05hb001.pdf
6. Grizzard J., Towards self-healing systems: re-establishing trust incompromised systems. Ph.D. thesis. Georgia Institute of Technology; 2006
7. Amari K, Techniques and Tools for Recovering and Analyzing Data from Volatile Memory, 2009, 40-50.

7 Cohen M, Bilby D, Caronni G., „Distributed forensics and incident response in the enterprise", Digital Investigation 8/2011, 101–10.
8 Grizzard J. Towards self-healing systems: re-establishing trust incompromised systems. Ph.D. thesis. Georgia Institute of Technology; 2006

UDC: 334.53:004”20”
007:004.056”20”

TECHNOLOGY AND SECURITY IN THE BEGINNING OF THE 21st CENTURY

Vojislav Gavrilovic[1]
Dragan Jevtic[2]

Abstract: War, as the most serious form of confrontation of people and materials, always forced humans to outsmart each other, to create new means and define new techniques for achieving victory. From catapults and crossbows to cruise missiles and combat robots, war (or at least fear of war) was that unfortunate catalyst of technological development. The destructive nature of war often stretched human creative potential to its limits. Many inventions initially created for military purposes, have later found an even wider use in the civilian sector.

In the 21st century, technology is advancing very rapidly, converting yesterday's fiction into today's reality. In fact, technological superiority has never been a more decisive factor in achieving military dominance than it is today. It gives the game changing advantage of an 'unfair fight' in which a technologically more advanced belligerent is almost sure to achieve victory, no matter how brave, trained or even numerous his opponent is. However, keeping the pace in this global technology race can prove to be challenging, especially for countries with modest economic capabilities. This means that in decades to come, only countries with strong economic basis will be able to ensure their armies are technologically up-to-date, and furthermore, be able to rely on advanced technologies safeguarding their national security. This restricted access to technology will continue to play a major role in the division of humanity.

This work is focused on the emerging technologies and their influence on national and global security in next several decades. We will try to cover some of the main technological innovations that transform and shape today's security doctrines, such as: increased robotization of combat systems, hypersonic weapons, cyber security and cyber warfare issues, drone evolution and other. I will also look into the ambitious projects of globally recognized technology pioneers such as the US Defense Advanced Research Projects Agency (DARPA) and the European Commission's Future and Emerging Technologies (FET), as well as their Russian and Chinese counterparts. Finally, we will try to conclude the work by describing the doctrinal effects that modern technology creates for armies of the 21st century.

Keywords: war, civilian sector, technology, robots, combat drones.

EVOLUTION OF UNMANNED AERIAL SYSTEMS

In the past decade the Unmanned Aerial Vehicle or UAV technology has become a part of everyday life. The UAVs have passed through the same path of evolution such as airplanes: first they were part of science fiction fantasies, then they became reality, at first in a reconnaissance role, then in a combat role and now they are becoming more autonomous through robotization. They are becoming smaller, faster, more sophisticated, more deadly and with multipurpose capabilities. And even though it seems that the US, Israel and a couple of other countries are the only ones in possession of combat drones, it can be expected that this technology will spread real far real fast. Defense One released an analysis in July this year according to which virtually every country on Earth will be able to build or acquire drones capable of firing missiles in the next 10 years. Even though this might be a bit exaggerated prognosis, it is obvious that drones are becoming more popular proportionate to their increasing operational capabilities. The recent report from RAND organization shows that (for now) 23 countries have developed or are in a process of developing armed drones and it is only a matter of time before this technology starts spreading. Once the Chinese military industry masters the process of producing cheap yet effective combat drones and starts exporting them to other countries, this technology will be virtually everywhere. And this proliferation of drones is not likely to be restricted or halted through current legal means. For example the MTCR (Missile Technology Control Regime) which could be used as a legal tool for control and restriction of combat drone proliferation was never signed by China. More importantly, armies around the world will not be the only ones interested in acquiring drones. A far greater threat comes from the possibility of non-state actors such as gangs or terrorist groups acquiring armed drones in the near future. Of course, these 'rogue' drones are not going to be

1 Student at master studies of terrorism, organized crime, security in Belgrade, vojislavgavrilovic90@gmail.com
2 Candidate at the Faculty of Political Science, University of Defense, Military Academy, Belgrade, jevta70@ptt.rs

as advanced as, for example, in today's terms, MQ-9 Reaper or X-47B are, but they could still pose a threat. For instance, recent conflicts in the Middle East showed the deadly use of low tech booby-trapped UAVs by Hezbollah. However, the power of conducting drone strikes anywhere on the globe will definitely remain a 'privilege' reserved for a few world powers.

Technological development of drones also opens a whole palette of new tactical and strategic potentials of these systems. This year's BAE System's Future Concepts program showed just a few amazing perspectives of drone development. The Future Concepts predicts use of revolutionary new technologies in drone production in relatively near future, more precisely by 2040. One of the main ideas behind the Future Concepts program is the development of robotic modular drones, organized into completely independent and versatile combat formations, able to conduct a multitude of different tasks on their own. Such concepts could transform the future of warfare in a fundamental way and it seems it is just a matter of time before armies start fighting each other through use of drone fleets, minimizing human losses (as a reminder, it seems the most probable theatre for such a 'drone showdown' is the Pacific region in which both China and Japan are rapidly developing their combat and reconnaissance drone capabilities along with worsening relations due to territorial disputes). BAE Systems presented several of those futuristic technologies. For example, in a project called 'Survivor', the scientists of BAE systems are experimenting with the use of adhesive liquid placed into a sort of mechanical 'bloodstream' of the drone. In the event of being hit by anti aircraft fire, this adhesive liquid would automatically 'patch' the damage on the fuselage of the drone. Another interesting project from Future Concepts is called the 'Transformer' and is based on the idea of building a long range drone consisting of several smaller ones capable of detaching from the mother drone. Each of these smaller drones would have a different role (for example: transport, combat, scout, etc.) and the whole system would be capable of assembling and disassembling in flight. And if this does not sound like the 'Star Wars', the project called DES (Directed Energy Systems) certainly does. DES incorporates the use of high power combat lasers into drone systems. Such lasers could be used for intercepting enemy aircraft and missiles. However the practical difficulties in developing this kind of weapons are related to finding adequate energy sources for providing lasers with enough strength and range to be effective. It is obvious that drones are platforms capable of incorporating various additional technologies. It should come as no surprise that in near future drones could be equipped with their own 3D printers. This would allow future drones to produce their own fleets of mini support drones based on the mission requirements. The potentials seem endless and not just for the military purposes. Drones are finding more and more use in civilian sector in every coming year, ranging from pizza delivery and agriculture tasks to monitoring wild fires and climate changes. Especially interesting and useful are the ideas of developing large cargo transport drones for civilian purpose. Of course, making precise predictions of future technologies is never easy, especially bearing in mind that even the less ambitious projects such as the F-35 Lightning II are proving hard to realize and that many projects that are highly futuristic turn out to be highly costly, technically problematic and of questionable practical value. However, some of the mentioned projects are sure to come into the zone of technical possibilities in decades to come.

This year's novelties in the UAV field were shown in AUVSI 2014 drone fare. The projects are numerous – from microdrones resembling insects, bats and leaves to hybrid drones possessing a combination of conventional (horizontal) drive and multirotor engines allowing vertical take-off and landing (VTOL). Such multirotor drones will have a great advantage in combat role because they are able to hover above the target and achieve maximum precision position before taking action, thus reducing the possibility of collateral damage. Another emerging technology involves submarine-launched drones as well as unmanned submarines which could combine into effective unmanned maritime and airborne task forces. The US Navy already conducted a successful test of a vertically launched drone from USS Providence submarine in December of 2013 and DARPA is already working on the development of unmanned submarines. Furthermore, DARPA's research of the so called 'atomic GPS' could provide drones with navigation systems that do not require satellite communication, making them far less hackable. Apart from this, the US Army is already conducting experiments aimed at equipping drones with electronic warfare systems and jamming devices. On the other side of the globe, the Russian Innoprom 2014 fare presented a so far unique hybrid amphibious UAV called 'Chirok'. This UAV does not require airfield of any sort for launching and it is capable of carrying 300 kilograms of deadly payload in internal bays. The mass production of this drone is expected to start in 2016. Another revolutionary technology has been demonstrated by the Norwegian company called the Prox Dynamics which presented its upgraded version of the nano-drone PD-100 Black Hornet. This 10 cm long helicopter drone, which first entered service in the British Army in 2012, has finally been equipped with night vision capabilities this year, significantly improving its overall usefulness on the battlefield. In the final weeks of 2014, more precisely on December 22, DARPA (Defense Advanced Research Projects Agency) put out a broad agency announcement seeking software solutions to help small drones fly better in tight enclosed environments. The project is called Fast Lightweight Autonomy program and is focused on creating a new class of algorithms to enable small, unmanned aerial vehicles to quickly navigate a labyrinth of rooms, stairways and corridors or other obstacle-filled environments without a re-

mote pilot. If this project ends successfully, it will open a whole new dimension of military reconnaissance, based on smart, insect-like spy drones.

The drone technology has become a necessary tool for any modern army's arsenal and is now rapidly penetrating into the civilian sector as well. Drones are being used for various tactical and strategic tasks by numerous and various entities, from USAF to Hezbollah, and for various tasks, from assassinating high ranking terrorists to monitoring spread of Ebola. Despite doubts expressed by some experts at the early stages of UAV development, drones have greatly exceeded their initial expectations and their importance and capabilities will only continue to grow in years to come. As Richard Whittle mentioned in his new book Predator: The Secret Origins of the Drone Revolution: "Drone technology has already changed the way people die, one day it may change the way people live."

HYPERSONIC WEAPONS

Development of hypersonic weapons is probably one of the most interesting and important processes in the field of military technological innovations in 2014. Indeed, it was a busy year for rocket scientists across the globe, especially for Chinese and American ones. In the beginning of December, China successfully conducted its third test of its hypersonic glide vehicle this year, code-named Wu-14 by Pentagon. Wu-14 had its first successful flight on January 9 this year, while its second test conducted in August resulted in a crash. Simultaneously, the US tested its Advanced Hypersonic Weapon (AHW) from the Kodiak Launch Complex in Alaska on August 25, which also resulted in failure. The very frequency of these tests on an annual basis signals the ongoing military competition between the two countries, which could easily evolve into a global hypersonic arms race, as Russia and India are joining in the effort to master this technology.

But what are hypersonic weapons anyway? There is a lot of confusion about the nature of these weapons even among the professional circles. The fact that hypersonic weapons have been among us in some form for decades only makes the confusion deeper. Hypersonic flight is typically defined as traveling at speeds of Mach 5, five times the speed of sound, or above. Intercontinental ballistic missiles, or ICBMs, are a well known type of hypersonic weapons. However, these ICBMs follow a ballistic arc up out through space, while the new hypersonic systems like the American X-51 or Chinese Wu-14 fly at five or more times the speed of sound *in the atmosphere*.

Hypersonic missiles fall into two distinct categories. In what is known as a boost-glide weapon, the hypersonic vehicle is first 'boosted' on a ballistic trajectory, using a conventional rocket. It may cover considerable distance as it flies to high altitudes, then falls back to Earth, gaining speed and finally, at some relatively low altitude, pulling into unpowered, aerodynamic, horizontal flight. After that, it glides at hypersonic speed toward its final destination. Hypersonic cruise missiles, on the other hand, are typically launched to high speed using a small rocket, and then, after dropping the rocket, are powered by a supersonic combustion ram jet, or scramjet, for flying at five times the speed of sound or faster. These hypersonic scramjets, like other jet engines, are 'air-breathing', meaning they burn their fuel by mixing it with oxygen from the atmosphere. On the other hand, ballistic missiles and satellites launched on rocket boosters must carry their own oxidizer with them. This makes hypersonic scramjets a lot smaller compared to ballistic missiles, meaning they can be launched from a variety of combat platforms, possibly even 5th generation fighter planes in the near future. The recent Chinese and American tests were of boost-glide systems, while the X-51 WaveRider, which the US successfully tested last year after a series of failures, is an example of the scramjet cruise missile. China plans to deploy its high-speed glide vehicle by 2020 and a scramjet powered hypersonic vehicle by 2025. In fact, the People's Liberation Army is developing hypersonic glide vehicles as a core component of its next-generation precision-strike capability.

Probably the greatest advantage of hypersonic missiles over their ballistic counterparts is their stealthiness and maneuverability. A ballistic missile launch is so bright and hot that it can easily be seen from space. The US has an entire network of satellites to do just that. Furthermore, once the booster cuts off from the ballistic missile, the warhead and its 'reentry vehicle' cannot *change the course.* They are stuck following a ballistic curve (hence "ballistic missile") which is easily predictable and countered by missile defense shields. On the other hand, scramjet hypersonic missiles like the X-51 also require a booster rocket, but a much smaller one, enough to reach Mach 4.8 rather than to exit the atmosphere. Then, once the X-51's scramjet engine takes over, it burns much less intensely but continuously, providing thrust throughout the flight. The end result is that a hypersonic missile has a much more complicated trajectory which brings it to its target extremely fast, making it much less detectable and much more maneuverable than a ballistic one.

Even though most people see hypersonic weapons as new delivery vehicles for nuclear warheads (especially after China confirmed that testing of Wu-14 was part of its strategic nuclear programme transformation), it is less known that hypersonic weapons may carry conventional instead of nuclear warheads. In fact, they may not carry warheads at all, as the pure kinetic energy generated by the awesome speeds of their

flight creates a powerful destructive force. This means not only that these weapons are 'ecology friendly', but - more importantly – their proliferation may not be controlled by any existing legal acts regarding nuclear weapons.

Development of hypersonic weapons entered its present phase when the Pentagon underlined its need for faster conventional weapons back in 1998. The well known example that explained the need for such weapons described the following situation. Osama bin Laden had been spotted in a terrorist training camp in the east of Afghanistan, but when Tomahawk missiles (capable of travelling at 880 kmph) were dispatched to kill him from a warship in the Arabian sea, the Al-Qaida leader left before missiles arrived to hit the target. This led to defining the so-called 'Prompt Global Strike' doctrine, which would allow the US Army to deliver precision conventional weapon strike anywhere in the world within one hour. However, this doctrine and, above all, the hypersonic weapon systems which it brought into life, raised concerns not as much among the Taliban as among officials in Moscow and Beijing. When Boeing X-51 WaveRider hypersonic scramjet was successfully tested in May 2010, Russian experts warned that these weapon systems, scheduled for mass production in 2015, may turn into a real threat, as they are unstoppable for old Russian S-300 and S-400 ballistic missile defense systems. In fact, even though the Prompt Global Strike doctrine is officially aimed at rapid neutralization of terrorist camps and individuals, Russian military already conducted analytic simulations in which thousands of hypersonic weapons were launched at Russia, mostly across the North Pole. It is hard to tell how far the Russian hypersonic weapon programme had gone compared to the Chinese and American ones, however many Russian experts, as well as President Vladimir Putin, underlined that the Russian answer to hypersonic weapons will be asymmetrical. Putin also stated in spring of 2004 that the Russian army will be equipped with highly maneuverable hypersonic weapons and Deputy Prime Minister of Russia Dmitry Rogozin confirmed this in his statement from October 2013 when he said that Russia was testing hypersonic weapons in utmost secrecy, adding that the experiments were planned to be finished in December 2014. Finally, the Russian government has announced that Moscow plans to field hypersonic missiles by 2020.

Despite Russian concerns, Pentagon officials are still not impressed with the level of development of their Prompt Global Strike capabilities. Simple mathematics says that even a Mach 5 missile (like the X-51 WaveRider) would take almost an hour to get from, for example, the US bases on Okinawa to the Chinese space facilities in Xinjiang, which is not fast enough. The simple vastness of the Asia-Pacific theatre demands even faster missiles. "Mach 5 doesn't buy you anything," said Robert Stein, a member of the Pentagon's Defense Science Board. "If you really want to get up into a regime where it is really helping, double that number. Now you're starting to talk," and really starting to get into some futuristic engineering. As usual, the home of that futuristic engineering is DARPA, whose scientists are working on hypersonic vehicles capable of reaching incredible speed of Mach 20.The first such project was DARPA Falcon Project (Force Application and Launch from CONtinental United States) which resulted in partial success after two tests of Hypersonic Test Vehicles, paving the way for a new project called 'Integrated Hypersonics'. The goal of the Integrated Hypersonics programme is to develop, mature, and test next- generation technologies needed for global-range, maneuverable, hypersonic flights at Mach 20 and above for missions ranging from space access to survivable, time-critical transport to conventional prompt global strike. This means that such hypersonic vehicles would not only be used to dispatch warheads around the globe extremely quickly or to launch satellites into the orbit, but also to deploy small groups of troops, probably elite special force. This opens a whole new palette of tactical aspects of future use of hypersonic weapons.

On the other hand, new ideas for defense against hypersonic weapons are emerging. It is obvious that ballistic missile shields of today are useless against hypersonic weapons of the future. Futuristic threats demands futuristic answers. Some of those answers are based on the use of directed energy weapons, such as a hypersonic capable rail guns or lasers. Such hypersonic rail guns would work like huge anti aircraft shotguns, launching hundreds of tungsten pellets in the direction of the coming hypersonic warhead. A more sophisticated solution is based on the use of high precision lasers capable of shooting down aircraft even at hypersonic speeds, however lasers of such range and strength are still not developed.

In the end, it must be said that this heated hypersonic arms race could in fact be terminated by a simple legal ban on testing and development of hypersonic weapons. Hypersonic weapon critics suggest that these systems have no foreseeable civilian role, no likely military role outside a major war between nuclear superpowers, and that they contribute to strategic destabilization and even possible nuclear Armageddon, as a conventional hypersonic missile launch could easily be misinterpreted as a nuclear attack. However, it seems that the last realistic opportunity to ban hypersonic weapons has been lost with the decline of relations between the West and Russia over Ukraine crisis. This unfortunate geopolitical event has led the world into a new type of Cold War, along with new arms race in which hypersonic weapons will probably have a major role.

RAPID PROTOTYPING AND 3D PRINTING

We are living in a time when the rate and scope of change in the battlefield operating environment is, at the very least, spectacular. Modern warfare is forcing many of the western armies to quickly adapt to rapidly evolving asymmetric threats in an effort to maintain tactical situational awareness. Yet it often takes years, sometimes even decades, to develop systems and technologies needed for these adaptations. That is where rapid prototyping fits in.

Rapid prototyping is a group of techniques used to quickly fabricate a scale model of a physical part or assembly using three-dimensional computer aided design (CAD) data. Construction of the part or assembly is usually done using 3D printing or "additive layer manufacturing" technology. This literally means transforming digital models into physical objects. The first methods for rapid prototyping became available in the late 1980s and were used to produce models and prototype parts. 3D printers are now used extensively in engineering, architecture and product design and now they are being embraced by the military, especially in the US army. Weapons like the Enhanced Sniper Rifle XM2010, or the sophisticated Boeing Phantom Ray UCAV are all results of rapid prototyping techniques. Rapid prototyping is becoming a more and more prominent tool of modern military engineering, faster and cheaper than traditional methods and irreplaceable in conditions where military needs are constantly being changed by the ever evolving battlefield challenges. This process is further perfected by adding the use of Finite Element Analysis (FEA) software which simulates the extreme conditions of the battlefield (such as high or low temperatures, vibrations or high pressure and others) in which the prototype durability and effectiveness need to be tested. This allows testing performance attributes of a product and its materials in a virtual environment before anything physical is manufactured.

As mentioned before, the US military has given more attention to rapid prototyping than any other army in the world. In July 2012, first rapid prototyping expeditionary labs were shipped out to American troops in Afghanistan in order to provide the ability of creating and modifying weapons and tools on the very frontlines. Each of those labs was built out of a standard 20-foot (6m) shipping container at the cost of some $2.8 million. They contained the following equipment: a conventional 3D printer (for plastic), an industrial CNC machine (steel and aluminum), plasma cutters, welders, routers, magnetic mounted drill presses, circular saws, jigsaws, electric hacksaws and satellite communications technology. All of those are operated by just 2 engineers per lab and if need arises, the whole lab can easily be transported by a helicopter to another location. But that is not all. In order to cut the costs of acquiring spare parts for weapons and equipment, the US military is currently developing its own rapid prototyping device. This small 3D printer is cheaper and lighter than the existing models and can replicate parts for the sensitive instruments and systems used by the military. This ambitious and futuristic project is being developed in the Future Warfare center at Space and Missile Defense Command in Alabama. Scientists of this institution are developing a 3D printer as an alternative to current commercial models. Their early prototype costs $695, compared to $3000 for a commercial printer and it is small and light enough to fit into a soldier's backpack or a "humvee" trunk.

It is obvious that this technology is revolutionary. These small devices could easily replace the massive manufacturing and logistics military chains in decades to come. Furthermore, use of such technologies could create conditions for experimentation and innovation throughout the military directed from the soldier up, rather than from the higher echelons down. On the other hand, new dangers could easily arise from this. Some gun hobbyists across the US have already successfully fired semi automatic AR-15 rifles using 3D printed parts. Further development and availability of 3D printing could allow people to literally print ammunition in enormous quantities. In the end, why not ask ourselves how much time would have to pass before a crime such as murder is done with the use of 3D printed weapon? Of course, these and other potential threats of 3D printing technology should not discourage or halt its further development, but inspire a timely defining of legal framework for future wide use of highly capable 3D printers.

CYBER WARFARE AND THE DIGITAL COLD WAR

The revolution of information technologies, as well as the radical increase in number of networked platforms has made cyber space one of the most important aspects of today's humanity. According to the Global Internet Report 2014 released by the Internet Society, there will be near 3 billion internet users in early 2015 and for the first time, the number of users from developing countries has exceeded the ones from developed countries. But not only numbers are increasing. The quality is increasing as well. Users migrated their fixed Internet access from dial-up to broadband, from fixed to mobile connection platforms such as smartphones and their usage shifted from text-based to predominantly video traffic, creating a new, multimedia generation. The Internet and the cyber space in general, have changed the world and will continue to do so. Thanks to cyber space, the whole knowledge of mankind will be available to every individual on

the planet in the coming decades. Open access to the Internet has revolutionized the way individuals communicate, entrepreneurs and corporations conduct business, and governments and citizens interact. At the same time, the Internet established a revolutionary open model for its own development and governance, encompassing all stakeholders.

Many nations are trying to adapt to this new reality and their aims and interests are now reflected in cyber space. And this does not mean 'high tech' nations only; in fact, cyber space offers unique opportunity for weaker and technologically less developed nations to catch up with the world powers in the context of a more and more valued resource – knowledge. The fact that cyber space is not only space, but even more activities in it, gives nations the right to manifest their sovereignty in its parts. For example, French cyber defense national strategy declares that information systems security is an area in which the sovereignty of France should be fully expressed. The United States and Russia have gone even further, concluding that computer sabotage coming from another country can constitute an act of war, meaning that these countries could respond with the use of traditional military force and even their nuclear arsenals in case of a full-scale cyber attack on their crucial networks and digital infrastructure. In 2009, the United States formed the Cyber Command (USCYBERCOM) as an armed forces sub-unified command subordinated to the United States Strategic Command. 'Cyber warriors' in the US military today number some 5000 personnel. The Global Information Grid (GIG) used by the US Army consists of approximately 7 million computers connected by some 15000 local and regional networks. On the other side of the globe, the Russian army and Russian security services continue to demonstrate high priority of cyber warfare capabilities. Russia's rapid and successful annexation of Crimea was greatly assisted by teams of the Russian Special Operations Forces (Spetsnaz) and other troops, supported by a variety of cyber warfare activities: from manipulating online social networks to disrupting regional computing and hacking enemy drones. The situation is somewhat different in NATO. The NATO cyber defense policy is primarily focused on the defense of communication systems owned and operated by the Alliance, while the protection of national critical infrastructures remains a national responsibility which requires nations to invest resources in developing their own capabilities. For the purpose of research and training in cyber security, the Alliance formed the Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia. There are some 40 staff members working in this Center and 11 NATO member states are involved in its work.

In the environment of insufficient international legal regulations regarding cyber space behavior, as well as numerous opportunities for aggressive achievement of national interests in cyber space, individuals, groups and states have developed ways of abusing the possibilities offered by the cyber space, out of which the most serious form is cyber warfare. Today, the effects of cyber attacks can have similar or even the same results as military attacks with the use of physical force, not only can they sabotage armies, but also cripple a nation's ability to function as a state. Regarding this possibility, Hamadoun Toure, the UN International Communication Union Agency's secretary-general, stated in Geneva 2009 annual conference that "the next world war could easily be a cyber world war, which would have disastrous consequences." The primary advantage of cyber warfare is its cheap and stealthy nature. In fact, in today's security, small teams of specially trained and equipped cyber Special Operations Forces can affect strategic outcomes more than much larger units of conventional forces. The combination of economic and cyber warfare can be especially damaging for developed countries, with hacking of stock exchange market systems being just one of the examples. This brings us to the conclusion that, in the coming decades, cyber warfare will become a very attractive option for small nations that are trying to achieve their interests in collision with the interests of world powers. For economically and technologically weak nations, cyber warfare is already a great alternative to conventional weapons. It is cheaper and far more accessible to these small nation-states and it allows these countries to pull off attacks without as much risk of getting caught or suffering repercussions. This will give a whole new dimension to an already dynamic 'digital cold war' that is being waged between the world's super powers.

Cyber warfare may still sound as science fiction to some people (even though there are plenty examples of its realistic nature such as the Stuxnet operation, Israeli operation that destroyed Syrian Al Kabir nuclear reactor in 2007, hacking of US drones by Iranian specialists and Iraq rebels, etc), however cyber warfare is already our reality and is characterized by its own forces, means, methods, aims and results. In the era of network-centric operations aimed at manipulating friends, foes and neutral subjects in situations of peace, crisis and war (or simply – everyone always) through force that is rarely traditional military force, but more often the force of ideas, cultures, information, media, economy, law, and other 'soft forces', cyber warfare is bound to have a role of utmost importance, as cyber space combines all of the mentioned and more, offering unique strategic capabilities.

CONCLUSION

The size of this work prevents us from analyzing other important technological innovations related to security and defense, such as cyborgization of soldiers, space elevators, militarization of the Low Earth Orbit, 5th and 6th generation fighter aircraft and other. However, even with the ones incorporated into this work, it can be concluded that the main characteristic of these new systems is speed. In fact, the speed of intervention which these new technologies will allow is likely to shrink the time of operations into a moment in the coming decades. Military commanders of the future will have to make decisions instantly, opening an era of 'instant warfare' doctrines. This means that militaries around the world will have to rely on predefined doctrines, measures and procedures, more than ever before, as the time for improvisation will shrink to the point of disappearance. This is especially the case with cyber warfare as it takes place in time instead of space, meaning it requires instant reactions. As a result of this request for speedy decision making, the need for expensive and sophisticated automated and robotized systems will continue to grow, again putting economically weaker nations into inferior position.

On the doctrinal level, this 'instant warfare' threat will force many nations and especially super powers to take a more proactive stance in their defense and security, relying more aggressively on prevention instead on reaction. This transformation could especially be boosted by proliferation of hypersonic weapons, as the nature of these weapons gives no room for strategic patience. Ultimately, with the lack of an improved international legal framework for the new reality of warfare, as well as geopolitical confrontations opened with the era of multipolarity, the risk of strategic destabilization is bound to be increased with the incorporation of these new and dangerous military technologies.

REFERENCES

1. Mladenovic, Dragan. International aspects of cyber warfare
2. Tucker, Patrick. How technology is transforming the future of national security, Defense One e-book, July 2014
3. Whittle, Richard. Predator: The Secret Origins of the Drone Revolution
4. http://www.nextgov.com/?oref=ng-logo
5. http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/
6. http://sptimes.ru/story/41307?page=4#top
7. http://freebeacon.com/national-security/china-confirms-third-test-of-hypersonic-missile/
8. http://thebulletin.org/argument-hypersonic-missile-testing-ban7412
9. http://www.pecat.co.rs/2011/02/rusija-sad-hipersonicna-trka-u-naoruzanju/
10. http://www.extremetech.com/extreme/134808-us-army-sends-rapid-prototyping-labs-to-afghanistan-prepares-to-battle-insurgents-with-3d-printed-equipment
11. https://www.wikipedia.org/
12. http://www.defenseone.com

UDC: 343.533::004“20“

CYBER CRIME SCENE IN 21st CENTURY
MALICIOUS HACKERS AS MAIN ACTORS

Igor Cvetanoski[1]

Jugoslav Ackoski[2]
Military Academy “General Mihailo Apostolski”, Skopje
Dejan Rancic[3]
University of Niš, Faculty of Electronic Engineering

Abstract: Research subject of this paper is cyber crime and its influence on personal, national and international security. The aim of this topic is to discern cyber crime as the most frequent form of the 21st century cyber threat. Research motive for cyber crime as the 21st century security threat was its ability to adjust to modern environment and to evolve continuously. As any other criminal activity, cyber crime shows the necessity of institutions to keep up with the progress of modern information technology and to increase personal and social awareness of this phenomenon. Globalization of cyber space has caused new risks and threats to personal privacy, electronic systems and data security.

Analyzing the accessible literature on cyber crime, there will be shown some definitions of cyber crime, its characteristics and goals. Furthermore we will underline the motives of cyber criminals and the methods of cyber crime. Next, there will be some examples of cyber crime that occurred in the world in the 21st century. Finally we will mention the institutions, measures and actions to counter cyber crime in the Republic of Macedonia.

According to prevention, we will state that it depends on many aspects, but some of them are: precisely defined international legislation in correlation with national legislations; international cooperation; cyber crime information gathering; sharing of information; establishment of the Computer Emergency Response Team (CERT) defined in the national security strategy; the CERT's employees who will be experts in this area; international cooperation among the national CERTs in specific cases and sharing of experience, etc.

Today modern technology provides great opportunity to use online tools in cyber crime activities.

Key words: crime, threats, cyber, hackers, cyber criminals, malware, CERT, gathering and sharing of information.

CONCEPTUAL DETERMINATIONS OF RESEARCH SUBJECT

The term crime is defined in many ways which depends on the type of a dictionary, so it is known to have multiple meanings. Some of them define this term as action or omission which constitutes an offense and is punishable by law; illegal activity; activity which is considered to be shameful, malicious or wrong; activity which represents a serious offense against the individual or the state and is punishable by law and so on. Crime has always posed a threat to the security of ordinary people in the society, and sometimes also for the state institutions. Lately this has become a greater threat whose nature has been transforming every year while undermining the capacity of governments to protect their citizens and themselves.[4] The meaning of the term threat in social sciences and dictionaries can be found in several definitions and meanings. One definition says that the insecurity of the state is defined by the threats which determine the agenda for national security as a policy issue. They vary in scope and intensity, pose risks that cannot be accurately estimated and depend on the probabilities which cannot be calculated.[5]

According to the Internet Corporation for Assigned Names and Numbers (ICANN) from the USA, every computer on the Internet has a unique numeric address which is similar to the uniqueness of a telephone number and which is a string of numbers that is difficult for most people to remember. This string is

1 Student of MSc studies in the field of Defense and Security, Military Academy “General Mihailo Apostolski”, Skopje, Associate member of “Goce Delchev” University, Štip, igorcvetanoski@yahoo.com
2 Associate member of “Goce Delchev” University, Štip, jugoslav.ackoski@ugd.edu.mk
3 dejan.rancic@elfak.ni.ac.rs
4 Питер Хју (2006). *Поим за глобална безбедност*.Скопје 2009: Табернакул, 258.
5 Бери Бузан (1983). *Луѓе, држави и страв.* Скопје, 2010: Академски печат,112.

called the Internet Protocol (IP) address. The Domain Name System (DNS) was invented in order to make it easier to find a given location on the Internet. The DNS translates IP addresses into unique alphanumeric addresses called domain names that are easier to remember than IP address. According to one of many definitions of Michael Benedikt published in MIT press in 1991, cyberspace was defined as a "new universe, which is parallel universe created and sustained by the world's computers and communication lines". In the context of cyber space often we can run across the notion virtual which can be explained as something that does not exist physically but with the help of software is becoming real.

Cyber crime encompasses any criminal act relating to computers and networks. Cyber crime in its broadest sense means the offenses of criminal laws of nation states that in any way involve computer systems and networks. The most common types of cyber crime are: theft of computer services; unauthorized access; software piracy; disclosure, theft and alteration of computer data and information; extortion using a computer; unauthorized access to a database; misuse of stolen passwords; child pornography; transmission of destructive viruses; industrial and political espionage.[6]

Nowadays there is no universal definition of the term 'terrorism'. Definitions of the term 'terrorism' have different backgrounds, so while some of them focus on terrorist actors, the others focus on terrorist tactics, goals and methods. According to the Federal Bureau of Investigation (FBI) of the United States, the new phenomenon known as cyber terrorism is defined as "pre-planned, politically motivated attack against information, computer systems, computer programs and data that result in violence against non-military targets (civilians) from non-state actors or clandestine agents".[7] The physical and the virtual world are diametrically opposed to each other. The correlation between these two independent worlds form cyber terrorism, new weapons with which modern technologically developed societies face.

Cyber sabotage includes the attacks which destroy vital equipment or control systems in such a way that was the worm Stuxnet. That is achieved by using a malicious code with overheating of central processor unit (CPU) of the computer or by causing the coupling of feedback to damage the operating cycle.

Cyber war is fought in the virtual world of computers, computer systems and networks. The goal is to rule the computer systems and networks. Offense and defense are conducted by the intrusion, infiltration and other active and passive methods, which consist of obstruction, disinformation or destruction of communication systems.

The strategy of information warfare is based on defense and attack on information and information systems. Although these techniques have always been part of the war, the importance of this form of conflict was drastically increased with the advent of computers and the Internet revolution in recent decades. Today it is an accepted fact that cyber war is a vital part of the current military operations and such attacks can be a potential strategic vulnerability of critical infrastructure of nations.[8]

CYBER SECURITY RISKS AND THREATS

The sources of cyber threats are ranging from states to private individuals. The difference is in: the damage, the extent of the threat of cyberspace, the level of threat; the subject who was destroyed, threatening the security (personal, collective or national), the motivation for which cyber attack is made, the cause of the cyber threat, etc. In this context, the actors of cyber attacks are:

1) States – use cyberspace and by using information resources gather information and conduct: espionage, disinformation, destabilization, intimidation or full cyber war.
2) Corporations – sometimes in collaboration with organized crime groups or individual hackers conduct industrial espionage and/or sabotage.
3) Malicious hackers – in the past, hackers had entered into computer networks because of prestige in the hacker community. Today, malicious hackers' motives are criminal, and changing to the most extreme forms of terrorism using cyber space.
4) Haktivists – haktivism refers to politically motivated attacks on websites or server's emails. The purpose of haktivists is to disrupt damage or destroy web sites in order to achieve political goals.
5) Disgruntled insiders – whose goals are to cause damage to the system or to steal sensitive data. According to the Federal Bureau of Investigation (FBI) in the United States, insider attacks are twice more likely than the attacks by strangers. In this context social engineering has increasingly been

6 Милосављевић,М. и Грубор,Г. (2009). *Истрага компјутерског криминала – Методолошко технолошке основе*. Универзитет "Сингидунум" – Београд, 291. Downloaded on 15th of December 2013. http://www.seminarski-diplomski.rs/biblioteka/Istraga%20kompjuterskog%20kriminala.pdf.

7 Achkoski,J. and Dojchinovski,M. *Cyber terrorism and cyber crime – threats for cyber security*. Military Academy "General Mihailo Apostolski" – Skopje. Proceedings of First Annual International Scientific Conference, Makedonski Brod, Macedonia, 09 June 2012. Downloaded on 16th of December 2013. http://eprints.ugd.edu.mk.

8 Роберт Ц. Бункер. (2003). *Не – државни закани и идни војни*. Скопје (2009): Нампрес,101.

applied. This method exploits the weakest line of defense of any organization – people. As a new trend, in foreign literature this term is known as people hacking where the trust of people is abused for personal gains.[9]

6) Terrorists – are people who want to destroy, disable or use critical infrastructure, endanger national security, cause mass casualties, weaken the economy and disrupt public morale and confidence. Although many terrorist groups currently do not have the capacity for cyber attacks, still there is no guarantee that they will not have it in the future.[10]

7) Phishers – are individuals or small groups of malicious hackers who stole identity or information with a fraud for personal gain (in the majority of cases for money).

8) Botnet operators – are malicious hackers who take control of a lot of computers and then use them for coordinated attacks, phishing, and spamming or for other malicious attacks.

9) Spammers – are individuals or organizations of malicious hackers who distribute unsolicited email (spam), as it solds products (often with hidden or false information).

10) Authors of spyware and malware – are individuals or organizations that create programs and codes of malicious software that are later used for cyber attacks on users of the system.

11) Pedophiles – are individuals who are more likely to use the Internet to exchange child pornography and find victims (using programs, social networks and online forums).

Malicious hackers led by different motives and reasons perform cyber attacks by malicious software/ programs (malware). Malware or malicious software is a harmful program that infiltrates computers in order to manage hidden everything on the computers: download or upload files, request confidential information, run certain programs, delete data, etc. When talking about malware, we are thinking of viruses, worms, spies, Trojans, rootkits, etc. Some malwares which are used for cyber attacks are the subject of research in this paper.

Viruses are computer programs that are usually hidden in seemingly simple programs, and usually carry a harmful work (as destroying data). These are programs that replicate themselves in other files they come in contact with. In order to function, almost all viruses are attached to an executable file. It is important to emphasize that without human action, such as starting the infected file, the virus cannot run and play, which means that a virus may exist in the system, but cannot infect it unless it is started by a user. Some viruses are capable only of boring effects, while others may do irreparable damage to hardware and software. Usually the effects of them are: deleted files, corrupted programs, disputed disfunctional system and the like. The bright side of all of this is that if the user was doing regular BACK-up of the data, they will easily be recoverable and the problem will be solved without major consequences.

Worms usually are small self-contained and self-replicating computer programs that attack computer network and very often do destructive actions. According to the design they are similar to viruses, but differ in the concepts and techniques they use to spread. Unlike viruses, worms have the ability to spread out without assistance. They are compromised of self-copied code that allows their spreading, propagation and load (payload). In most of the cases, payload does not have any function and it only serves for dissemination. But in other worms it serves for malicious purposes such as spamming, opening backdoors, denial of service attacks, damage and the like. The biggest problem with worms is their ability to multiply quickly in the system. So instead of distributing only one copy of the worm, the computer can simultaneously send hundreds of copies to other computer systems. Because of this ability worms consume too much memory bandwidth and thus slow down the system and the network until it becomes unusable. In most of the cases it is not a serious obstacle and it can be removed quickly after its notification.

Trojans or Trojan horses are seemingly useful computer program that contains hidden instructions that when activated, perform illicit and harmful things in the computer. The problem in this case is that the programs which are present in the system are not noticed through some of the symptoms that are common for viruses and worms as downtime and inoperability of the computer system or network. They can be active for long periods and the system without noticing any damage.This is the reason why the notification of Trojan infection means it is too late to react. The reason for the large number of computers infected with Trojan horses is not in their software capabilities, but in the reluctance of users who open the infected files without any awareness of the consequences which Trojans could affect on the system.

Spyware or Spies is software that is installed on the computer without user's knowledge and transmits information about the activities of the user's computer via the Internet.

9 Beaver, K. (2010). *Hacking For Dummies, 3rd Edition*. Wiley Publishing, Inc. 111 River Street Hoboken, NJ, 386. Downloaded on 16th of December 2011. http://www.dummies.com/cheatsheet/hacking

10 United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity," *Science* 326 (13 November 2009): 943-4; See Martin Charles Golumbic, Fighting Terror Online: The Convergence of Security, Technology, and the Law (New York: Springer, 2007).

Adware is installed software that provides information about the habits of the user for browsing the Internet, thereby allowing the opponent to find out targeted goals.

Backdoors avoid normal security control and allow the attacker unauthorized entry in the system or computer.

Rootkits are tools of Trojans that modify the existing software operating system with which the attacker can enter, maintain and hide in your computer or network.

Sniffers are applications used to monitor and analyze the traffic in a network.

Malwares' ability is to do some of the following things:

– theft of private data, photos and documents;
– stealing passwords and e-mail accounts;
– theft of credit cards, business plans and projects;
– espionage, monitoring and surveillance;
– creating networks of bots;
– spread of viruses, worms and other harmful programs;
– slowing down the computer
– download and upload data;
– rename, redeployment and deletion of data;
– corrupting and disrupting the work of some programs;
– falsification of records to download software, music and movies;
– remote assistance;
– formatting the computer;
– Playing with sound, keyboard, screen and web camera and so on.

Overall, malware analysis is an interesting and challenging existing topic in the field of computer security. Complexity of this analysis is only one area of the work of professionals who deal with this issue.

MALICIOUS HACKERS ROLE IN PERFORMING CYBER ATTACKS

Nowadays, cyber attacks are performed by so called malicious hackers, who are nothing else but criminals, also known as cyber criminals, cyber terrorists and so on. There basic aim is to penetrate into a computer, computer network or system through cyberspace, with the ultimate objective of disruption of the system stability, taking over control of the system (zombie system), episode of refusal of services, stealing of personal data, stealing of the monetary funds from their own accounts, propaganda, spying, changes to data, abuse of Critical Infrastructure and many other criminal activities with the help of malicious software (viruses, worms, etc). Malicious attackers include two concepts: malicious hackers and malicious users. Malicious users (mostly disgruntled insiders) are internal attackers in an organization that compromise computers and sensitive information from within as authorized and trusted users.[11]

Unlike malicious hackers, ethical hackers hack into systems to discover vulnerabilities and protect the system from unauthorized access, improper use and abuse. This means that they use the same software tools and techniques as malicious hackers do to discover security vulnerabilities in computer networks and systems, while their activity is known by the owner of the network or system.

So called security deserves attention of researchers in the field of information technology (IT), which are publicly known IT professionals with extensive technical knowledge. They not only observe and follow the weaknesses of computers, computer networks and applications but also writing tools and codes to use. If there are no such persons, there would not have been testing tools from open sources. Persons in charge of Information Security often visit blogs, columns in newspapers and emails of these security researchers in the IT sector. Thanks to their research, the security of computer systems is up to date and upgraded.

Hackers consider themselves elite based on merit and knowledge. The more you do the greater respect you will achieve. There is no written hacker ethic as an official document, but the closest to that term is one that is determined by Steven Levy, who in 1984 wrote his book "Hackers: Heroes of the Computer Revolution", pointing out the following six basic principles:

– Access to computers and to what cannot be learned about how the world works - should be unlimited and full.

11 Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler. Демократско управљање изазови сајбер безбедности. Downloaded on 15 December 2013. http://www.fbd.org.rs/akcije/POJEDINACNE/CYBER%20ZA%20WEBSITE.pdf.

– All information must be free (public).

– Do not believe in authorities, promote decentralization.

– Hackers should be assessed according to the work they have done, but not according to false criteria such as degrees, age, race or position in society.

– The computer can create art and beauty.

– Computers can change your life for the better.[12]

Hackers are unique individuals, so it is difficult to make a precise and universal profile of a hacker. Each of them has their own unique motives, methods and values. According to skills for computer working, and the interest and ethical point of hacking itself, we distinguish the following types of hackers:

– Old School hackers are the developers of the 1960s from Stanford or MIT Universities, for which the term hacking is a medal of honour. They are interested in coding and analysis of systems, but what they do is not related to criminal activity. Despite the fact that they do not have malicious intentions, they still believe that the Internet was designed to be an open system.

– Script kiddies, Cyber punks, Wanabee hackers, Kiddie hackers or Cyber joyriders' hackers are those whose only intention in infiltration in the system is to cause harm or exploit information. Basically, they are the hackers who are responsible for most attacks against home users. They use developed programs and tools available online which are used without much knowledge of the functionality of the applications. These individuals are usually students who praise of their companions and try to earn self-image to be hackers. Bored in school, very skilled with computers and technology, they download scripts or hack systems intended to disrupt or vandalize. Analyzing this type of hackers we will recognize that this group belongs to malicious hackers.[13]

– Intermediate hackers are mostly people who know about computers, networks, and have sufficient knowledge of programming to be able to understand what it can do a script, but like the previous group use forged but familiar tools to attack.

– Professional criminals, malicious hackers or Crackers – this group of hackers are known as professional criminals. They live by disruption of systems and selling information. They can be hired by corporations to work for government espionage, but may have to do with organized crime groups. These hackers use their skills and tools for destructive or offensive attacks such as viruses' dissemination, performing attacks to ban access (DoS - Denial of Services), as well as attacks on compromised computer network and system and the like. These are the most extreme representatives of malicious hackers also known as cyber criminals.

– Coders, Virus Writers and Ellite Hackers are experienced hackers, who consider them to be elite. They have extensive experience in programming and writing code. They have their own networks for experimentation that are called Zoos. There lay their products and leave the others to use the Internet in their codes. They can penetrate deep into the system, and thereby hide their tracks. Each hacker aims to this level of hackers.[14]

Information security depends on the efforts of users to remove weaknesses, to re-install software that will detect and neutralize viruses and other malicious software, to install and configure so called firewalls, to take care when sharing information, programs and articles in emails, etc. Malicious hackers are constantly present and continually looking for easy targets across cyberspace.[15]

Malicious hackers' activities are:

– Espionage – steal a lot of information because of different reasons.

– Propaganda – any information in writing, image or video they currently publish via social networks or on some sites.

– Denial of service – dening the use of a particular service or computer by the right user.

– Amendment of data – twisting the information for the purpose of propaganda, distortion of the website and so on.

12 Levy, S. (1984). *HACKERS: Heroes of the Computer Revolution*. A Delta Book Published by Dell Publishing a division of Bantam Doubleday Dell Publishing Group, Inc. 1540 Broadway New York, New York 10036, 367. Downloaded on 09 January 2014. http://maben.homeip.net/static/S100/books/heroes%20of%20the%20computer%20revolution.pdf

13 Christian S. Fötinger& Wolfgang Ziegler. Understanding a hacker's mind – A psychological insight into the hijacking of identities. White Paper by the Danube-University Krems, Austria, 48. Commissioned by RSA Security. Downloaded on 15th of December 2013. http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf

14 Melnichuk, D. (2008). The Hacker's Underground Handbook:Learn What it Takes to Crack Even the Most Secure Systems. Downloaded on 08th of January 2014. http://mirror7.meh.or.id/ebooks/The_Hacker_s_Underground_Handbook.pdf

15 I.P.L. Png, Candy Q. Tang, Qiu-Hong Wang (2006). Hackers, Users, Information Security. *Workshop on the Economics of Information Security (WEIS 2006)*. Downloaded on 15th of January 2014. http://weis2006.econinfosec.org/docs/54.pdf

– Abuse of critical infrastructure – the connection of critical infrastructure to the Internet, makes it vulnerable to attack from malicious hackers.[16]

For attacking the systems, malicious hackers use various methods of attack, but the most frequently used are:

– Hacking as activity performed by malicious hackers (generally including cyber criminals). The main goal of malicious hackers is unauthorized entering the system from the outside or from the inside to take unauthorized procedures for authorization and identification, to disrupt the proper functioning of the system, to steal data and information system and sell stolen information, etc. Malicious hackers can be rented from various companies to work as spies for some governments, may have some connections with organized crime and terrorist groups and so on. The reasons for these actions are different: material gain, revenge, entertainment, etc.

– Social engineering, this method is using the weakest line of defense of any organization – people. As a new trend this term in foreign literature is known as people hacking with abused trust as a character trait of people for personal gains.[17]

– Malicious software that involves the use of viruses, worms, Trojans, spyware, etc.

– Attacks prohibiting access (DoS - Denial of Services Attack) used for blocking system that is targeted to claim the huge demand for services per time, and the system is not able to answer, because of that it is completly blocked.

– Fraud bank card that is on the rise worldwide.

– Phishing attacks. These attacks are activities when unauthorized users use fake e-mail messages and fraudulent websites of financial institutions trying to mislead consumers to disclose confidential personal data.[18]

Phases in hacking systems

Ethical and malicious hackers follow the same phases of hacking systems. Hence, the process of hacking can be divided into five distinct phases. Phases in hacking systems are given in Figure 1.[19]

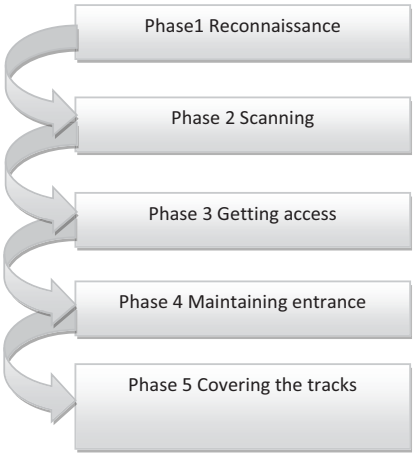


Figure1 - *Phases of hacking*

Phase 1: Passive and active reconnaissance

Passive reconnaissance involves gathering information on potential targets without taking into account the knowledge of the individuals or companies. Passive reconnaissance can be as simple as looking at the building to identify the working hours of employees. Passive reconnaissance is mostly done on the computer. When hackers are seeking for information about a potential target, they usually search the Internet to get information about an individual or company. This process is used to collect information regarding the assessment of the target (Target of Evaluation – TOE). Social engineering and so-called dumpster div-

16 Geers, K.(2011) Heading off hackers: Criminals wield computers as cheap, anonymous weapons. *Per Concordiam. Journal of European Security and Defence Issues*, 2 (2), 21 – 27.
17 Beaver, K. (2010). *Hacking For Dummies, 3rd Edition*. Wiley Publishing, Inc. 111 River Street Hoboken, NJ, 386.Downloaded on 15th of December 2011. http://www.dummies.com/cheatsheet/hacking
18 CARNet Hrvatska akademska i istrazivacka mreza. *Phishing napadi*. CCERT-PUBDOC-2005-01-106., CARNetCERT u saradnji sa LS&S.Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-01-106.pdf
19 Graves, K. (2010). Certified Ethical Hacker Study Guide. Wiley Publishing, Inc., Indianapolis, Indiana, 392. Downloaded on 08th of January 2014. http://files.laitec.ir/wp-content/uploads/2013/06/CEH-Study-Guide.pdf

ing (which literally means diving in a container) are part of passive methods for information gathering by hackers.

Sniffing the network is another way of passive reconnaissance and can provide valuable information on the range of IP address, hidden servers and networks and other services of the system and the network. Using this method hacker sees the flow of data in order to identify the time and transaction traffic. This method offers the opportunity to look at the overall flow of information through the network and often includes usernames, passwords and other sensitive information.

Active reconnaissance includes the search of the network aiming to discover users, IP addresses and network services. This process is sometimes called rattling the doorknobs and involves greater risk of detection than passive reconnaissance. Active reconnaissance allows hackers to gather information about the security of the system, but the process itself increases the possibility of catching the hacker.

Active and passive reconnaissances combined give an opportunity to detect useful information in order to perform an attack. For example, very often it is easy to find the type of web server and the version of the operating system used by the company. This information may also be provided by the hackers to find vulnerabilities in that version of the operating system and used to provide better access.

Phase 2: Scaning

The scan is a process in which information gathered from reconnaissance is used for better study of the system. The tools that hackers could use during the phase scan are: Dialers, Port scanners, Internet Control Message Protocol (ICMP) scanners, Ping sweeps, Network mappers, Simple Network Management Protocol (SNMP) sweepers, Vulnerability scanners, etc. Hackers require any information that can help them attack the target. In addition they request for the data for use in computer names, operating system (OS), installed software, IP addresses, user accounts, and so on.

Phase 3: Getting access

The real hacking begins at this stage. The disadvantages of the system detected during the scanning phase and reconnaissance are now utilized for gaining access to the system that is targeted. The attack of hackers can be derived through local wired or wireless computer network (LAN - local area network); through local access to a computer or the Internet. It can perform the following attacks: stackbased buffer overflows, denial of service (DoS) and session hijacking. Phase gaining access to the world of hackers is known as owning the system, because while the system has been hacked, the hacker takes control over the system and it will be used in the manner as hacker wants.[20]

Phase 4: Maintaining entrance

When a hacker once gains an access to the system that was the target of the attack, he wants to keep this approach for future exploitation and attacks. Sometimes hackers protect the system from attacks by hackers or other security personnel by providing their exclusive access by malicious software: backdoors, rootkits and Trojans. Once a hacker owns the system, he can use it as a base to launch further attacks on other systems. Thus owned computer system is called zombie system.

Phase 5: Covering the tracks

When malicious hackers are able to gain and maintain access to a system, they hide traces detection by security personnel in order to continue to use the already owned system, to eliminate evidence of hacking aiming to avoid legal consequences. Hackers try to remove the traces of the attack by log files or IDS alarms (Intrusion detection system - a system for detecting intruders). Examples of activities that are performed during this phase are:

– Steganography,

– Tunneling protocol, and

– Log files changing.

In the above mentioned phases of hacking into systems, especially during phase 1 – reconnaissance and phase 2 - scanning, malicious hackers gather information about the system and its weaknesses in order to be prepared to attack the system and provide access to it, while the ethical hackers use the same methods and tools trying to gather information that are necessary to protect the system and prevent the entry of malicious hackers. These are the phases through which malicious and ethical hackers outwit in cyberspace, and the winner is the one who has more knowledge, skills in working with computers, persistence, patience, calmness and desire to reach the goal.

20 Graves, K. (2010). *Certified Ethical Hacker Study Guide*. Wiley Publishing, Inc., Indianapolis, Indiana, 392. Downloaded on 08th of January 2014. http://files.laitec.ir/wp-content/uploads/2013/06/CEH-Study-Guide.pdf

CYBER CRIME SCENE IN THE 21ST CENTURY

The number of criminal activities in the area of cyber crime that occur worldwide and on national level is significantly higher than the above mentioned. The aim is to show that no country is immune to this modern threat nowadays, which is constantly changing in shape and capacity. Cyber crime like any other crime knows no borders, nations or individuals, but its well known environment is cyberspace.

In the last six years several serious cyber attacks were detected where the actors were malicious hackers, which significantly attracted the attention of cyber security. These include cyber attacks against the Baltic States: Estonia in spring 2007, the other ones against Georgia in July and August 2008, which coincided with the Russian invasion of Georgia and finally, malicious software called Stuxnet which attacked the Iranian nuclear plant. The latest cyber attack opened a new chapter in cyber warfare, very dangerous and with new tactics of action compared to the previous distributed denial of service attacks (DDoS).[21] In addition, there will be some other examples presented that took place in the 21st century crime scene.

To start with the FBI operation called "Ghost Click" in November 2011, in which six citizens of Estonia were arrested because of the action during which they infected more than 4 million computers in more than 100 countries, with a virus that allowed them illegal earnings of $14 million through collecting the percentage of advertisements on the Internet.

The second action of the FBI, which was set in June 2012, is so called operation "Card Shop", in which 24 people were arrested from eight countries on four continents, stealing and selling the credit card data. The stolen data were returned to the banks and the losses were avoided.

Because the so called "Russian union" in spring stole about 6.5 million passwords from social network LinkedIn, one of the victims filed a lawsuit claiming that it is not only the problem of not properly kept data by the LinkedIn, but also of those whose personal data were compromised who were deliberately not informed of the attack, which seriously violated the security of the personal data of its users.[22]

Richard Bjelich, the chief computer security officer of the company Computer Security Mandiant, after the analysis found that 94% of companies that are their customers do not know that they were attacked, in this case of Chinese hackers who were in search of trade secrets and other information that might have brought advantage in business. Richard Bjelich and his company in the hacking world are known as ethical hackers, whose task is scheduled to enter the system customers to find holes and in the best case to patch them.[23]

Almost at the same time with the actions of the FBI, the famous Information Security Company McAfee published the white paper in the journal Guardian Analytics that disclosed sophisticated hacker attacks which targeted bank accounts of companies and individuals with large amounts. This operation is called "High Roller", which started with the theft in Italy and throughout Europe, Latin America, all the way to the United States. With this attack the hackers managed to fail passwords and banking information, and managed to divert money to their account. After supplying the virus it was independent, performed the whole activity on its own, but it is interesting that it was directed by 60 very powerful computers from Russia. In this attack more criminal groups (ten) were involved and they embezzled 78 million dollars and had all the features of highly organized crime.

Over the past, in the 21st century, the famous hacker group Anonymous, committed many attacks, broke the websites of several state institutions (CIA, FBI, Interpol, French police, law enforcment in the United States and others), International organizations and political parties around the world, accusing them that stifle freedom and democracy in modern societies. Favorite weapon in their struggle attacks are distributed denial of services. This group was directly or indirectly involved in the so-called "Arab Spring". They were also actively involved in the protest "Occupy Wall Street" in hacker attacks on New York's Stock Exchange. In January 2012, they failed to intercept telephone communication between the agents of the US FBI and Britain's Scotland Yard, which once again demonstrated their knowledge of cyber space. During 2010, 2011 and 2012 the group Anonymous set more activities in so called "Operation Avenge Assange". Anonymous also attacked the Internet servers of companies felt violated their ethical code. Examples include the attacks on network servers of Sony Playstation or trying to attack servers of Amazon or Paypal.

On January 1, 2014 hacker group "Syrian Electronic Army" (SEA) has hacked Skype's Twitter and their official Microsoft blog, supposedly to warn people to stay away from services in emails of Microsoft. Figure

21 Lawson, C. (2011). *Working paper Beyond cyber-doom: Cyberattack Scenarios and the Evidence of History* No. 10-77. Dowloaded on 21st od December 2013. http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history.pdf

22 Halpern, S. (2013). Дали су хакери хероји. *Форум за безбедност и демократију*. Едиција видици и путокази, број 3 март 2013 . Downloaded on 15th of December 2013. http://www.fbd.org.rs/akcije/POJEDINACNE/VIP3.pdf

23 APT 1: Exposing one of China's Cyber espionage units. *Mandiant.* Downloaded on 08th of January 2014. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

2 shows the message that was placed on the official Skype's Twitter on January 1, 2014 by the SEA. People in charge in Skype said that the personal data of the users are not compromised.[24]

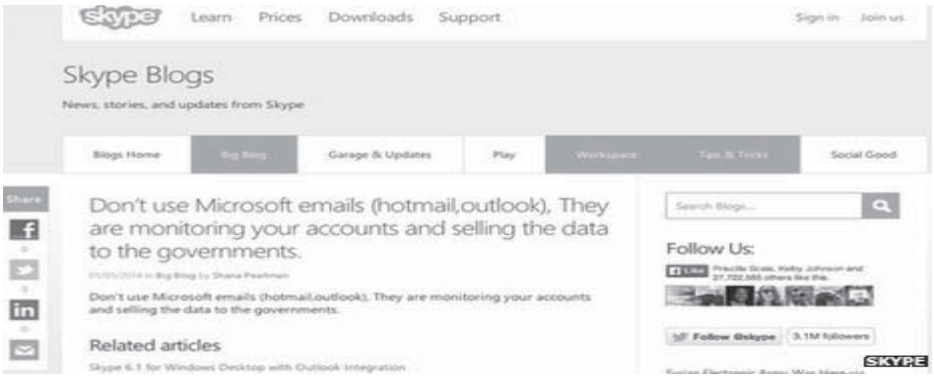


Figure 2 *SEA notification posted on Skype Blogs*[25]

In 2008 a dangerous worm Conficker appeared, also known as Downup, Downadup and Kido. Conficker is a computer worm that attacks the operating system Microsoft Windows and usese advanced techniques of abuse of infected computers that makes it resistant to removal. This attack is considered to have caused the biggest worm infection after 2003, when it was attacking the worm SQL Slammer. In 2009 this worm infected the computer network of the French Navy, key parts of the Ministry of Defense of the United Kingdom, the armed forces of Germany and others. Conficker uses different techniques for its dissemination which make it quite resistant, and it helped his designers often upgraded. Famous were his five versions found in the period from November 2008 to April 2009. Conficker taunted the following symptoms: automatic reset when locking the user's computer; denial of the services of the operating system Microsoft Windows; slow response to the management service domain of customer requirements; suppression of LAN; unavailability of websites whose content is related to antivirus programs and services for the Windows Update and lock the user's computer.[26]

In May 2009, a private Canadian company for security known as "Defense Intelligence", found a huge botnet known by the name of Mariposa which managed to infect over 13 million computers in more than 190 countries worldwide. Among the infected were the computers of known banks and more than half of the 1,000 best-known companies. This botnet was used by Spanish owners designed for theft of a number of personal data, especially the details of bank accounts and credit cards. Also, parts of the botnet were rented to the various organized crime groups. After its discovery, a Canadian security company collaborated with the Spanish security company "Panda Security", the US FBI and Spanish police for detection of network owners, their arrest and imprisonment of a botnet.[27]

Finally, malicious software called Stuxnet which attacked the Iranian nuclear plant opened a new chapter in cyber warfare, very dangerous and with new tactics of action compared to previous attacks of distributed denial of service (DDoS). In July 2010 with the discovery of cyber worm Stuxnet, which hit the Iran's nuclear plant at Natanz, a new way of cyber warfare was discovered. Stuxnet infected more than 60,000 computers, of which more than half of Iran; other countries that were infected with the computer worm were: India, Indonesia, China, Azerbaijan, South Korea, Malaysia, USA, UK, Australia, Finland and Germany. German expert Ralph Lagner explains Stuxnet "as a great military cyber made bomb that was used to complete the cyber attack on Iran's nuclear program. In the computer world such a thing had never been seen". Stuxnet had excellent technical features. Stuxnet, as a sophisticated computer program was designed to enter and control remote external systems in quasi-autonomous form. It represented a new generation of so-called fire-and-forget malicious software that can be directed precisely to selected targets in cyberspace. Those to whom it Stuxnet was directed were not connected to the Internet, so had to be dropped by a hardware component such as a USB stick, to provide access and establish control. After entering the sys-

24 Whitcomb, D. (2014). Skype says user information safe in Syrian Electronic Army hack. *Reuters објавено на 2 јануари 2014г.* Downloaded on 12th of January 2014. http://news.yahoo.com/syrian-electronic-army-says-hacked-skype-39-social-025056851--finance.html

25 Hollister, S. (2014). Syrian Electronic Army hijacks Microsoft blog and Twitter account. *The Verge on January 11, 2014.* Downloaded on 11th of January 2014. http://www.theverge.com/2014/1/11/5299716/syrian-electronic-army-hijacks-microsoft-blog-and-twitter-account-for

26 Управљање сигурносним инцидентима.*CARNet Hrvatska akademska i istrazivacka mreza, CARNetCERT u saradnji sa LS&S.* Downloaded on 15th of December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-266.pdf.

27 Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler. *Democratic governance challenges of cyber security.* DCDCAF HORIZON 2015 WORKING PAPER No. 1. Downloaded on 21st of December 2013. http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf.

tem, Stuxnet first attacked frequency converters which slowed down complete Iranian program to enrich uranium and produce nuclear weapons, which in accordance with some experts' assesment for six months. Stuxnet computer worm is a new era in warfare in cyber space, with a different structure and mode of action against selected targets from all previous cases.[28]

On September 1, 2011, in the Laboratory of Cryptography and Systems Security (CrySyS) at the University of Technology and Economics in Budapest, Hungary, new computer worm called Duqu was unveiled. This worm was very similar to Stuxnet in its configuration. Because of the similarity of these two worms there is some assumption that the creators of Duqu had already known the code of Stuxnet. Both worms have forged digital certificate prevented antivirus and network administrators to disclose, and its purpose was to gather information for future attacks against third parties.[29]

Over the past three to four decades, with the commercial use of computers and according to some statistics since the early 1980's illegal activities in cyberspace started for various motives: crime, terrorism, espionage, sabotage and the like. Some of these activities are included in this section. The large number of cyber attacks and threats with daily occurrence give an accent on cyberspace as a medium for future modern warfare.

Attacks in cyberspace covered in this section are performed by malicious hackers looking for their appetites, and actuated by different motives. The attacks in cyberspace continuously evolve and become more sophisticated. Information–technological development allows access to various malicious softwares available in cyberspace. It increases the threats and challenges in this space which from day to day are more complex and more difficult to defend from intelligent, tolerating, gifted and very skilled opponents – malicious hackers. Weapons which are applied in this war in cyberspace (personal computers) are publicly available to any individual who wants to own them.

Despite repeated ambiguous perceptions of cyber threats, cyber destructive scenarios remained an important tactic of theorists in the field of cyber security. Cyber destructive scenarios are hypothetical stories about expected cyber attack and are designed to serve as cautionary tales shifting the attention of politicians, the media and the public on issues related to cyber security. Examples include attacks against critical infrastructure in a country: the power grid, the financial system that would lead to economic loss or complete economic collapse, the transport system which could lead to accidents in the air and rail traffic, attacks of dams that would cause flooding or attacks on nuclear power plants that would cause accidents in the nuclear reactor, overheating, etc.

INSTITUTIONS, MEASURES AND ACTIONS TO COUNTER CYBER CRIME IN THE REPUBLIC OF MACEDONIA

In the Republic of Macedonia there are many laws that govern the issues of information (relating to personal data and classified information) and the institutions that they own and use the information, and what should be taken into account when defining the security of these information systems. These laws create a framework for the protection of information related to personal data and classified information to public and state security, as well as those related to the defense capabilities of the Republic of Macedonia.[30]

In the context of protection and information security as the most important laws in Macedonia we would like to mention the following: the Law on Classified Information (Official Gazette No. 9/04), the Law on Protection of Personal Data (Official Gazette No. 7/05), the Law on Free Access to Public Information (Official Gazette No. 13/06), the Law on Electronic Communications (Official Gazette No. 13/05), the Law on Monitoring of Communications (Official Gazette No. 121/06) and the Criminal Code of the Republic of Macedonia (Official Gazette No. 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06), the Law on Electronic Data and Electronic Signature (Official Gazette No. 34/01), the Law on Evidence of Insurers and Users of Pension and Disability Insurance (Official Gazette No. 16/04), Decree on office and archive operations (Official Gazette No. 58/1996) and others.

In accordance with the the Law on Electronic Management (Official Gazette No. 105/09 and No. 45/2011), Article 32 paragraph (3) and Article 33 paragraph (2), the Minister of Information Society in 2010 brought "rules of the standards and rules for security of information systems used in the bodies of

28 Rohozinski, R. and Farwell P. James. *Stuxnet and the Future of Cyber War.* Online publication date: 28 January 2011. Downloaded on 21st of December 2013. http://www.cyberdialogue.ca/wpcontent/uploads/2011/03/James-Farwell-and-Rafal-Rohozinski-Stuxnet-and-the-Future-of-Cyber-War.pdf.

29 Богданоски,М., Ристески, А. и Богданоски, М. *Индустриски сајбер напади – глобална безбедносна закана.* Воена академија "Генерал Михаило Апостолски " – Скопје,Факултет за електротехника и информациски технологии – Скопје. In: International conference "The Faces of the Crisis", European University, 09-10 March 2012, Skopje, R. Macedonia. Downloaded on 14th of December 2013. http://eprints.ugd.edu.mk.

30 Водич за информатички и комуникациски технологии (ИКТ) на Метаморфозис, бр.4 (2007). *Безбедност на информациите и зошто да се заштитиме?* Downloaded on 05th of February 2014.. http://www.metamorphosis.org.mk/

communication by electronic means". The rule book contains the set rules and standards for security of information systems used in ministries, state bodies, organizations established by law, the courts, public prosecutors and the State Attorney, legal and other persons who are by law entrusted to public authorities, municipal authorities of Skopje and the other municipalities of the City of Skopje, in establishing of electronic communication.

In 2011 the Ministry of Information Society and Administration (MISA) has rendered other documents of importance for security of information systems:

– Guidelines for monitoring and management of incidents related to information security, and

– Guidelines for actions assessment and risk management.

Based on the aforementioned Law for electronic management, in accordance with Article 34 paragraphs (2) and (4) and Article 35 paragraph (2), the Minister of Information Society has brought the "Regulations on the form and content of the records of the databases of bodies that mutually communicate by electronic means, the manner of its conduct, the format and content of the notification form to establish the basis for its maintenance and storage, as well as the changes that relate to its status, the manner of reporting, and methods of use, enrollment, access and preservation of records of the bases of administrative services by electronic means. It prescribes the form and content of the records of databases of ministries in Macedonia, the state bodies, organizations and other organs of the state, courts, public prosecutors and the State Attorney, legal and other persons who are by law entrusted to public authorities, municipal authorities of the city of Skopje and other municipalities of the City of Skopje (hereinafter: authorities) mutually interacted electronically, the way of its performance, the format and content of the notification form, for the establishment, maintenance and storage base, as well as changes related to its status, notification and method of use, registration, access and preservation of records of the bases of administrative services through electronic communication.

In 2011 MISA brought the Guidelines on the method of use, registration, access and preservation of records of the bases of administrative services electronically.[31]

According to the Law on Criminal Procedure (Official Gazette No. 150 of 18 January 2010), which functions from 01/12/2013, the main role in the resolution of criminal cases is given to the public prosecutor (PP), who together with judicial police (police officers from the Ministry of Interior, officials of the Financial police and law authorized persons of the Customs police working on detection of crimes) and the police (the general name of the judicial police in terms of this law, and the members of the police in the term of the Law on Police, and members of the Military police), and also monitor their work. PP additionally has an opportunity to detect offenses within the scope of cyber crime by the use of special investigative measures (SIM).[32]

In Macedonia, Ministry of Interior Affairs (MIA) is the only organization that has the capacity to detect, monitor and gather evidence of crimes in the area of cyber crime. Since February 2013 the MIA is equipped with forensic laboratory, due to the increased growth of Internet crime and a growing need for expertise on smart phones, notebooks or other technology for communication and data storage.[33]

As regards the necessary measures and actions that should be taken to increase the security of information systems in state institutions, the following steps should be considered:

– To develop and adopt the necessary legal framework in order to improve information security, and in accordance with the existing international conventions and agreements;

– National strategy and policy for information security;

– Modification of the existing laws on important areas sensitive to the threat of information security (e.g. E – Government, E – infrastructure; E – business, E – Health, E – education; E – citizens and E – documents);

– Determination of the person/department/sector for information security (CISCO - Chief Information Security Officer), in every state/public institution;

– Imlementation of activities for the purpose of raising awareness of the risks, threats and challenges in cyberspace, the need to protect the information and quick recovery from possible cyber incident/attack (these activities will refer to the following subjects: general employees and citizens in society, non-governmental sector (NGO), sector economy, government/public institutions and enterprises and local government);

31 Официјална веб страна на Министерството за информатичко општетство и администрација. *Информациска безбедност – законски решенија за заштита на податоци во информациските системи.* Downloaded on 13th of February 2014. http://www.mioa.gov.mk/?q=node/2620

32 Закон за кривичната постапка. Службен весник на РМ бр. 150 од 18.01.2010.

33 Интернет портал IT (8 фев 2013г.). *МВР доби нова форензичка лабараторија за компјутерски вештачења.* Downloaded on 15th of February 2014. http://it.com.mk/mvr-otvora-nova-forenzichka-laboratorija-za-kompjuterski-veshtachen-a/

– Appointment of state organizational infrastructure to deal with these incidents (Centers for Incident Registration and Support in case of breach of information security), and
– Involvement in international activities to increase cooperation, development projects and other activities related to combat information incidents.

Prevention of the cyber crime threats requires the establishment of a separate institution/team to deal with the threats and challenges in cyberspace, globally known as Computer Emergency Response Team (CERT). These teams have not been established in Macedonia yet, although during 2013 their formation was announced, with the task of protecting and providing recommendations for the protection of IT systems of government institutions and the private sector. Debates on the rationality for the establishment of these teams were led on the forum of the Internet portal "IT" on the theme "Developing CERT/CIRT team in Macedonia". In addition to the question "Should we create CERT/CIRT team in Macedonia?" 78% of surveyed IT members voted "yes" for the establishment of these teams, which is a high percentage of the justification for establishing these teams.

CONCLUSION

Cyber crime is increasingly appearing in more complex forms difficult to detect and prevent. The malicious software as one of the methods of cyber crime is accessible in cyberspace. The term hacker was used a long time ago, but in the context of IT society it begins to be applied in the second half of the 20th century. The constant change of the shape and form of cyber threats in cyberspace requires continuous and appropriate adaptation to protect this area. Malicious hackers (cyber criminals) have the main goal to enter the system and continue to have all the benefits of our personal nature such as personal data, bank accounts and so on. They penetrate into the computer without our knowledge and undertake all illegal measures.

In contrast, ethical hackers are people who are hired to find the weaknesses of our system, to eliminate and at best to find the perpetrator. The best experts for information security come from ethical hackers. Hackers engaged in research who published the results on blogs for sharing the research are excellent for the correction of the systems and engines of modern technological development. Cyberspace is the home of hackers regardless of their motives. Cyberspace has connected people around the world, but made them dependent on new technology and exposed to new risks and threats present only in it.

The phases of operation of hackers are the same as for the malicious and ethical hackers. The better we know the stages of action, thinking, the attack to be used, a set of tools, purpose and motives of malicious hackers we will create better protection. If the attacks in cyberspace in the beginning were only for entertainment and intellectual prestige, then have been only a criminal act for financial benefit, furthermore continued to be destructive, and evolved in coordinated attacks in the real and the virtual battlefield, the expectation in the future is that they will be more and more complex. Awareness of each individual constantly rapidly increases about the risks arising from cyber threats.

Social engineering has always been a good tool for criminals to access information of a personal nature of the potential target for implementation of activities in the area of cyber crime. Information gathered through social engineering in many cases resort to negligence and accident. In this context there is the case of the growing misuse of credit/debit cards where the main cause is human negligence and low awareness of the threats that lurk us everyday. So often we have witnessed cases when markets throughout Macedonia, often people who pay with credit/debit cards, being in a hurry tell loudly the PIN code to the vendor instead of entering it for identification and authentication, thereby exposing themselves to risk of it being written/remembered from a third party, and later abused for extracting money from the bank account.

The biggest threat to operation of cyber criminals in so called E-projects and E-services of the Government, will occurre due to: low awareness of the employees of the threats in cyberspace, ignorance, negligence and disregard of the safety rules and procedures. Cyber crime would be executed due to people as a security risk.

As it can be seen, there is inevitable need for the establishment of CERT/CIRT teams in Macedonia as a tool for preventing attacks under the auspices of cyber crime and facilitate cooperation between the executive and judicial power between states. The future will show that still the biggest threats to cyberspace derive from non–state actors, because the weapons of warfare in this space are commercially available and inexpensive, and malicious hackers know how to operate with them very well.

REFERENCES

1. Achkoski, J. and Dojchinovski,M. *Cyber terrorism and cyber crime – threats for cyber security.* Military Academy "General Mihailo Apostolski" – Skopje. Proceedings of First Annual International Scientific Conference, Makedonski Brod, Macedonia, 09 June 2012. Downloaded on 16th of December 2013. http://eprints.ugd.edu.mk.
2. APT 1: Exposing one of China's Cyber espionage units. *Mandiant.* Downloaded on 08th of January 2014. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
3. Бери Бузан (1983). *Луѓе, држави и страв.* Скопје, 2010: Академски печат.
4. Beaver, K. (2010). *Hacking For Dummies, 3rd Edition*. Wiley Publishing, Inc. 111 River Street Hoboken, NJ, 386. Downloaded on 16th of December 2011. http://www.dummies.com/cheatsheet/hacking
5. Benedikt, M. *Introduction to Cyberspace: First Steps.* MIT Press, 1991. Downloaded on 05th of February 2015. http://homes.ieu.edu.tr/nozgenalp/MCS490/Media.Culture.and.Technology-Readings/week.11-introduction.to.Cyberspace%20First%20Steps%20Benedikt.pdf.
6. Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler. Демократско управљање изазови сајбер безбедности. Downloaded on 15th of December 2013. http://www.fbd.org.rs/akcije/POJEDINACNE/CYBER%20ZA%20WEBSITE.pdf.
7. Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler. *Democratic governance challenges of cyber security.* DCDCAF HORIZON 2015 WORKING PAPER No. 1. Downloaded on 21st of December 2013. http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf.
8. Богданоски, М., Ристески, А. и Богданоски, М. *Индустриски сајбер напади – глобална безбедносна закана.* Воена академија "Генерал Михаило Апостолски " – Скопје,Факултет за електротехника и информациски технологии – Скопје. In: International conference "The Faces of the Crisis", European University, 09-10 March 2012, Skopje, R. Macedonia. Downloaded on 14th of December 2013. http://eprints.ugd.edu.mk.
9. Concise Oxford English Dictionary (Tenth Edition) on CD ROM 2001 Version 1.1. Copyright Oxford University Press 1999, 2001. Oxford University Press, Great Clarendon Street, Oxford OX2 2DP, UK. Software developed by Toni Smith(tony@werdz.com). Definition of cyberspace from Concise Oxford English Dictionary (Tenth Edition).
10. Concise Oxford English Dictionary (Tenth Edition) on CD ROM 2001 Version 1.1. Copyright Oxford University Press 1999, 2001. Oxford University Press, Great Clarendon Street, Oxford OX2 2DP, UK. Software developed by Toni Smith(tony@werdz.com). *Definition of cyberspace from Concise Oxford English Dictionary (Tenth Edition).*
11. Cyber Terrorism and Cyber Sabotage (2012). *Intelligence Briefings.* Downloaded on 18th of December 2013. https://janes-ihs-com.ezproxy.members.marshallcenter.org.
12. Christian S. Fötinger& Wolfgang Ziegler. Understanding a hacker's mind – A psychological insight into the hijacking of identities. White Paper by the Danube-University Krems, Austria, 48. Commissioned by RSA Security. Downloaded on 15th of December 2013. http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf
13. CARNet Hrvatska akademska i istrazivacka mreza. *Phishing napadi*. CCERT-PUBDOC-2005-01-106., CARNetCERT u saradnji sa LS&S.Downloaded on 16th December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-01-106.pdf
14. Водич за информатички и комуникациски технологии (ИКТ) на Метаморфозис, бр.4 (2007). *Безбедност на информациите и зошто да се заштитиме?* Downloaded on 05th of February 2014.. http://www.metamorphosis.org.mk/
15. Encyclopaedia Britannica Online Academic Edition. Encyclopædia Britannica Inc., 2013. Web. 11 Dec. 2013. Downloaded on 16th of December 2013. http://www.britannica.com.ezproxy.members.marshallcenter.org/EBchecked/topic/1498241/cyberwar.
16. Ganguly,S. *Impact of Cyberterrorism in digital world*. FTMS Global Academy Pte Ltd, Singapore. Downloaded on 18th of December 2013. http://www.ijcsits.org/papers/vol1no12011/6vol1no1.pdf .
17. Geers, K.(2011) Heading off hackers: Criminals wield computers as cheap, anonymous weapons. *Per Concordiam. Journal of European Security and Defence Issues*, 2 (2), 21 – 27.
18. Graves, K. (2010). *Certified Ethical Hacker Study Guide*. Wiley Publishing, Inc., Indianapolis, Indiana, 392. Downloaded on 08th January 2014. http://files.laitec.ir/wp-content/uploads/2013/06/CEH-Study-Guide.pdf

19. Halpern, S. (2013). Дали су хакери хероји. *Форум за безбедност и демократију.* Едиција видици и путокази, број 3 март 2013. Downloaded on 15th of December 2013. http://www.fbd.org.rs/akcije/POJEDINACNE/VIP3.pdf

20. Hollister, S. (2014). Syrian Electronic Army hijacks Microsoft blog and Twitter account. *The Verge on January 11, 2014.* Downloaded on 11th of January 2014. http://www.theverge.com/2014/1/11/5299716/syrian-electronic-army-hijacks-microsoft-blog-and-twitter-account-for

21. ICANN. *Beginner's Guide to DOMAIN NAMES.* Downloaded on 05th of February 2015. https://www.icann.org/en/system/files/files/domain-names-beginners-guide-06dec10-en.pdf

22. Information and Instructional Guide:Hacking secrets revealed. Production of S&C Enterprises, Consultation Group, 75. Downloaded on 08th of January 2014. http://hackersinternational.com/access/content/Hacking_Secrets_Revealed.pdf

23. I.P.L. Png, Candy Q. Tang, Qiu-Hong Wang (2006). Hackers, Users, Information Security. *Workshop on the Economics of Information Security (WEIS 2006).* Downloaded on 15th of January 2014. http://weis2006.econinfosec.org/docs/54.pdf

24. Интернет портал IT (8 фев 2013г.). *МВР доби нова форензичка лабараторија за компјутерски вештачења.* Downloaded on 15th of February 2014. http://it.com.mk/mvr-otvora-nova-forenzichka-laboratorija-za-kompjuterski-veshtachen-a/

25. Lawson, C. (2011). *Working paper Beyond cyber-doom: Cyberattack Scenarios and the Evidence of History* No. 10-77. Dowloaded on 21st od December 2013. http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history.pdf

26. Levy, S. (1984). *HACKERS: Heroes of the Computer Revolution.* A Delta Book Published by Dell Publishing a division of Bantam Doubleday Dell Publishing Group, Inc. 1540 Broadway New York, New York 10036, 367. Downloaded on 09th of January 2014. http://maben.homeip.net/static/S100/books/heroes%20of%20the%20computer%20revolution.pdf

27. Маринковиќ, Д. Информациони рат, Замке виртуелног света. *Одбрана 62-65.* Downloaded on 15th of December 2013. http://www.voa.mod.gov.rs/sr/publikacije/zamke-virtuelnog-sveta.pdf

28. Melnichuk, D. (2008). The Hacker's Underground Handbook:Learn What it Takes to Crack Even the Most Secure Systems. Downloaded on 08th of January 2014. http://mirror7.meh.or.id/ebooks/The_Hacker_s_Underground_Handbook.pdf

29. Милосављевиќ,М. и Грубор,Г. (2009). *Истрага компјутерског криминала – Методолошко технолошке основе.* Универзитет "Сингидунум" – Београд, 291. Downloaded on 15th of December 2013. http://www.seminarski-diplomski.rs/biblioteka/Istraga%20kompjuterskog%20kriminala.pdf.

30. Официјална веб страна на Министерството за информатичко општетство и администрација. *Информациска безбедност – законски решенија за заштита на податоци во информациските системи.* Downloaded on 13rd of February 2014. http://www.mioa.gov.mk/?q=node/2620

31. Oxford Dictionaries. Definition of crime from Oxford Dictionaries Online.Downloaded on 13th of February 2014. http://www.oxforddictionaries.com/definition/english/crime?q=crime

32. Oxford Dictionaries. (2011). *Definition of virtual from Oxford Dictionaries Online.* Downloaded on 16th December 2012. http://www.oxforddictionaries.com/definition/virtual?view=uk

33. Питер Хју (2006). *Поим за глобална безбедност.* Скопје 2009: Табернакул.

34. Rohozinski, R. and Farwell P. James. *Stuxnet and the Future of Cyber War.* Online publication date: 28 January 2011. Downloaded on 21st of December 2013. http://www.cyberdialogue.ca/wpcontent/uploads/2011/03/James-Farwell-and-Rafal-Rohozinski-Stuxnet-and-the-Future-of-Cyber-War.pdf.

35. Роберт Џ. Бункер (2003). *Не – државни закани и идни војни.* Скопје (2009): Нампрес.

36. United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity," *Science* 326 (13 November 2009): 943-4; See Martin Charles Golumbic, Fighting Terror Online: The Convergence of Security, Technology, and the Law (New York: Springer, 2007).

37. Управљање сигурносним инцидентима.*CARNet Hrvatska akademska i istrazivacka mreza, CARNetCERT u saradnji sa LS&S.* Downloaded on 15th of December 2013. http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-266.pdf.

38. Whitcomb, D. (2014). Skype says user information safe in Syrian Electronic Army hack. *Reuters објавено на 2 јануари 2014г.* Downloaded on 12th of January 2014. http://news.yahoo.com/syrian-electronic-army-says-hacked-skype-39-social-025056851 – finance.html.

39. Закон за кривичната постапка. Службен весник на РМ бр. 150 од 18.11.2010 година.

UDC: 343.533::004

BRIEF ANALYSIS OF CHARACTERICS AND COUNTERMEASURES AGAINST MINOR CYBERCRIME

Jingwen Xu[1]

National Police University of China, Computer Crime Investigation Department, Shenyang

Abstract: Minor[2]cybercrime gets its particular characteristics by absorbing the features both of the traditional minor crime and the emerging cybercrime. The spring up of this distinct kind of crime coincides with the Internet being widespread together with the intelligent devices as its crime rate is on the rise meanwhile. The particularity of the subject of crime, the novelty of the crime means and the seriousness of its social harm has jointly attracted much public attention. The paper starts with a brief analysis on the reasons and characteristics of this crime. In other words, in face of complex cyber environment, minors are mentally immature in general and thus may commit this specific crime. Hence, the minor cybercrime subject appears to be of lower age, group organized while the consequences present to be of more seriousness and violence. The paper then continues making efforts to explore the reasonable countermeasures towards the crime while addicted to the idea of combining the crime fighting and prevention. The countermeasures raised in the last part based on active guides and loving care of minors so as to achieve the goal of integrating influential education and penalty which are worth mentioning.

Keywords: minor cybercrime, crime causes, crime characteristics, crime countermeasures.

INTRODUCTION

Minor crime, environmental pollution together with drug addiction and drug selling are universally acknowledged as "three worldwide hazards". Despite of the spread of modern civilization, the Internet has also produced a series of social issues. In other words, minor cybercrime bears the brunt of the fruits. In the United States, there was once a minor named Kevin Mitnick who hacked into the North American Aerospace Defense Command Center at the age of 15. Back to the Gulf War period, a Dutch boy even hacked into the Pentagon computer system when he was only 10. According to a survey in the United States, over 80 percent of domestic cybercrimes were conducted by rookies working within five years with an average age of 22. Coincidentally in China, an investigation carried out by the information database *www.lawyee.com* showed that in the year of 2013, a total number of 265,439 minors had been judged by courts nationwide with 21% of them (numbered 55,817) were minors below 18 years of age. Shenzhen procuratorial organ once made a research on the subjects of cybercrime from 2011 to 2013. Among all 37 subjects of the crime, 28 of them were post-80s with the proportion of 76% while 8 of them were post-90s. The youngest one was only 17.

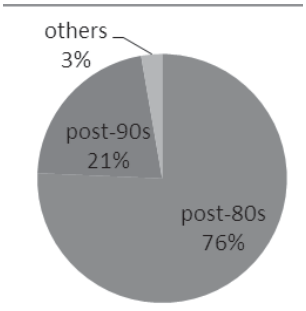


Figure 1 *Shenzhen Procuratorial Organ's Research on Subjects of Cybercrime*

It is not hard to see, minor cybercrime issue has become a prominent social challenge worldwide. As such, the paper tried hard to trace the sources of minor cybercrime and therefore attempted to establish coping mechanism against the crime.

1 mia_xu_mia@163.com

2 "In law, a minor is a person under a certain age — usually the age of majority — which legally demarcates childhood from adulthood. The age of majority depends upon jurisdiction and application, but is generally 18." From http://en.wikipedia.org/wiki/Minor_(law)

BRIEF ANALYSIS ON CHARACTERICS OF MINOR CYBERCRIME

The minor cybercrime subject appears to be of lower age

1. Networked society is the trend of social development

2014 was the 20th anniversary of China's first connection to the Internet. According to the white paper named *the 35th Statistical Report of China Internet Development Conditions*, by the end of 2014 Chinese net users have reached 649 million while the Internet penetration rate has reached 47.9%. In addition to this, both the amount of net users and mobile web users were also on the rise year by year. At the end of December 2013, juvenile net users[3] have reached 256 million with an overall proportion of 71.8 % (26% more than the national average Internet penetration of 45.8%) increased by 5.4 % compared with the year of 2012 with a continuing growth trend.

Table 1 *Statistics about Internet usage*

	2011	2012	2013	2014
Net users	513 million	564 million	618 million	649 million
Mobile web users		420 million	527 million	557 million

2. Minor is the main force of the Internet population

Another survey named *the 2013 Report of Online Behaviors of Chinese Youth* conducted also by *CNNIC* revealed that by the end of 2013 juvenile net users have reached 256 million while mobile web users were 221 million. Besides, juvenile mobile web users hold a proportion of 68.3%, 4.7% higher than the previous year. What is more, *CNNIC* survey also found that juveniles have also increased their online time. In addition, it is noted that minors have occupied a remarkable increasing penetration. By the end of 2013, the proportion of minors under the age of 18 occupied more than half of all juvenile net users.

Table 2 *Statistics about online behaviours of the Chinese Youth*

	2010	2011	2012	2013
Juvenile net users	212 million	232 million	235 million	256 million
Juvenile mobile web users	170 million	185 million	196 million	221 million
Minor net user proportion	46.5%	55.9%	63.6%	68.3%
Online time (hours per week)	14.3	16.5	18.4	20.7

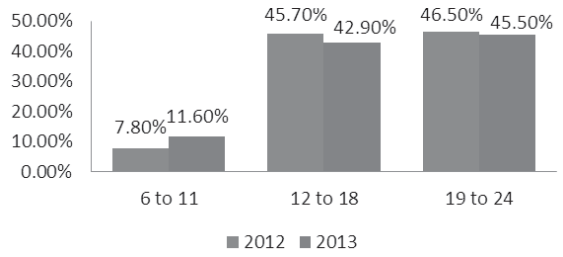


Figure 2 *Age structure of juvenile net users*

Therefore, we can conclude that minors have been the main force of the Chinese net users, as well as the main trend of minor cybercrime presents to be an extension to a lower age. At the same time, smart phones, popularity of tablet PCs together with the everywhere present network culture all contribute jointly to the increase proportion of minors in traditional cybercrimes.

The minor cybercrime presents to be group organized, of more seriousness and violence

Compared with the traditional crime, the criminals of minor cybercrime are fresh and with less experience. In general, they seldom commit crimes independently. Instead, they usually have to finish the crime with the help of search engine or the help from some "experienced" net friends. In addition, the develop-

3 Juvenile refers to the people under the age of 25.

ment and popularization of instant communication software also contributes a lot to the group organized feature of minor cybercrime.

Table 3 *Web Application Penetration of Juveniles*

	Search information	Instant Communication	On-line Game	E-commerce
Juvenile net users	80.5%	91.1%	65.7%	50.0%
Net users	79.3%	86.2%	54.7%	48.9%

As can be seen from the above chart, besides the instant communication software and search application, on-line game is also juveniles' main purpose of using the Internet. It is no exaggeration to say that violence and pornography have become more and more common or even becoming selling points of some unscrupulous game developers. Blindly imitating or copying scenes of the games may stimulate young game players commit serious offenses such as violent crimes and rapes.

In addition, network evolution of traditional crimes has also caused more serious criminal consequences. It is due to the reason that cybercrime spans the boundaries between social space and cyberspace. Cybercrime usually goes deep into the economy, culture, politics and daily life.

ANALYSIS OF THE CAUSE OF MINOR CYBERCRIME

Subjective reasons

Based on *An Analysis Report on Social Behaviors of Post-95s* conducted by Tecent Co. in 2014, nearly 60% of post 95s blocked their parents in social networking. Some juvenile respondent thought: "it makes me feel that my parents are monitoring me, it's terrible. I don't know how to behave in SNS (Social Networking Services)." Another respondent said: "we have grown up; we have our own thoughts and privacy. There are some sensitive topics such as intimate relationship or some complaints we don't wanna let them know."

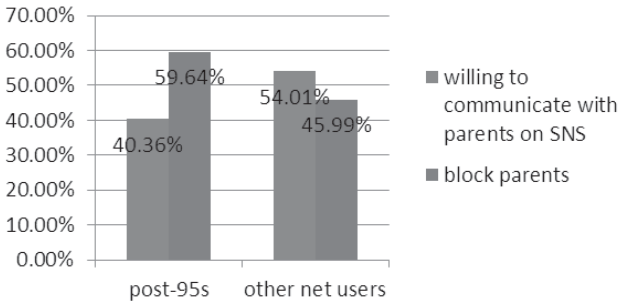


Figure 3 *SNS Acceptance of Parents*

Contrary to the above reality situation, juveniles around 20s are more willing to speak in cyberspace and hold high acceptance of social platforms. Put another way, social networks have become part of their life necessary. What's more, compared with adults, post-95s are more willing to speak actively on social platforms with ten percentages point higher. Lack of initiative in real life yet full of initiative in virtual world shows that communicating with one's identity disguised or concealed may make post-95s feel more confident and of more sense of identity.

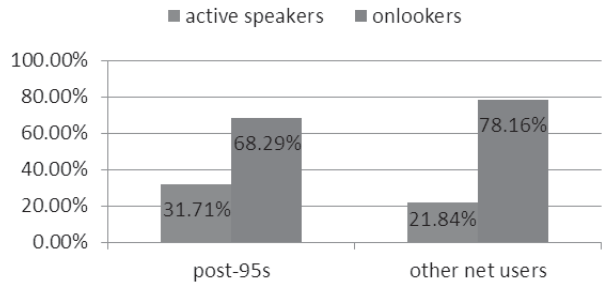


Figure 4 *Activity Degree of post-95s and Other Net Users*

Generally, minors are neither intellectually fully developed, nor physically mature. With underdeveloped personality and value concept system, their capabilities of self-control and self-protection are week. Given all above into consideration, minors are more vulnerable to both their own emotional effect and outside influences. In cyberspace, which is a virtual "free" space without parents' supervision and basic discipline, it is often found that minors tend to lose their objectivity, rationality, and capability of being calm to certain phenomenon or situation. The fact, that minors lack the ability to make the right judgment of relatively complex public social phenomenon and to grasp the scale of their own behaviour, increases the occurrences of minor cybercrime. In addition, as particular as the life stage minors are at, their emotional catharsis, obsession with adventure and escaping, as well as blind conformity to psychological characteristics are observed in the virtual world.

Objective reasons

Low cost of cybercrime and low technological threshold have both become reasons of minor cybercrimes. On the whole, the crime subject of cybercrime is transforming from experts of specialized knowledge into juveniles of basic computer knowledge. According to *the 35th Statistical Report of China Internet Development Conditions*, by the end of 2014, net users with secondary education held the largest proportion. Junior middle school education level represented 36.8% while net users with high school education or technical secondary school accounted for 30.6%.

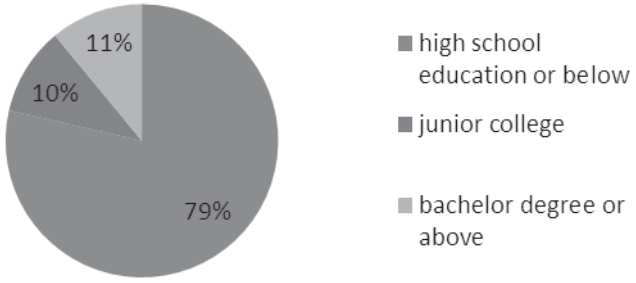


Figure 5 *Educational Background Structure of China's Net Users*

As an example, Suzhou procuratorial organ once conducted a survey concerning the education degree of the defendant. The result revealed that suspects with high school educations or less occupied 63%, while suspects with junior middle school education held the highest proportion of 35.05%.

Again for illustration, in the *CNNIC* survey, it is also found that the proportion of minors surfing at Internet cafés was 27.4% appearing a decrease trend year by year. In contrast, the proportion of minors surfing via mobile phones represented as 86.3% appearing increase year over year. As Internet cafés have a complicated staff composition and complex information stored in computers, it is hard to overlook the impact of premature interaction with the certain community brings to minors. The inappropriate and unhealthy information that can be found through Internet, as well as the complex subculture of networks, have unsounded psychological impact to minor crime. For instance, one can easily find pornography, lust information, and violent content and games from the internet. These could all form mental stimulation leading to a possible minor crime. What's more, more convenience of accessing to the Internet with smart phones may also bring about difficulties in supervising.

The unhealthy social trends, mixed media information, especially some hot posts of money worship on BBS or forums, hedonism and other adverse social trends, seriously erodes the health of minors.

COUNTERMEASURES TOWARDS MINOR CYBERCRIME

Positive guide

The law against minor crime varies by countries. As to China, we have not yet reached an identical standard. However, laws and regulations all share one basic point, which is to protect minors. Given they are still in the process of growing up, on the one hand, minors are immature, lack self-control; on the other hand, they offer great possibility to be corrected and reformed. Even law still shows tolerance for minors; growth education should really focus on positive guide and reasonable precautions.

As to the legislation, although cybercrime develops and changes fast, we should at least agree on a general legislative idea. If so, we could timely adjust and adapt to the future evolution of the crime and therefore combat it. Taking the Computer Ethics Institute in the United States as an example, it has established Ten Commandments concerning computer ethics. To be specific, they are: should not hurt others by taking use of computers; should not disturb others while they are doing computer works; should not peek others' files; should not steal by the use of computers; should not commit perjury by using computers; should not use or copy software without pay; should not take use of others' computer resources without permission; should not steal others' intellectual property; should be fully aware of the consequences of your programs; should use the computers with deep consideration and carefulness. None of the above commandments is law or regulation, yet it provides moral code for all the people.

In addition to the legislature, relevant social institutions should also shoulder due responsibilities. For example, Culture Sectors should tighten up the management of the Internet culture such as the Internet literature, Internet audio and video, and Internet games. The Industry and Commerce Sector together with the Public Security Sector should jointly supervise and control the geographic site selection of internet cafés. "Internet cafés should be built at least 200 square meters far away from schools" is one of China's administration regulations towards Internet café management. However, the reality effect still remains open to question.

Last but not the least, parents should pay more attention to daily supervision of minors, reasonably arranging time and content for minors of using networks. Meanwhile, it is their duty to observe the growth and changes of their children with appropriate parenting. As far as in school, students should have sufficient access to current events, the latest society activities under good guiding. Minors should also get legal awareness education, making them fully aware of the deterrent force of law so that they would have better understanding of the boundaries.

Reasonable penalty

A well-established penal system is urgently needed to help prevent minor cybercrime, in case active and positive guide may fail. In China's legal system, we adhere to the principle of education, influence and rescue, and the legislative principle of positive guide combining with reasonable penalty.

The age of criminal responsibility under the Criminal Law refers to natural hazards on their social behaviour should be held criminally responsible must reach the age. "The concept of minor is not sharply defined in most jurisdictions. In many countries, including Australia, India, Philippines, Brazil, Croatia, and Colombia, a minor is defined as a person under the age of 18. In the United States, where the age of majority is set by the individual states, minor usually refers to someone under the age of 18, but can in some states be used in certain areas (such as gambling, gun ownership and the consuming of alcohol) to define someone under the age of 21. In the criminal justice system in some places, 'minor' is not entirely consistent, as a minor may be tried and punished for a crime either as a 'juvenile' or, usually only for 'extremely serious crimes' such as murder, as an 'adult'. In Japan, Taiwan, Thailand, and South Korea, a minor is a person under 20 years of age. In New Zealand law, a minor is a person under 20 years of age as well, but most of the rights of adulthood are assumed at lower ages: for example, entering into contracts and having a will are legally possible at age 15."[4]

In China, minors below 14 are fully free of criminal responsibility; minors between 14 and 16 are responsible for several serious crimes; minors over 16 are of full criminal responsibilities. As have been mentioned before, the main trend of minor cybercrime presents to be an extension to a lower age. Thus, maybe we should adjust the age of criminal responsibility to the specific kind of crime. This needs to be stressed that we are not aiming at punishing, instead, we aim to deter much more than penalty. In addition, as the minor cybercrime presents to be of more seriousness and violence, modestly lower the age of criminal responsibility may also benefit on cracking down severely violent form of crimes.

It is worth noting that the penal system we are talking about here should not only include the penalty against minor cybercrime, but also includes the penal system against adults' unethical behaviour on the Internet.

CONCLUSION

Minors are not only the main forces in cyberspace, but future dominant force to the society as well. As the Internet culture is a double-edged sword, we should pay more attention to its drawbacks due to our duties of standing by the minors' sides. The legislature, relevant social institutions and families should join hands together stepping up anti-minor cybercrime campaign.

4 http://en.wikipedia.org/wiki/Minor_(law)

REFERENCES

1. http://en.wikipedia.org/wiki/Minor_(law)
2. 2013 Report of Online Behaviors of Chinese Youth. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/qsnbg/201406/P020140611557842544454.pdf
3. 35th Statistical Report of China Internet Development Conditions, 2014. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201502/t20150203_51634.htm
4. An Analysis Report on Social Behaviors of Post-95s. Internet Frontiers, 2014(10).
5. Criminal Procedural Law (3rd edition). Law Press China.
6. Ge Liming. Youth Cybercrime and Control System Construction. Legal Research, 2014(07).
7. Hu Jiang. The Internet Age and Minor Delinquency Prevention and Countermeasures. Law and Politics Explore, 2014(01).
8. Li Shujuan. Minor Crime and its Governance Path Network to Explore. Journal of Yunnan University Law Edition, 2014(1).
9. Liu Qi, Bao Yun, Yi Jun. Cultivation of Legal Accomplishment about the Internet towards Minor. China Youth Study, 2014(12).
10. Long Kuichen. Legal Analysis of Minor Cybercrimes. Law and Social, 2014(03).
11. Mo Xiuzhuang. Study of Legal Control of Minor Crimes concerning the Internet. Legal System and Society, 2014(11).
12. Pang Yu. Research on Problems among China's Laws and Regulations concerning the Internet. Study of Law, 2015(2).
13. Sun Tiecheng. Issues about Cybercrimes. Conference Proceeding of 2014 Seminar on Criminal Law Countermeasures towards Cybercrimes, 2014.
14. Survey on Chinese Adolescent Behavior in the Internet, 2013. http://www.CNNIC.cn/hlwfzyj/hlwxzbg/qsnbg/201406/t20140611_47215.htm
15. Tian Hongjie, Wang Ran. Research on Current Situation and Regulation Path of Cybercrimes. Conference Proceeding of 2014 Seminar on Criminal Law Countermeasures towards Cybercrimes, 2014.
16. Wang Shufang. Study of China's Minor Cybercrime. Vocational Technology, 2014(10).
17. Yu Chong. The Status Quo and Development Trend of Minor Cybercrime under the Background of Triple Network. Minor delinquency, 2014(1).
18. Zhao Yunfeng, Zhou Jing. Causes and Countermeasures concerning Minor Cybercrime. Minor delinquency, 2014(4).
19. Zhang Mengdong. Characteristics and Criminal Justice of Cybercrimes—based on Cybercrime Cases Handled by Shenzhen Procuratorial Organ. Conference Proceeding of 2014 Seminar on Criminal Law Countermeasures towards Cybercrimes, 2014.

UDC: 343.533::004
316.624:004

ANALYSIS ON CYBER PICKING QUARRELS AND PROVOKING TROUBLES CRIME

Daoning Sun[1]

National Police University of China, Computer Crime Investigation Department, Shenyang

Abstract: A year ago, the judicial interpretations relevant to the cyber picking quarrels and provoking troubles crime were published. Since then, several famous cyber persons have been involved in this crime. The cyber picking quarrels and provoking troubles crime have raised a hot debate in the fields of theory and practice. The field of theory is devoted to the research domain of the criminal law. The field of practice is different. The field of practice focuses almost on the same thing: aimed at the case characteristics and based on the requirement of the public security, they discuss the problems that are to be paid more attention to during the investigation of such cases. This paper discusses the culture attribute and crime cost of the cyber picking quarrels and provoking troubles crime from the angle of relationship crime. Based on this, this paper probes into the differences between the cyber picking quarrels and provoking troubles crime and the traditional picking quarrels and provoking troubles crime. At last, this paper proposes that continuing to enhance the cyber law and continuing to strike the crimes are not only a responsibility, but also an adscription of our research on crime.

Keywords: cyber picking quarrels and provoking troubles crime; cyber; crime.

INTRODUCTION

Analyzing the crime problems from different aspects can make us understand the cyber picking quarrels and provoking troubles crime more clearly. It has been only a year since the judicial interpretation published some famous cases of cyber picking quarrels and provoking troubles crime that had been committed. During this period people warmly discussed the cyber picking quarrels and provoking troubles crime happening in cyberspace and their harmful consequences. The crime is related to many factors. Therefore, we will pay our attention to the analysis of the phenomenon of crime as much as possible.

SOME RELATED FACTORS OF THE CYBER PICKING QUARRELS AND PROVOKING TROUBLES CRIME

Émile Durkheim, a famous French sociologist and criminologist, argues that all kinds of social phenomena should be regarded as something that is outside the reality of the individual to study. Although the cyber picking quarrels and provoking troubles crime are new crime types, they are only social phenomena. Exploring some related factors is not based on the traditional criminology. But it is based on the relationship criminology. It is a criminal charge existing only in the Chinese criminal law.

The cyber culture

Some people think that the cyber culture is a connection between cultural citizenship and Internet-based media[2]. Most scholars agree that cyber culture has both a broad and narrow definition. Cyber culture is based on its technology to support all cultural activities. It has its values and cultural activities in the form of synthesis[3]. There is no denying that the construction of cyber culture of the socialism with Chinese characteristics has made great achievements. At the same time, the construction inevitably produces some disharmonious factors. The factors have weakened mainstream ideology, national culture, the morals, etc. The cyber picking quarrels and provoking troubles crime are highly correlated with the public opinion environment of the cyber culture. In the modern life, the Internet has become our important means of expressing personal opinions and ideas. It is the important environment and route of transmission of

1 sundaodaoning@126.com

2 Goode, Luke. Cultural citizenship online: the Internet and digital culture. *Citizenship Studies*.Oct2010, Vol. 14 Issue 5:p. 527-542

3 Feng Wan. Analysis on cyber culture and characteristics. *The education academic issue*.2010-4, p63.

the cyberspace public opinion formation. The cyber culture is virtual, fast, multivariate, and extreme and it weakens control. It causes the confusion of the cyberspace public opinion environment. Additionally, it provides conditions that challenge the normal order of social management of the crime. The boring aggression of cyber cultures subtly influences affected potential troublemakers to criminal crime motive.

The crime cost

The cyber picking quarrels and provoking troubles crime have four kinds of behavior. First, one of the kinds is a random attack. Second, one of the kinds is chasing, intercepting, abusing and threatening others. Third, one of the kinds is a random possession of others' property or damage, occupying public or private property. Fourth, one of the kinds is creating disturbances in a public place, resulting in serious disorder. Apart from crime of passion and aggressive crimes directly, most of the potential criminal persons naturally are estimating the crime cost when having in mind crime motives.

According to a formula[4]:

Cybercrime cost = Direct cost +Opportunity cost +Legal punishment*Seized probability + Social additional cost.

In cyber picking quarrels and provoking troubles crime, there are direct cost, opportunity cost and social additional cost caused by specific virtual of the cyber space. A criminal person will save a lot of manpower and cost in his direct cost. And that is one of the characteristics of the implementation of traditional crime using the internet as a tool or means. The probability of crime of preset effect is greatly increased by using the specific attribute of the network. As a new type crime, the cyber picking quarrels and provoking troubles crime have few precedents to guide.

THE HETEROGENEITY OF THE CYBER PICKING QUARRELS AND PROVOKING TROUBLES CRIME

The cyber alienation

Compared with the traditional picking quarrels and provoking troubles crime, the cyber picking quarrels and provoking troubles crime have a new form which is different from the past. And that caused some of the problems in the applicable law. According to the author's survey data:

		Frequency	Percentage	Effective percentage	Cumulative percentage
Effective	Random attack others	350	72.0	72.3	72.3
	Chasing, intercepting, abuse, threatening to others	17	3.5	3.5	75.8
	Random possession of others' property or damage, occupying public or private property	111	22.8	22.9	98.8
	Creating disturbances in a public place, resulting in serious disorder	6	1.2	1.2	100.0
		484	99.6	100.0	
		2	0.4		
Total		486	100.0		

As we all know, the behaviors of the chasing, intercepting, abuse, threatening to others and creating disturbances in a public place, resulting in serious disorder have the least proportion. It conforms to our knowledge about the traditional picking quarrels and provoking troubles crime. The definition of "public" expanding interpretation is including cyberspace. The cyber alienation of traditional picking quarrels and provoking troubles crime are caused by the virtual and the generational differences of the network. The virtual has the definition which has the technology dimension and the social dimension. At the same time, the cyberspace is changing from the information media to the life platform. This generational difference has become a powerful booster of crime.

4 Xiaobin Chen. Analysis of cybercrime cost and control.2002-10,Vol.18 NO.6,p126

Crime and punishment

The release of judicial interpretations relevant to the cyber picking quarrels and provoking troubles crime means that the cyberspace has the nature of public. This trend is unified with the security policy making of other countries[5]. The crime motive of picking quarrels and provoking troubles is out of social discontent mood. And this is definitely a serious challenge to the normal public order. It is not only that the cyber picking quarrels and provoking troubles crime have the constitutive requirements of the picking quarrels and provoking troubles crime. But it, as a new form of crime, has new features. It mainly reflects its objective behaviors. These behaviors are using the network abuse behavior and the behavior of fabricating and spreading false information, creating disturbances. What is more important, those behaviors are identified as crime that must reach the legal level.

THE FIGHT AGAINST THE CYBER PICKING QUARRELS AND PROVOKING TROUBLES CRIME AND THE CRIME PREVENTION

To strengthen the network legislation, making the network running in justice

The network management experience of developed countries and regions in the world shows that the suitable design and implementation of network legal system is the fundamental guarantee for safeguarding the order of Internet communication and promoting the development of network culture industry. China has the world's largest number of Internet users that are experiencing the tough period of reform and opening up. China is in the primary stage of socialism and will be in it for a long time which is the basic starting point of legislation. However, according to incomplete statistics, there are hundreds of various network laws and regulations at present. It is undeniable that the current existence of the network system is imperfect legislation, lack of structure and content and other defects of legislative issues cannot be ignored. All sectors of society have now reached the consensus to strengthen the network of legislation. In this context, practitioners and theorists have many suggestions for the network legislation. In these discussions, it is a good way to carry out the legislation network with unified legislation mode. The legal departments involve many aspects, network as a new thing, if the basic law on the network is not specified (this law should be involved in criminal, economic, civil and other departments law relating to the network part), however, it is hard to expect a department law to further standardize the legislation work of network branch law. It is necessary to continue the strengthening of the network legislation, to make the network running in the justice, thus preventing the crime of picking quarrels and provoking troubles of network.

Carrying on striking the Cybercrime, ensuring a safe circumstance for cyberspace

Our research on crimes frankly aimed at combating them efficiently. Though emerged in recent years as a new type of crime, Cybercrime presents increasing frequency and holds general characters of the traditional crimes. Both the government and related sectors have invested a lot, as the human and financial costs, in combating the cybercrimes. Moreover, the public security organ and other relevant organs have also made comprehensive blow against cybercrimes. To be specific, China has set up two organs in policing mechanism specialized in combating cybercrimes. The majority cases belong to the Criminal Investigation Department with the joint efforts of the Internet Regulation Department. However, when coming across some specific technical cybercrimes, the above working pattern may reverse. In some Chinese mainland regions, public security organs attempt to introduce the so-called virtual community in the daily police work, thus preventing particular potential public security cases from transforming into cybercrimes and nipping it in the bud. The above efforts still need to be examined in the practice, yet the working pattern has made difference in striking the Cyber picking quarrels and provoking troubles crime. Nevertheless, the fight against the Cyber picking quarrels and provoking troubles crime cannot be conquered with the pure effort of technique, the arduous war also need the cooperation between the traditional criminal investigation work with community policing and the Public security mediation work. Hence, only by striking the cybercrime and ensuring a safe circumstance for cyberspace can we effectively control cybercrimes.

5 Lakomy,Miron, The Significance of Cyberspace in Canadian Security Policy *Central European Journal of International & Security Studies* Jun2013, Vol. 7 Issue 2, p. 62-79 p. 18

CONCLUSION

With the development of science and technology, cybercrimes is developing incredibly fast. It is not only a problem which can be solved by the government or by repressive and violent measures, but it is also the enemy of people. The government, the relevant regulatory authorities, self-regulatory organizations of enterprises, individual citizens have been paying more and more attention to the creation of a good cultural environment in China. Actively guided public opinion is a good method that can prevent crime. We have to put a lot of manpower and resources to build a better network environment. A better network environment cannot exist without the stricter legislation and effective fight against cybercrimes. It is a long way to effectively fight against the new types of cybercrimes.

REFERENCES

1. Xiaodong, Teaching Books of Computer Crime Case Investigation, Beijing, CHN: Publish-House of China People' Public Security University. TSBN 978-7-5653-0068-4/D.0048: 2010
2. Goode, Luke. Cultural citizenship online: the Internet and digital culture. *Citizenship Studies*.Oct2010, Vol. 14
3. Feng Wan, Analysis on cyber culture and characteristics. *The education academic issue*.2010-4
4. Lakomy Miron, The Significance of Cyberspace in Canadian Security Policy. *Central European Journal of International & Security Studies*. June 2013

UDC: 343.85:[343.4/.5:621.395.721.5

THE PREVENTION OF NETWORK SECURITY THREATS IN MOBILE AGENT SYSTEM

Fangzhou He[1]
National Police University of China, Shenyang

Abstract- Mobile agents are computational systems that can travel autonomously among different nodes in the network, in order to achieve a user or an application's goals, such as computation or information collection. Data transports of mobile agents occur between distributed mobile agent environments, which are placed on diverse agent platforms. Mobile agents can be implemented in short order, can reduce network latency, and can interact with each other and different environments automatically. However, these characteristics also disclose some security issues, such as unauthorized access, modification of data, and network security threats. The security issues of mobile agent are especially important for e-commerce applications, including stock markets and electronic auctions.

Keywords: Network Security, Mobile Agents, Security Issues.

INTRODUCTION

This paper explores the common network security threats in mobile agent system, and then provides suitable solutions and security techniques to keep the mobile agent system safe. The rest of this paper is structured as follows: In section 1 we investigate the characteristics of mobile agent system. In section 2 we discuss the security issues when adopting the mobile agents. In section 3 we analyze the security principles for protecting the mobile agent systems. In section 4, we provide suitable security techniques in mobile agent system. In section 5, summary and conclusion are presented.

THE ADVANTAGES AND DISADVANTAGES OF MOBILE AGENT SYSTEM

Mobile agents provide a new possibility for the development of applications in distributed systems. Mobile agent is a kind of special agent that can move from one platform to another where it can continue its tasks. The applications of mobile agent technology are diversiform which include e-commerce, personal assistance, real-time control, distributed information search and retrieval, monitoring, military command and control, network management, building middleware services, parallel processing, and so on. There are large numbers of advantages of using the mobile agent paradigm rather than traditional paradigms such as client-server based technology. Using a mobile agent paradigm could reduce network usage, improves fault tolerance, dynamically updates server interfaces, introduces concurrency, and assists operating in various environments.

Although numerous benefits are expected, mobile software agents also have some disadvantages which primarily in the area of security. These disadvantages have raised many concerns about the practical application of mobile software agents. One of the most important is the possibility of tampering an agent. In the mobile agent system, the agent's code and internal data could be easily changed during the transmission or at the malicious host sites.

The security issue of mobile agent has triggered much research effort in order to find a suitable solution, thus users will be cautious to decide if using mobile agents. Current research efforts in the area of mobile agent security adopt two different points of view. Firstly, from the platform standpoint, we need to protect the platform from malicious mobile agents, such as viruses and Trojan horses that are visiting it and depleting its resources. Secondly, from the mobile agent viewpoint, we need to protect the agent from malicious platforms[2]. Both points of view have attracted much research effort.

The purpose of this paper is to discuss various security issues related to mobile agent systems, and discuss main solutions to keep both mobile agent and mobile agent platform secure.

1 ceo_xp@msn.com
2 Chris Mitchell, Institution of Electrical Engineers. Security for mobility, 2004.

SECURITY ISSUES IN MOBILE AGENT SYSTEM

The most valuable property of mobile agents is the mobility. However, because of this benefit the mobile agents could be exposed to multiform attacks, such as intentional or accidental misuse of the information, data, or resources of hardware or platform; subverted, destroyed, stolen, and captured by other malicious agents and platforms. As the following, we will divide these attacks into four categories: agent to agent, agent to platform, platform to agent, and other to agent platform, and discuss them with more details.

Agent to agent

The agent to agent category describes some types of threats in which malicious mobile agents utilize other agents' security flaws, and attack other normal agents. These threats include denial of service, masquerade, unauthorized access, and repudiation.

Agent to agent: denial of service

The malicious mobile agents may destroy the execution layer which cannot access the system resources or services, and it can also send incorrect or trash information for preventing other agents to reach their goals punctually or correctly, such as block network, delete important files purposely, or a malicious mobile agent at work on another agent in an endless transport task or interact with the agent in particular transport task with the insignificance and single purpose for using up the agent's resources.

Agent to agent: masquerade

In this attack, a malicious mobile agent may endeavor to camouflage its personal characteristics in order to trick the agent who is communicating with it, and gain access to host resources and services, or destroy the whole host. For example, a malicious mobile agent may pose as a trusted vendor that provide products and services, and attempt to deceive other agents to furnish some useful information for it, such as bank account information, some types of digital cash, credit card details, or other important personal information. Masquerading as malicious mobile agents damage both the agents that are deceived and the agents whose identity were stolen, particularly in agent societies, where the reputation is recognized and used as a kind of ways and means to build trust mechanism.

Agent to agent: unauthorized access

If a mobile agent platform has powerless or no access permissions components and encryption techniques at all, a malicious mobile agent can directly disturb other agents by reworking or accessing the agent's code or data, or by invoking its public methods, such as reset to initial state, attempt buffer overflow, and so on. Changing of an agent's code can thoroughly modify an agent's behavior, such as turning a normal mobile agent into a malicious one. A malicious mobile agent may also attempt to access the services and resources of a host computer without correct permissions, and steal private information, such as clandestinely recording a user's private information, and then transmitting it to an unknown site.

Agent to agent: repudiation

Repudiation takes place when an agent communicates or transacts with another agent, but later proclaims that the communication or transaction never happened. Repudiation is really not an easy thing to solve except in case if the proper mechanisms are provided, because it is difficult to estimate if the motive of repudiation is intentional or just an unintentional mistake. Because an agent may repudiate any communications or transactions and bring on a misapprehension, it is important to provide the transaction maintenance records for both mobile agents and agent platforms to help solve this kind of debate.

Agent to platform

The agent to platform category describes some types of threats in which malicious mobile agents utilize an agent platform's security weakness, and attack other normal agent platforms. These threats include denial of service, masquerading, and unauthorized access.

Agent to platform: denial of service

In this attack, the executing mobile agent may overload an overmuch amount of the agent platform's operation resource or service, or terminate or directly shut down the mobile agent platform. The cause for this kind of attack can be intentional by executing attack scripts of malicious mobile agent to exploit system security weaknesses, or accidental through program design bugs. The mobile agent system must approve an agent platform to operate and execute the agents that their codes have been generated by any other organizations and also may have not been tested in an actual application environment. Thus, we need program testing, independent testing, design reviews, configuration management, and other system engineering techniques to help us to avoid malicious mobile agents into an organization's system.

Agent to platform: masquerade

A masquerading agent disguises another agent's identity in order to access the platform resources and services, or bring other mischief to damage the platform. The masquerading agents also mask as other unauthorized agents, and shift the faults of some behaviors that they do not want to be held responsible.

A masquerading agent can destroy the normal agents that have constituted in the agent societies and their correlative reputation.

Agent to platform: unauthorized access

In unauthorized access attack, a malicious mobile agent may try to access the services and resources of the platform without appropriate permission, this kind of attack may damage both normal agents and the agent platform. In order to prevent this attack, a mobile agent platform must provide a security policy specifying access control mechanisms applicable to various mobile agents. This kind of access control mechanisms need the mobile agent platform to assign a mobile agent's permission and each mobile agent must keep to the platform's security policy for interacting with each other.

Platform to agent

The platform to agent category describes some types of threats in which malicious platforms attack the mobile agents. These threats include denial of service, masquerade, alteration, and eavesdropping.

Platform to agent: denial of service

A mobile agent look forward to the platform can implement all of the agent's requests faithfully, allocate resources averagely, and provide uniform quality of service. However, a malicious platform may disregard all of the requests of trusted agent, insert unacceptable delays for critical tasks, and refuse to run the codes of agent or end the agent's service without any prompt in advance. On a malicious platform, the normal agents may become deadlocked if the agents waiting for the results of a nonresponsive agent. A normal mobile agent may also become livelocked when the agent performs some tasks continuously and may never complete these tasks.

Platform to agent: masquerade

In masquerade attack, a malicious mobile agent platform may mask as another platform in order to mislead trusted agents about their real goals or correlative security mechanism. This kind of malicious mobile agent platforms may lure trusted agents to communicate with them, and then obtain important private information from these agents, or even damage the foreign agents or the platforms whose identity were stolen. The malicious masquerading agents can damage other agents through the messages and the behaviors; however a malicious masquerading platform can do more damage through misleading agents than a single malicious agent.

Platform to agent: alteration

In the alteration attack, a malicious platform may juggle mobile agent information by inserting, deleting or changing the agents' codes, states, data, and behaviors. This kind of attack may harm other agents and platforms if the agent's code or state was altered by a malicious platform. A malicious mobile agent platform may also modify agent communication messages, for example, change a "buy" message to a "sell" message purposely or change data information in financial transactions. Although this kind of goal-oriented modification of the agent's code is more arduous than changing a transaction message simply, the malicious attacker has a specific motive and guerdon.

Platform to agent: eavesdropping

Due to the fact that the platform can access the agent's code, state, data and behavior, the visiting agents must pay attention to the problem that their financial transactions, trade secrets, marketing strategies, or other important information may be exposed to. In eavesdropping attack, a malicious mobile agent platform monitors the state of a mobile agent, identity of the elements that mobile agent is communicating with, and the types of services requested by the mobile agent in an effort to obtain sensitive information from it. This kind of attack is normally used when the mobile agents' code or data are encrypted. However, in mobile agent systems, the harm of eavesdropping attacks is further deteriorated. Because the mobile agent platform cannot only wiretap communications between different agents, but also can wiretap every single command executed by the agent.

Other to agent platform

The other to agent platform category describes some types of threats in which outer elements, including mobile agent platforms and agents themselves, compromise the agent platform's security. These threats include denial of service, masquerade, unauthorized access, copy and replay, and annoyance.

Other to agent platform: denial of service

The agent platforms provide services which can be accessed both locally and remotely. Thus, the denial of service attacks can destroy the inter-platform communications, and mobile agent platforms are also aggressed by familiar denial of service attacks directed against the communication protocols and operating system infrastructure.

Other to agent platform: masquerade

An agent can request services both locally and remotely. A mobile agent can mask as another trusted agent on a remote platform, and request resources and services without proper permissions, or work together with a malicious platform in order to mislead other remote platforms. In the same way, a remote platform can also mask as another approved platform, and deceive other trusted agents or platforms for their true identities.

Other to agent platform: unauthorized access

Since common attack scripts can be downloaded freely on the Internet, the platform and remote access approach must be protected discreetly. On a remote platform, the agents may request resources and services without correct permissions, and may control all resources directly, or even destroy the operating system. For an administrator, the security mechanisms of remote administration may be advisable that can manage several distributed platforms. However, if remote administration is allowed, the account information of system administrators may become the target of unauthorized access attacks.

Other to agent platform: copy and replay

When an agent transfers from one platform to another, its security issues will be increased at a time. An interceptor can capture a complete agent or a message during transmission, and try to clone or copy the agent or the message, and then resend it. For instance, an interceptor has intercepted an agent's "sell" message, and repeats this message time after time, so the agent will sell times without number.

Other to agent platform: annoyance

The annoyance attack includes opening many windows on the host computer, closing windows without notification, or making the host computer beep ceaselessly. This kind of attacks is not a very serious problem to the platform, but they still need to be prevented[3].

SECURITY PRINCIPLES

For protecting the mobile agent systems, we must rely on some cryptographic techniques. There are four main security principles based on cryptography: integrity, availability, confidentiality, and accountability. In this section, we will briefly discuss a set of security principles in mobile agent systems.

Integrity

The mobile agent itself cannot stop a malicious agent system to change its data, code, or state, however, the agent may try to discover these attacks. Thus, the mobile agent platforms should monitor the agents and protect their data, code, and state that cannot be changed by any other unauthorized agents, and only allow the shared data to be modified by trusted agents or authorized processes.

A malicious platform may change the instruction sequence of the agent cunningly, and disturb transactions between agents and tamper with the sensitive data. Thus, the integrity of the local and remote agent platforms is a very important issue for mobile agent system. Because of releasing open source of operating systems and platforms, unauthorized organizations or administrators can modify the agent platform and the infrastructure facilely, and makes it easier for a malicious platform to harm a mobile agent's integrity that is interacting with a mobile agent platform. For solving this problem, we must provide system access control mechanism to safeguard the integrity of the mobile agent and platform itself. Many security mechanisms of mobile agents must balance the development cost and expectant performance[4]. Thus, under the current security mechanisms, when a particular security-sensitive transaction occurs, agents may choose the mobility first, and then limit the type of the transaction.

Availability

For ensuring the availability of local and remote agents' data and services, timeliness of service must be made, capacity must suit service needs, and distributed data must be provided in an appropriate form. The mobile agent system must be able to provide deadlock management and exclusive and simultaneous access. The mobile agent system also must be able to support fault-recovery and fault-tolerance mechanism, and then the system can discover and recover from software or hardware errors[5].

In a mobile agent environment, the agent system may have to handle hundreds or thousands of computation and communication tasks. However, if the system cannot handle so many requests, it must provide graceful degradation mechanism, and then rapidly inform all of the agents that it cannot provide such service anymore.

3 Jefferey J. P. Tsai & Lu Ma. Security modeling and analysis of mobile agent systems, 2006.
4 Liu Yang. Based on social network crime organization relation mining and central figure determining, 2012.
5 Loureiro S, Molva R, & Roudier Y. Mobile code security, 2010.

Confidentiality

Mobile agent systems must ensure confidentiality of any sensitive information carried by an agent or stored on a platform. The eavesdropping agent can capture private data and obtain an unjust advantage from the message flow and the content of messages. Thus, we must monitor the message flow, and allow mobile agents to detect an ACL (Agent Communication Language) conversation signature pattern for inferring useful information from an agent conversation.

Mobile agents communicate with each other through a proxy, and the proxy's location is well-known. Thus, if the agents attempt to conceal their existence through platform directories, they must keep confidential for their location also, and the platform must be able to compel different mobile agents to become anonymous.

Accountability

Each mobile agent or process must be held accountable for their behaviors, such as change security policies of a platform or access to a file. Thus, every agent or process on a mobile agent platform must be authenticated and identified uniquely. In order to provide accountability, we need to maintain a log of security-relevant events which display the responsibility of agent or process for each event, and must ensure the log be protected against unauthorized change or access. The security-relevant events should include the name of agent or process, type of event, time of event, and the result of the event (e.g., success or failure). This kind of logs also can help the agent platform retrieve important data from a security loophole or software and hardware failure.

Accountability is also necessary when building trust mechanisms among different mobile agents or agent platforms, and can prevent malicious attacks effectively. Although mobile agent which must be authenticated may obey the security mechanisms of the agent system, the malicious actions are still exhibited by disseminating unnecessary information intentionally. Thus, we need to provide an additional auditing mechanism to identify the malicious behavior of agents.

In mobile agent environments, for avoiding masquerade attacks, mobile platforms themselves must be able to authenticate the identity of other agents and correlative platforms. In such a manner, agents themselves must be able to authenticate the identity of other platforms or correlative agents. However, we must establish an appropriate measure for authentication. For instance, if a mobile agent just wants to query a product's price, it may only have to "read" permission, and need not authenticate itself, but if the agent wants to purchase a product, the agent must be authenticated first[6].

SECURITY TECHNIQUES IN MOBILE AGENT SYSTEM

In the previous section, we described some threats and main security principles in mobile agent system. In this section, we will describe various security techniques for protecting both agents and agent platforms themselves. Based on the principle of trust, we will divide these security techniques into two categories: mobile agent security and mobile agent platform security.

Mobile agent security

This section describes a set of techniques which are designed for protecting the mobile agent from the attack of malicious platform. These techniques include mobile cryptography, dummy data, obfuscated code, execution tracing, and co-operating agent[7].

Mobile agent security: mobile cryptography

Mobile cryptography is used to encrypt both data and function of agent, and ensure their integrity and privacy. For encrypted data, the agent data is encrypted and sent to platform for execution. For encrypted function, the function of the agent is encrypted based on some encryption techniques and implemented as a program.

Mobile agent security: dummy data

The dummy data is a specific data which is stored in an agent's database and it cannot be changed when the agent executes its function. Thus, when the agent comes back from another platform, if the detection entities are not changed, this means that the data of agent is not destroyed yet. This technique requires that the dummy data should not be adverse to the results of the detection.

Mobile agent security: obfuscated code

For protecting a mobile agent, we can use obfuscating algorithm to generate blackbox agent from the agent specification, in such a way that nobody can obtain a complete function of the mobile agent. Sometimes an agent only needs to be protected for a short time, therefore, a time-limited protection approach is

6 Neeran Mohan Karnik. Security in mobile agent systems, 2007.
7 Peter Braun & Wilhelm Rossak. Mobile agents: basic concepts, mobility models, and the tracy toolkit, 2005.

proposed as an advisable alternative. The main difficulty of this technique is how to quantify the time limit of blackbox protection provided by the obfuscation algorithm.

Mobile agent security: execution tracing

The execution tracing technique can detect any possible malicious behavior that attempt to tamper with a mobile agent, such as illegal modification of the mobile agent function and state. In this technique, each platform must generate a log for recording actions performed by a mobile agent during its execution. However, the logs bring two disadvantages. One is the size of the logs; another one is the management of these logs.

Mobile agent security: co-operating agent

In order to protect a mobile agent against the malicious platforms, the co-operating agent technique distributes critical tasks of a single mobile agent between two co-operating agents. Thus, this technique can reduce the possibility of the shared data being thieved by a malicious platform.

Mobile agent platform security

This section describes a set of detection and prevention techniques which are designed to keep the mobile agent platform secure against a malicious mobile agent. These techniques include path histories, sandboxing, code signing, proof-carrying code, and state appraisal.

Mobile agent platform security: path histories

The realization of path histories is to let a mobile agent maintain a trusted history record of the platform previously visited by the mobile agents, and the platform can know where the mobile agent has been processed. Depending on the information in this record, the fresh visited platform may determine whether to process or restrict the mobile agent requests and what level of services, resources and permissions should be assigned to the agent[8]. Path histories require each visited agent platform to submit a signed record to the path. This record should indicate the identity of current platform and the next platform's identity to be visited in the mobile agent's travel life. The major drawback of the path history technique is the cost of the path verification.

Mobile agent platform security: sandboxing

Sandboxing is a software technique that can limit the execution of certain code, such as communicating via network, invoking programs on the client side, and accessing to a file system. In order to ensure malicious mobile agents cannot cause any harm to the current platform, the sandboxing technique compels a fixed security strategy for the execution of the remote codes. In a mobile agent system, local agents are processed with full permissions and have access to vital platform resources, and the mobile agents are executed in a very restricted area known as sandboxing, therefore preventing access to sensitive platform resources.

Mobile agent platform security: code signing

The code signing mechanism can distinguish trustworthy code and other untrustworthy objects using the technique of digital signatures, and verify the code identity of producer, then the trusted code can be allowed access to vital platform resources, but the code signing cannot assure that the code is in fact trustworthy. Microsoft's Authenticode is a familiar implementation of code signing, such as Java applets and ActiveX controls. However, there are two major drawbacks of using the code signing technique. Firstly, the code signing technique assumes that all the code producers on the trusted list are reliable, so the mobile agent may obtain full permissions from such a producer. Thus, a malicious mobile agent can damage the whole current agent platform directly, or open a back door for other malicious agents by changing the security policies. Secondly, the code signing mechanism is excessively restrictive towards mobile agents that are coming from unauthentic entities.

Mobile agent platform security: proof-carrying code

The proof-carrying code technique requires an agent to carry a formal proof that the agent can accord with a certain security policy. Then the execution platform can check the agent with the proof before running the agent, and assign proper permissions to the agent. The main difficulty of the proof-carrying code technique is how to generate such proofs in an intelligent and effective way.

Mobile agent platform security: state appraisal

In a mobile agent environment, an agent popularly carries the following information: code, collected data, static data, and execution state. The execution state of a mobile agent is dynamic data which changes during the agent's execution on a mobile platform. The state appraisal mechanism can ensure that a mobile agent has not become malicious or illegal, and also can help a mobile agent platform to detect the current state of an agent, and hence decide what permissions an agent can be assigned to[9].

8 Richard Mörbel & Sönke Schmidt. Prevention and suppression of organized crime, 2007.
9 W. Jansen & T. Karygiannis. Mobile agent security, 2010.

CONCLUSIONS

As we know, the mobile agent system's prospect is cheerful that has already been applied in many familiar fields, such as electronic commerce. However, this technology has brought some very serious security issues also, and then affected the network security. In this paper we have attempted to discuss some main security threats and principles in mobile agent system, and also described a set of security techniques which can enhance the security level for both mobile agents and platforms. Through analyzing such issues, the security of a lot of internet applications will be enhanced. Unfortunately, there is not any single security mechanism which can guarantee true mobile agent system security now. Nevertheless, we can yield powerful security mechanisms through combination of various techniques. Therefore, based on this research, we can say that it is possible to create a secure mobile agent system until a more powerful attacking method is developed.

REFERENCES

1. Chris Mitchell, Institution of Electrical Engineers. Security for mobility, 2004.
2. Jefferey J. P. Tsai & Lu Ma. Security modeling and analysis of mobile agent systems, 2006.
3. Liu Yang. Based on social network crime organization relation mining and central figure determining, 2012.
4. Loureiro S, Molva R, & Roudier Y. Mobile code security, 2010.
5. Neeran Mohan Karnik. Security in mobile agent systems, 2007.
6. Peter Braun & Wilhelm Rossak. Mobile agents: basic concepts, mobility models, and the tracy toolkit, 2005.
7. Richard Mörbel & Sönke Schmidt. Prevention and suppression of organized crime, 2007.
8. W. Jansen & T. Karygiannis. Mobile agent security, 2010.

UDC: 621.397.42
343.123.12

VIDEO INVESTIGATION TECHNOLOGY DEVELOPMENT AND RESEARCH

Hao Liu[1]

National Police University of China, Shenyang
China Criminal Police University, Shenyang

Abstract: Along with more and more application of the idea for strengthening the police with science and technology, and construction of public security information, the video investigation technology has gradually become the fourth forensic investigation method for the public security organization to solve cases following criminal technology, moving technology and network investigation technology.

The video investigation is the result of the combination of modern information technology and investigation practice, which has been widely applied in the practice of modern forensic investigation. It has amply absorbed the excellent achievements of modern information technology, its unique technical features, which can greatly improve the detection ability and detection efficiency of the investigation organization, and that can effectively realize social prevention and control, combat crime and maintain social stability.

In this paper, the author discusses in detail and analyses video investigation from five aspects, the summary of video investigation, the technical features of video investigation, the theoretical basis of video investigation, information gathering, current situation analysis and the application of video investigation in our country, the existing problems and development of video investigation, and the importance of video investigation technology as a new forensic investigation method are fully affirmed.

Keywords: Video investigation; Information Analysis; Detection efficiency; Detection capability.

INTRODUCTION

Video surveillance is being more and more applied by the people in recent years; this is because of the spread of internet, computer technology, the development of modern information technology, and the image processing technology. To maintain the social stability of the peaceful city, large amount of funds have been invested to build the "Sky Net Project" in order to maintain social order. Video investigation technology has been used widely in criminal investigations, economic crime investigations, and duties criminal investigations. Video investigation technology is now becoming the fourth largest investigation technology followed by public security criminal technology, mobile technology, and network surveillance technology.[2] The core content of the video investigation which I collected and analyzed is the investigation of the information about the suspects, circumstances, and legacy in order to help the investigator to determine the suspects, find the clues, and also improve the detection capabilities. However, the study of the video investigation technology is still in the initial stage, and lacks the support of theory in the practice activities; this reduces the effectiveness in the detection activities. So, it is necessary to enrich and improve the theory study in the video technology in order to get enough effectiveness.

VIDEO INVESTIGATION SUMMARY

The concept of Video investigation

Video investigation technology refers to using the video surveillance technology in criminal investigations i.e. to use the video surveillance to discover and keep an eye on during the crime in order to determine physical characteristics of the suspect, and collect and analyze investigation information.[3] The development of the investigation technology is always accompanied by the development of modern science. Investigation must always be followed by the development of science and technology, so as to combat the crime in an effective way in order to protect and the society and keep it stable. The development of video investigation is generated by the video surveillance technology, and has been widely used today.

1 liuhao8142@126.com
2 Zhan Ming Sun, Xiao Chuan Zhang: Application of the Video Surveillance in the Investigation, Journal of Yunnan Police Officer Academy, 2010.4,p.108
3 Tao Li: The research of Standardization of Video Investigation, Journal of Liaoning Administrators College of Police and Justice, 2011.1, p.20

Application of video investigation in practice

Along with the development of "Sky Eye Net" project, the video surveillance system is widely used in every province, district, and special region. Video investigation is used in the public security investigation, criminal investigation, economic crime investigation, and duty crime investigation, thus it can combat all kinds of crime effectively. Installing the video surveillance in main streets, roads, and major criminal areas, could help to reduce criminal activities. According to the different major criminal areas, to concentrate on these areas, put more care and widely arrange, and then set the video investigation system with giving priority to prevention, comprehensive coverage, focus on the care that is established can help effectively combat crime and maintain the safe and solidity of society.

Current video investigation information collection, analysis of the current situation and application of the video investigation at home and abroad

-Analyzing and collecting the current situation and application of the video investigation information abroad.

Today, the developed countries have accumulated a lot of experience in the video surveillance technology, such as monitoring the streets, the county, public community, and large public buildings. The latest developments of the modern information technology, the broadband technology, and the computer technology are continuously applied into the video surveillance systems. Designing the "theater observation" in the United States, The U.S. wants a video surveillance system that can take a clear picture even of the driver's face, to use the video surveillance system to track record and analyze the movement of a car. The system uses high-tech computer technology to identify the make, color, shape, and license plate number of the vehicle which is being supervised, even to distinguish the face of the driver and passengers by the camera.

If the license plate number of the vehicle is recorded in the database, the computer system will automatically make warning. It can also find the parking records of the target vehicle in the past few months, and the computer system even can compare and identify the vehicle which appeared near the place where the terrorist activity happened recently. Even if 2000 cars appear in the same place, the computer system will compare the routes of the vehicle, and find out the vehicle which has the same starting point and the ending point.

The video surveillance technology In China has been developing fast in the past few years, the construction of video surveillance system for security purpose has begun to take place, and many provinces and cities have formed a comparatively fully functional video surveillance systems such as Zhejiang Province. At the end of the year 2000, the installation and application rate of the security system key point unit reaches 100% around the province. And the dynamic video surveillance system for social public security is under construction, the transformation of digital network has been completed. As of June 2007, ☒ in the 11 cities, and 101 counties (city, area)) in the province, in addition to the 4 underdeveloped counties, the other 97 counties (city, district) all has completed first-stage project construction task, there is a number of counties (city, district) that have completed the second-stage or third-stage project construction tasks. The total capital investment is 601000000 yuan in the complete province. The public security has constructed 9245 surveillance points, and has constructed 8044 surveillance points which are based on the platform of public operator.☒

In addition, 8930 surveillance points of web surfing cafes, KTV, hotels, and acquisition of waste material places, are constructed and added up to 26219 already existing ones. In 2006, 2698 criminal suspects were arrested with the help of the dynamic video surveillance system in the province, 2486 public security cases were under investigation, and 1072 criminal cases were cracked. In the past 3 years, 6669 cases have been cracked by using video surveillance, including 296 homicide cases, 293 category five cases, and 6280 robbery cases in Zhejiang province, and the effectiveness of crime combating has initially appeared.

TECHNOLOGICAL CHARACTERISTIC OF VIDEO INVESTIGATION

Immediacy of video investigation

The video surveillance can record the crime process in the direct or indirect way, and record the bio-image, behavior characteristics of the suspect visible, but also property information, the crime scene and other

related information, to support the investigators to improve the ability to crack the case in the effective way.[4] On the other hand, the investigators can understand the case intuitively by watching the video feed, which can be of great help to analyze the case and get clues, and also to determine the number of criminals at the crime scene, physical characteristics and the exact way of performing the crime. This can help speed up the cracking time, reduce the costs, and improve the results. At the same time, the video surveillance can determine the direction and scope of the investigation effectively, and to provide all kinds of effective clues for cracking the case.

On the other hand, the investigators can have a general understanding of the image and behavior characteristics of the suspect through video surveillance, the investigators can even clearly see the physical characteristics of the suspect. The video investigation is developed in the areas with high crime, public security hot spots and feeble prevention and control spots, and the video surveillance can help investigators to carry on monitoring at any time, find out the ongoing crime, and then apprehend the criminal suspect. Video surveillance can help us to improve our ability to directly find and arrest criminal suspects under the condition of dynamic crime.

Objective and details of video investigation

Video surveillance information has all the characteristics of objective, detailed, and accurate visual surveillance. All kinds of crime information are recorded by video surveillance system, thus it can comprehensively and objectively provide the facts which are related with crime. One the one side, the investigators can appropriately carry out investigating at the crime scene and collect and inspect evidence relying on information provided by the video surveillance system, and the investigators also can accurately reconstruct the relevant circumstances which occurred in the criminal behavior during the criminal process, what can provide an exact basis for the development and direction of the criminal investigation. On the other hand, after the case is cracked, during the process of criminal proceedings, the video surveillance can provide real, original, objective proceedings evidence. The information which is recorded by the video surveillance is the legal audio-visual material evidence, and the information can prove the facts of the crime, and then the suspect will be restrained by law.

Repeated use of video investigation

The criminal case can be recorded by the video surveillance through the video, sound recorder, and picture recorder. This could help the investigators repeatedly watching and using the recorded data, information of cases and situation of criminal suspect in the process of cracking cases, and then the investigators can carry on studying and determining in depth. The content of the video information itself cannot be damaged and lost in any form. We can have more profound and comprehensive understanding of the circumstances of the case through watching and using the video information, and the situation of the criminal suspect can be understood and mastered fully. The video surveillance information is different from other investigative information, and the investigators can use and watch the information at any time without causing any damage to the video itself.

Information expanded of video investigation

Investigating through video surveillance gives details to the investigators intuitive image information, etc., through these images and information, analysis and processing, it expands the monitoring information, and fully exploits the information and use of video surveillance. Thus we can easily find the crime suspect's characteristics, direction and possible way of escape, learn the physical characteristics of the suspect, voice, diet, etc., to provide phone calls into specific places (cafes, hotels) and other available depth investigation detection channels, helps to quickly and efficiently determine the scope of the investigation in order to discover and locate the suspect.

Meanwhile, the police department can get additional information through the expansion of video investigation. The investigators can gather information about other criminal suspects in the same case, and also can get an insight in the living exchanges of criminal suspects in the different kinds of cases, in order to string the related cases, and determine if it is the same criminal act, or a group of criminal acts.

4 Xueliang Tang, Behavior and Dignity of Investigation, Chinese Criminology Review, 2012.6, P.14

THEORETICAL BASIS OF VIDEO INVESTIGATION

Space-time theory of video investigation

The space-time of cases is the forming elements of the facts of the case, which is the basis of the case. During the investigation, if the investigators need to know the current situation of the case, the first thing to do is to determine the space-time of the crime. The facts of the case mainly consist of two basic elements: people, and object. The "people" is the key factor in the case and they reflect the facts. The "people" includes the criminal suspect, the victim, the witness(es), etc. The "object" is another basic factor of the case, which can reflect specific facts of the case through the storage information content.[5]

Whether the person or object appearing in the case is associated with the case, the place and time are the main points. When the investigators analyze the case, they will analyze if the appearing people are criminal suspects, victims, witnesses, or attestants. The investigators also analyze the appearing objects, whether they are evidence, clues, or the information pertinent to the case, and the information of time and sequence which is reflected by the objects.

The essence of evidence investigation advocated is the associated investigation, and it is very important to master the relevance to crack the case. The video surveillance can accurately grasp the case point in time, and also can record objective and precise time when the criminal act happened, the process of criminal act, to the final result of criminal act. At the same time, the video surveillance can accurately record the crime scene, from the central to the peripheral area, and then expands to the extended area of the criminal act through video tracking. Through the video investigation, investigators can accurately master the facts of time and space in the case, and then grasp the relevance of the facts of the case and improve the efficiency of investigative work.

The theory of identified the species identification and the same identification of video investigation

Video surveillance can record some information that appear during the process of criminal act, including the contents of the physical characteristics, clothing characteristics, behavior modes, on-site evidence, weapons and vehicles of the criminal suspects. The most important thing is that video surveillance is able to collect two basic elements of the facts which are called the "people" and "object" in the case.

The investigators analyze and identify the content to carry out investigation. The investigators can put information which collected by the video surveillance into two categories. One is able to identify the same information and the other can identify the species of information.

The theory of criminal information of video investigation

Video surveillance can record various kinds of criminal information intuitively, and video surveillance has the highest degree of associating with the initial information which is most helpful for the investigators to crack cases. The most outstanding feature of the video investigation information is the initial and repeated use. The video surveillance can record all sorts of information when the crime act happened for the first time, which can provide strong support for the investigation with the initial information. At the same time, the video investigation information can be repeatedly used without damaging the information itself, and also can exclude the external factors to affect the information itself. That can provide a guarantee for the investigators to understand the case totally.

ANALYSIS AND USE OF THE STATUS OF VIDEO INVESTIGATION INFORMATION GATHERING IN OUR COUNTRY

The collection of video information mainly has two aspects: firstly there is the issue of video surveillance installation and dispatch; secondly there is the issue of retrieval and preservation of the important information. These two aspects directly determine the development and effect of the video investigation work, which is the key to the video investigation.

When the public security organs and other relevant security departments install and dispatch the video surveillance, they must persist on the goal of "full coverage and all-weather surveillance". Make efforts to

5 Zhong Hong Ma, The Comparative Study Between the Investigation Model of Intelligence Information and Traditional Investigation, Police Technology, 2007.6, p.17

establish the video surveillance all-round without loopholes in various traffic arteries, special places, and other areas with high crime incidence. Image information, space-time information and physical characteristics of the criminal suspect are called three aspects of the focus video information. Taking and storing the video surveillance information contain three aspects, taking range, finding surveillance points and preserving information.

Installation of video surveillance

When installing the video surveillance equipment the investigators need to pay attention to several issues. Firstly, when laying the system transmission power lines, the transmission lines often cross roads, trees and etc. These projects must be done by a professional security engineering company, and have a fairly standard design and construction. Secondly, the problem is night's lighting. The effect of cameras installed in some places are good during the day, but the effect of images are bad at night due to the surrounding lighting is not installed and the combat effectiveness cannot be played. The investigators must note the problem of night lighting in the process of installing and ensure the surveillance is installed around the lighting facilities, ensuring the results of surveillance. Thirdly, the camera cannot be installed directly on buildings around or poles, which will not only contrary to the principles of safety, and cannot monitor all-round surveillance for the range effectively. The correct way should be set up the surveillance bracket on the buildings and utility poles. And the surveillance will be installed and fixed. Fourthly, the issues are the installation angle of camera. Because the height of the installation has requirements, some junctions install ball machine at the same time, but also install multiple gun machine to monitor pedestrians and vehicles. However, because the angle is too high, the focal length of the camera is not long enough, most of them monitor from the top to down, the people face which are taken are deformed, which has bad identification. We must have a good height in the installation commissioning, carrying out on-site shooting experiment to ensure to have an appropriate height and normal surveillance effect.

Dispatching of video surveillance

The large direction and target of the dispatching of the video surveillance are "full coverage, all-weather surveillance", striving to achieve the effect of seamless. This requires the video surveillance has scientific layout, making the greatest effort to improve the surveillance system and ensuring the video investigation is able to obtain the corresponding video information in each key points.

Focal points of gathering video investigation information

The focuses three aspects of the collection of the video information include image information collection, space-time information collection, physical characteristics collection of the criminal suspect and behavior characteristics collection. Image information collection is the basis and security of the video investigation. Space-time information collection is the key of the video investigation. Gathering information about the physical characteristics of the criminal suspect and their behavior is the core of video investigation. If the collection of the video investigation information is carried out according to the foregoing, it will help to improve the detection efficiency and crack case quickly and accurately.

Transferring and preservation of video investigation information

Transferring and preservation of video investigation information is the starting point of the video investigation work, the transferring and preservation of the video investigation information is also the premise and foundation of whether the video investigation work can be completed. Thus, the criminal investigation department should often pay attention to the collection of distribution maps of all the surveillance points within the jurisdiction, fully grasp the distribution situation of surveillance points, ensure that the work can be carried out quickly after the criminal case. At the same time, the public security departments should also be noted for periodic maintenance of the video surveillance systems and the inspection for the installation situation of the video surveillance of the entertainment venues.

Analysis and application of video investigation information

The analysis of video investigation information is the core and key link of the video investigation work. After all surveillance information is collected, the investigators decide on how to use this information to

guide investigation, the end result is that all the problems are how to analyze and apply the video surveillance information, how to make this information to help in our investigation work, ultimately guide to crack the case and contribute to the fight against crime.

The analysis and application include image processing of video surveillance information which includes the methods for image enhancement, such as the conversion of surveillance video, clear processing of video surveillance image, difficult video surveillance image processing and etc. Compare and analyze through the physical and behavior characteristics of the suspect in the video investigation information. After obtaining the video information through investigation experiments, the known information obtained about the criminal suspect can be accurately analyzed and measured. Through analyzing the information of video surveillance, investigators can track criminal suspects. The investigators can find related information of criminal suspects through analyzing video surveillance information. The investigators analyze the comparison of video surveillance images, simulate actions and belongings of the criminal suspect at the same time and place, further argue the process of cracking crime of the criminal suspect and wearing characteristics, belongings and vehicles.

PROBLEMS AND DEVELOPMENT DIRECTION OF VIDEO INVESTIGATION

The problems of relatively low quality image displaying and processing technology

The problem has low resolution ratio. There are many reasons that the surveillance image of the video surveillance system has low resolution ratio. For example, the reasons of camera lens, light, use and maintenance, also has the reasons of the selection of surveillance site and equipment's commissioning.

The problem is low pixel. The video surveillance systems, which in order to pursue large coverage, it is a ball machine used for covering the entire intersection in the security surveillance of major traffic crossing. The range of surveillance is too large and people and vehicles are very small in the picture. There are only a few pixels on the face that cannot see the faces and license plates clearly.

The problem is noisy. The noise of video image directly affects the quality of image. The high noise is one of the causes of blurry video image. Because the taken distance is too far, the environment is too dark, signal jamming and other factors will make the noise of the picture increase.

The problem is image quality. The static images are often blurry which is taken by video surveillance system. The reasons of forming blurry are diverse during the filming process, such as the models of defocus blurry, motion blurry, low pixel blurry, noise blurry, low light blurry, low resolution ratio blurry and etc. Each model must correspond to a different processing method, face with the blurred images and attempt again and again with different processing methods.

Problems of lacking supervision and management of video surveillance system

The overall construction thought of image surveillance system for urban social order should according to the principle of who is benefited, who builds, and the thought that government guidance, Social participation, and market operation.[6] According to the requirements of the "Three Basics" project construction, the new residential, hotel and entertainment venues, such as the newly open, proposing mandatory requirements to install the surveillance, and relevant departments should pay attention to the design, construction and acceptance. In particular, some units and regions with high security and defense requirements, such as school, nursery school, hospital etc. These units must actively cooperate with the installation of video surveillance of the investigation authorities, build management institution of the video surveillance, strengthen supervision and do the job effectively.

Installation problems of video surveillance equipment

Because of the angle of the camera installation, at some junctions many gun machines are also installed to monitor pedestrians and vehicles, as well as the installed ball machine. However, because the angle is too high, the focal length of the camera isn't long enough, most of them from up to down, so the taken face is too deformed causing bad identification.

6 Jia Xiang Ding, The analysis of Present Situation and Development Trend of Image Surveillance system for Urban Social Order, Policing Studies, 2008.7, p.78

In recent years, with the widely use of video investigation across a wide range of our country called building the "Sky Net Project". The video investigation has become a new and important investigation mode in the investigation cases. The video investigation helps us improve the investigation efficiency and reduce the cost of the investigation, and the most important thing is to help the public security organs to effectively combat crime and maintain social stability. The structure of video surveillance system, which is more than just the work of public security, also needs the various government departments to work together. I believe that with the progress of science and technology, with further practice and study of the video investigation, the work of video investigation will achieve new successes.

REFERENCES

1. ZhanMing Sun, XiaoChuan Zhang: Application of the Video Surveillance in the Investigation, Journal of Yunnan Police Officer Academy, 2010.4, p.108.
2. Tao Li: The research of Standardization of Video Investigation, Journal of Liaoning Administrators College of Police and Justice, 2011.1, p.20.
3. Xueliang Tang, Behavior and Dignity of Investigation, Chinese Criminology Review, 2012.6, P.14.
4. Zhong Hong Ma, The Comparative Study Between the Investigation Model of Intelligence Information and Traditional Investigation, Police Technology, 2007.6, p.17.
5. Jia Xiang Ding, The analysis of Present Situation and Development Trend of Image Surveillance system for Urban Social Order, Policing Studies, 2008.7, p.78.
6. Calic J., Campbell N., Dasiopoulou S., Kompatsiaris V(2005),A Survey on Multimodal Video Representation for Semantic Retrieval, the Third International Conference on Computer as a tool(Eurocon 2005), IEEE

UDC: 340.134:[343.533::004

SOME ASPECTS OF CREATION OF NATIONAL LAW ENFORCEMENT TRAINING STRATEGY IN THE SPHERE OF CYBERCRIME

Alexander Lepiokhin[1]

The Academy of the Ministry of Interior of the Republic of Belarus

Abstract: the article addresses some aspects of preparing and creation of national law enforcement training strategy in cybercrime sphere, including justification for training strategy, objectives of the training strategy, training requirements, training capabilities and resources and other considerations. Nowadays cybercrime has become the most important and difficult problem for all countries. That is why there is a need for a new approach to combat this kind of crime. One of the ways for resolving this problem is the creation of a National Cyber Centre, which includes practical specialists and scientists and trainers, which will be working there (investigator – 2/3 time -real case, 1/3 working time - teaching trainers - 1/3 time -real case, 2/3 working time - teaching and science).

Keywords: training strategy, cybercrime sphere, main objectives, training requirements, training capabilities and resources, national cyber centre.

INTRODUCTION

As the use of technology increases on an exponential basis, crimes against the confidentially, integrity and availability of targeted computer systems are more common. Offences committed by means of computer systems, such as fraud, child pornography and intellectual property crimes are increasing rapidly. Moreover, police work involves the recognition and collection of evidence in an electronic form in relation to any offence. All these facts call for joint actions of all countries in this sphere.

Within the framework of international cooperation between Belarus and the Council of Europe and the countries of the Eastern Partnership (Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine) our country took part in the project CyberCrime@EAP. One of the focuses of this project is to develop national training strategy in cybercrime sphere.

Adoption and implementation of a sustainable and standard based training strategy for law enforcement officers will mean that at all law enforcement officers receive training at the appropriate level to be able to recognize and deal with electronic evidence, to investigate crimes involving technology, and to investigate cybercrime and forensically examine electronic evidence. The Council of Europe, through the CyberCrime@IPA joint project with the EU encouraged countries of South-eastern Europe to develop comprehensive law enforcement training strategies.

Belarus follows the global trend of moving from an industrial society towards the information one with a rapid growth of telecommunications and interactive technologies in recent years. Today even remote villages may have access to the Internet.

According to the data of the International Telecommunication Union, in 2013 Belarus occupies 41st place by the ICT Development Index out of 157 countries of the world (Korea leads in the ranking) and surpasses most of the CIS countries [1].

Belarus has the National Programme related to the accelerated development of services in information and communication technologies in the period 2011 - 2015. The purpose of the National Programme is to create conditions for accelerated development of services in information technology, promoting the development of information society on the basis of innovation and to improve the quality and efficiency information for the population, business and government, including the formation of the state system of providing electronic services to ensure effective application of modern ICT [2].

The national program includes 9 sub-programs:

"National Information and Communication Infrastructure", "E-Government", "E-Health", "E-employment and social protection", "E-learning and human capital development", "Formation of national content," "Electronic Customs", "Security of ICT and digital trust", "The development of export-oriented IT industry".

1 prav_informatika@mail.ru

The implementation of this programme advanced the use of ICTs both by citizens in their everyday life and in the activities of government and business entities. Nowadays, the Internet is widely used by people and organizations for paying taxes, various utility bills, obtaining information, etc.

At the beginning of 2014 the total number of subscribers and Internet users in Belarus amounted to 9.4 million, of them 8.4 million are private persons. Number of subscribers to wireless Internet access increased to 6.6 million.

At present there are 102,000 registered domain names in Belarus. According to the non-commercial organization CENTR, which studies ways of development of national domain zones (primarily European ones), in November 2013 – February 2014 the BY zone grew by 5.7%, showing the fastest growth among European domain zones. The Belarusian domain zone went ahead of the Portuguese domain zone, the Icelandic one and the Czech one [3].

The domain zone BY is at the peak of its growth in anticipation of the 20th anniversary of the zone's establishment. Over 55% of all the domain names in the Belarusian domain zone were registered in the last two years.

The National Security Concept of Belarus of 2010 mentioned several threats facing the ICT field:

– Rise of crime using ICT technology within Belarus;

– Unauthorised access from outside to the information resources of Belarus that harm its national interests;

– Insufficient safety arrangements protecting the vital information facilities [4].

Since 1999 when information security crimes (cybercrimes) were first described by the Criminal Code of Belarus the advance of information technologies has changed old crimes and has brought about new forms of crimes involving computer data and various computer systems. The statistics indicates that the number of such crimes is on the rise. In 2012 over 2,000 high-tech crimes were recorded. In 2013 the number exceeded 2,500 [5].

Cybercrimes represent an international problem because, as a rule, such crimes are committed by transnational organized criminal groups, the members of which use the Internet, easily cross virtual borders between nations, and exploit the imperfect legislation of various countries. In Belarus the legislation allows fighting such crimes effectively. We understand that domestic and interstate cooperation adequate to these challenges can help law enforcement agencies counteract cybercrimes.

We have an increase of cybercrime such as:

– illegal access to computer systems;

– unauthorized actions with data stored in a computer system;

– online use of stolen credit card;

– skimming;

– illegal online payments;

– production of false cards;

– creation and distribution of viruses, botnets;

– spyware;

– creation and distribution of pornographic content;

– DDoS attacks against websites of public authorities;

– GSM fraud; breaches of telecom regulations, including illegal broadcasting.

Growing of computer-related crime such as:

– advertising and selling drugs (chemical) in Internet;

– money laundering and transferring money throw electronic payment system (e.g. Web money and others);

– sharing of society dangerous information in Internet (about explosive materials, weapons, way of creation of drugs);

– abuse of privacy in Internet;

– human trafficking.

There are some specific crime areas:

– Child pornography on Internet

– Money laundering on Internet

– Using electronic payment systems in criminal purpose

– Other crimes (electronic evidence related to any offence)

THE MAIN OBJECTIVES OF THE TRAINING STRATEGY

On the one side:

– Operatives from Ministry of Interior

– Investigators from Investigative Committee

– Examiners (Experts) from Forensic Committee

– Prosecutors

– Judges.

On the other side:

– Trainers and teaching Stuff from Academy of MIA (Ministry of Interior)

The Academy of the Ministry of Interior provides for university degrees in law (4-year course) with specialisations in various fields related to law enforcement; it provides for most staff of the Ministry's agencies, of the Investigative Committee.

The Training Centre (Academy of MIA) provides training on cybercrime issues for new recruits and international students. The courses, approved by international specialists, include training on child abuse on the Internet and other cybercrime issues.

Within the high-tech crime units (Ministry of Interior and Investigative Committee) the new staff already has certain skills in the handling of electronic evidence. Training is organised on a regular basis to upgrade the knowledge and improve professional skills. These units frequently prepare guidelines for other units of the Ministry and Committee on the handling of electronic devices, interacting with ISPs. Belarus considers that all forms of international cooperation, including joint training, are useful. Arrangements with academic institutes or industry bodies – provided they are not yet in place –would also be an asset to develop and deliver training courses on cybercrime and digital forensics.

The following groups and subjects have been identified as the target for training: First Responder (Operatives from Ministry of Interior), they should know:

– Securing the crime scene

– Digital data storing media and devices

– Operating Systems basics

– Search & Seizure (all digital media, computers and cell phones, network devices that could contain vital information, labelling, packing and transport)

– Types and Modus Operandi of cybercrime and cyber related offences

– Cyber Crime Investigator from Investigative Committee should know:

– Introductory IT forensics & Network Investigations

– Internet Investigations

– Advanced computer technical training

– Computer Forensic (Encase, XWays, FTK);

– Linux & MAC OS

– Wireless LAN & VoIP

– Databases & Data mining.

Experts from Forensic Committee should know:

– Basic computer forensics (Partition - Format, File Signatures, Deleted Files, System Shutdown)

– Operating systems (Linux, Mac, Windows)

– File Systems - Fat, Ntfs, Mac, Linux

– Working principles of data storage (CD/DVD, HDD, Bluray, Flash, MMC etc.)

– Database basics

– Network forensics

– Malware analysis

– Steganography

– Live data forensics

– EnCase

– FTK

– Xways.

TRAINING REQUIREMENTS (NEEDS ANALYSIS)

Specific key points:

1) Collecting of electronic evidence (EE) – type of EE, the way of seizure, discloser of different type of EE
2) Storing of EE (proper methods for this, different type of situation – system on or off mode, packing and labelling EE, creation of proper service document of its actions
3) Transferring EE to examiners (experts) and definite the questions in different situations (it depends from type of EE, mobile phone, hard disk, DVD disks, live-analyse and purpose of analyse
4) Analysing of result of examination with together another evidence
5) Using result in criminal procedure (who, how, goals).

Level of training:

1) First responders (operatives, investigators from local police station)
2) Specialized units of MIA and Investigative committee
3) Experts (examiners)
4) Trainers (teaching stuff).

TRAINING CAPABILITIES AND RESOURCES

For this purpose we can use at first period teaching stuff from Academy of MIA also invited in special cases, questions – investigators, forensic experts and technical specialist

In second period (later) – if we will create Nation Cyber Centre (NCC) - teaching stuff will composed by practical specialists, scientists and trainers which are will be working there (for example- investigator – 2/3 time -real case, 1/3 working time - teaching trainers - 1/3 time -real case, 2/3 working time - teaching and science.

Now we have:

– Academy of MIA

– International training centre

– Practical units of MIA, Investigative Committee which are sharing of practical knowledge.

A course on high-tech crime was introduced at the Academy in 2011 and at the international training centre. It deals with international cooperation, national and international legal framework, investigation measures, interview of suspects and specific cybercrime offences.

The Department on Investigation of Crimes against Information Security and Intellectual Property of Main Investigative Department of Investigative Committee of the Republic of Belarus currently organises another training on electronic evidence, use of special investigative measures and other, as well as on methodology and practice of investigations. The Investigative Committee approved this course and provided for the trainers.

In March 2013, 94 persons attended in Investigative Committee a seminar on cybercrime. Many governmental bodies, including the Academy, the Ministry of Justice, the Prosecutor General and the Ministry of Interior took part in the event.

An international conferences on cybercrime were conducted since 2010 at Academy of MIA, and in 2013 was common conference at the Institute for National Security and in this year such event were carried at Academy of MIA.

THE MAIN OBJECTIVE OF THE NATIONAL TRAINING STRATEGY (OUR GOAL)

is to create a National Cyber Centre (NCC), which includes specialist from each state agency. The Investigative Committee of Belarus in April 2014 has put forward an initiative to set up a center to counteract cybercrimes in Belarus. The official said that plans have been made to set up a cutting-edge center at a Belarusian education institution for the sake of discussing the theory and practice of counteracting cybercrimes. The center will enroll both university professors and law enforcement officers, who specialize in cybercrime investigations.

We think, that the center is supposed to enable research in the area of criminal law, criminal proceedings, and forensics. It will host regular meetings of scientists, representatives of law enforcement agencies and the private sector for the sake of sharing experience and finding solutions to existing problems, for working out strategic approaches to cybercrime control, for working out educational problems for this field.

On April 2014 the Investigative Committee hosted a work meeting to discuss the creation of the cybercrime center in Belarus. The meeting gathered representatives of the Investigative Committee, including those involved in information security crime investigations, representatives of the Supreme Court, the Prosecutor General's Office, the Interior Ministry, the State Security Committee, the Operations and Analysis Center under the President of the Republic of Belarus, the State Border Committee, the State Forensics Committee, and the State Customs Committee. The experts also discussed matters concerning investigations into information security crimes, the application of criminal law norms that envisage responsibility for information security crimes, and procedural peculiarities involved in such investigations.

WHAT WE NEED TO ACHIEVE OUR GOAL

– A decision for creating of NCC from decision makers;

– Modern equipment, soft and methods of forensics, detecting and teaching;

– Preparing of teaching stuff in modern methods in this sphere, by using two languages: Russian, English.

The questions of certifications will be resolved in according of Belarussian Education Code with Ministry of Education and International Partners – may be CoE – ECTEG, Interpol, another international cybercrime centre by recognised of each other.

SOME CONCLUSIONS

1) Creation of National Cyber Centre is main goal of our national training strategy.

2) Participation in EU educational and practical projects (ECTEG, carrying out joint operations in combating cybercrime and sharing information and knowledge is very useful for each side).

3) Practical assistant from EU bodies in teaching methods, equipment and special software is required.

4) It would be helpful to form a permanent international work group (including members from each country of Eastern Partnership and international organizations and experts) for each activity (law enforcement training, judicial training, international cooperation in sphere of cybercrime) and organize an international scientific and practical conference on problem of combating cybercrime in each interesting country (1 conference in each country).

REFERENCES

1. www.itu.int/en/ITU-D/Statistics/Pages/stat/.

2. www.belpost.by/eng/news/NATIONAL-PROGRAM/.

3. http://eng.belta.by/all_news/society/Belarusian-Internet-domain-zone-growth-fastest-in-Europe_i_72682.html.

4. http://www.mfa.gov.by/docs/en/bf_2006/04.National%20security.pdf.

5. http://mvd.gov.by/ru/main.aspx?guid=3311.

6. The date of access 09/02/2015.

UDC: 343.982:004

INVESTIGATIONS ON CRIME SCENE INVOLVING COMPUTER NETWORK TAKING AN ADULTERATED WINE TRADE AS EXAMPLE

Li Na[1]

National Police University of China, Cyber Crime Investigation Department, Shenyang

Abstract: With the development of the computer and Internet technology and with the popularity of the computers and Internet, the number of crimes involving computers is increasing dramatically. The computer needs investigating in most crimes. Besides, it is a good practice to make use of computer network to handle the crimes involving computer network. On some occasions, investigating the computer network is a must and the only way to solve the crimes. During investigating, it is important to follow the appropriate procedure and rules. This paper starts from the specific steps and activities on the crime scene involving computer networks which are considered as the appropriate procedure and rules. Then the paper focuses on a real criminal case to show the investigating methods on the crime scene involving computer network. This paper covers the investigations from the arrival at the computer crime scene to the seizure of the evidence. It shows how important the computer network is in investigating the crime cases.

Keywords: investigate; computer network; crime scene.

INTRODUCTION

With the increase of the crimes involving computer network, the situations in which computer network on the crime scene is examined are becoming common and often it is a must. Many crimes can be solved successfully through investigating the computer network. Additionally, investigating the computer network should be conducted on the crime scene. In the course of investigating the computer network, the examination of the computer network on the crime scene is the key step. It determines the following work on the criminal case. On one hand, the data in the computer network is fragile and volatile and it is easy to disappear and impossible to retrieve, so the forensics must be conducted on the computer scene. On the other hand, the network is very complicated, it is hard to reconstruct and examine it. So it is a must to investigate the computer network on the crime scene to solve the crime. During investigating the computer network, the appropriate investigating activities should be applied. The methods and skills should be used as well in order to solve the crime involving the computer network.

INVESTIGATIONS ON CRIME SCENE INVOLVING COMPUTER NETWORK

On the crime scene, investigating the computer network is very important, as there is almost no standalone computer, almost all the computers have some kind of relevance with the network. Besides, there are two more aspects that cannot be left. The first is to investigate the computer. The second is the traditional investigation relevant to the crime. The computer network should work together with these two aspects to solve the case.

INVESTIGATING THE NETWORK

Because almost all the computers are networked, there must be some clue in the network. The investigator should know much about the network and mine the clue in the network.

Take a cyber theft for example. Except for the basic data related to the cyber theft, the investigator should know how the suspect did it. In order to accomplish a cyber theft activity, the suspect must know the technique or it is very probable to utilize some kind of software to conduct cyber theft software. Sometimes the software or program is in the victim's computer, but it is not always the case. The software may be stored in another computer within the same network. The investigator should examine the network to judge what

1 windlisa@126.com

kind of special software is installed in the computer or in any computer on the network. If there is such technique or software, an accomplice may be considered. If the victim's computer is viewed, the focus is on the remote accessing possibility. View the network information and judge which port is open. It is crucial to determine who visited the victim's computer.

INVESTIGATING THE COMPUTER

There are two kinds of important clues to be mined in the computer. One is the basic volatile datum; the other is the clue which can tell the investigator where the evidence is.

CAPTURING THE VOLATILE DATA

The first and most important information to collect is the date and time of the system and compares it with the Greenwich Time. It can determine when the file was created or when the case happened. Next, the downloading should be stopped, because it is possible to cover the unallocated space which may contain information. As known, if the unallocated space is covered, it is impossible to recover the data stored there.

If the computer is shut down, the volatile data will disappear and usually it is impossible to retrieve them. So the volatile data should be examined and collected right now, including the running processes, the running software, the editing document, the browsing web pages, network information and so on.

Sometimes it is hard to judge what is running according to the screen display, even if it is an application, let alone the background process. The process can tell what is running. Take QQ for example, the QQ icon does not appear in the task bar, but the process of QQ.exe is displayed in the Windows Task Manager, as shown in Figure 1 and Figure 2. According to the Windows Task Manager, we can know what is running.

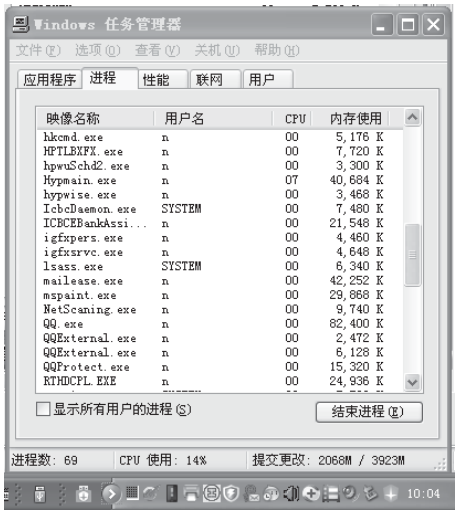


Figure 1 *Windows Task Manager*

Figure 2 *QQ Instant Messenger Configuration Window*

Some software, such as QQ instant messenger, cyber gambling client and financial management software, is password protected. If it is running, examine it right now, or the chance may never come again. The running software often can provide us with critical evidence. Some cyber gambling activities rely on the web pages, but others may rely on the client software. It is usually password protected just as MSN. In an adulterated wine trade case, the investigator finds the password protected financial software is running, so he displays the buy-and-sell records and takes a photo of it. It shows what the adulterated wines are and how many bottles are bought.

Some data of an editing document are not stored in the hard disk, but in the memory, if the computer is shut down or the document is closed, the document will lose some information. So before closing it, remember to load it into the hard disk although it will change the information in the hard disk.

The browsing web page is also the volatile information. The default configuration of web explorer is to save the history records for a certain period of time. It is easy to configure the web explorer not to save the history records even for one day. It is necessary to collect the browsing web pages right now.

MINING THE CLUE

It is the key step which leads to the evidence determining if the prosecutor can win the case in the court of law or at least if a suspect can be caught in time. Before conducting the activity of investigation, view the crime scene and understand the case, knowing about what the case is: cyber theft, locating the suspect on the run or a homicide case. Different cases should be examined in different ways and clues are different, too.

If the investigator wants to locate the suspect on the run, the work guidance is completely different. The software is not important at all. What is the key point is where he is now, so all the information about his possible track is the focus. In a homicide case, the suspect, named Ma Jiajue ran away after killing four classmates. The investigator finds out that many browsed web pages on Ma Jiajue's computer are about a small village in Hainan, including the citizens, the weather, the place to live and so on. With this information it is not that hard to locate the suspect.

TRADITIONAL INVESTIGATION RELEVANT TO THE CRIME

The traditional investigation such as the fingerprint, video surveillance and so on should be conducted on all crime scenes. Besides, it may be necessary to seize the computer. Before you disconnect the wires, mark the connecting wire and the port, shown in Figure 3, for the future reconstructing of the computer or the scene.

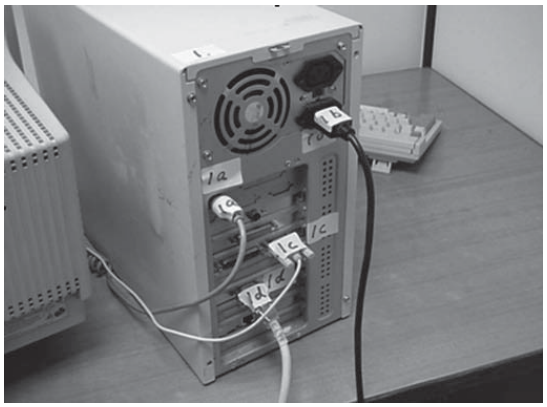


Figure 3 *Marker*

CASE: ADULTERATED WINE TRADE

CASE INTRODUCTION

Take a real case for example: An individual's complaint is about a big KTV entertainment shop. He said that the shop was selling many kinds of adulterated wines, such as Chivas Regal, Black Label and Red Label.

Regarding this case, what needs confirming is how many bottles of adulterated wines on earth the shop has bought and sold.

CRIME SCENE OF THE KTV BUILDING

Now, what should the investigator do regarding this case? First, the investigators examined the crime scene. It is a large shop. It is 6-floored building. It has about 200 rooms. Every room is very big and well

decorated, as shown in Figure 4. As of the business scale, two points can be concluded. The first is that the management way should be good. It is impossible to write the buying and selling records by hand because it is a large amount of work. So it is probable that the shop has the invoicing software that is some kind of computer management system. What we should do is to find out its invoicing software, checking the buying records and selling records to judge the bottles of adulterated wine the shop has bought and sold. The second is that the investigator cannot see any wire in the room because all the rooms are well decorated, so all the wires are deployed in the wall. Besides, the building structure is complicated. So where is the computer, where is the invoicing software? That is a real question.

Figure 4 *Lobby*

Then the investigator asked him about the invoicing software for recording the buying and selling goods. He told the investigator that they did not have any kind of invoicing software. They wrote the buying and selling records by hand. It was impossible to write so many records by hand in such a big shop.

C. INVESTIGATING COMPUTER NETWORK IN THE MANAGER'S OFFICE

Next, the investigator asked the manger to take them to his office. The office room was not decorated that much, as shown in Figure 5. There was just simple furniture and a white wall. We found that there were three computers in his room. The manager said one was for the manager, the second was for the deputy manager and the third was for the secretary. The room was not well decorated, so we could see the wire of the secretary's computer, as shown in Figure 6. And along with the wire, we saw the switch board. There were some wires connected to it. So we counted the wires, 12 wires were connected with the switchboard. That is to say there were 12 computers in this building.

Figure 5 *Manager's office*

Figure 6 *Wire of the secretary's computer*

INVESTIGATING THE COMPUTERS IN THE MANAGER'S OFFICE

The investigator checked the data in the computers of the manager's office. The investigator did not find any kind of invoicing software in the manager's computer and the vice manager's computer. Then the investigator examined the secretary's computer. They found a program. It was a KTV management program, as shown in Figure 7.

Figure 7 *KTV management software*

Besides, the investigator found the Sybase in the secretary's computer. That means that the KTV management application program must access some server.

The investigator should make it clear which server the program was accessing. So the investigator browsed the secretary's computer for the answer. They opened the Sybase and searched for relevant files. Finally, they found out the server's IP address that KTV management program was accessing, that is 129.134.4.200.

SEARCHING FOR THE COMPUTER WITH THE IP ADDRESS OF 129.134.4.200 WITHIN THE NETWORK

What the investigator should do is to search for the computer with the IP address of 129.134.4.200. That computer was accessed by the KTV management program and that was the server which held important data. That computer most probably held the invoicing program.

The investigator searched all the places they could see within the building for the computer with the IP address of 129.134.4.200. The IP addresses of the computers in the building could be any IP address, but not 129.134.4.200, as shown in Figure 8 and Figure 9. Besides, the investigator had not found out all 12 computers. There must have been other computers in some place within the building.

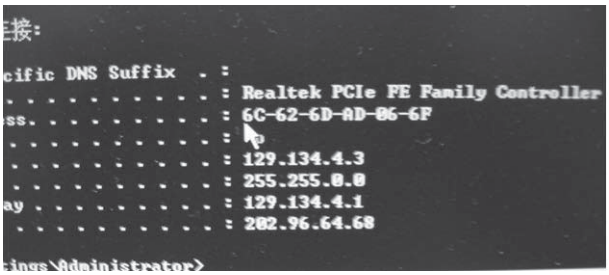


Figure 8 *IP address*

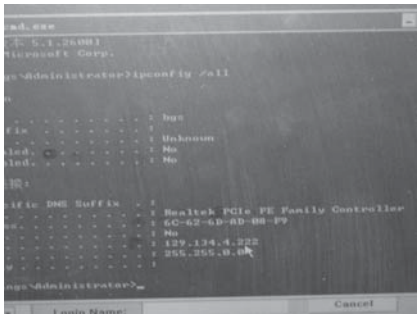


Figure 9 *IP address*

TRADITIONAL INVESTIGATION

By now, although the investigators knew that there were 12 computers and the server's IP address was 129.134.4.200, they could not find them. The shop was too big and the structure of the building was very complicated. The investigator began to change the way of investigating. The shop was big, so there must have been the video surveillance to monitor the shop. The investigators found the display screen of the video surveillance in the manager's office. On the display screen, they found that there was one room with computer they never got in. There were two computers running, one currency counter and one safe. That room could probably be the financial office. The computer in the room could possibly be the server and the computer held the invoicing program.

The investigators found the room at the end of a shadowy corridor and got in. The computers in the room were running and the financial software was running, too. The investigators browsed the content listed in the financial software. They found that the purchase price of the same alcohol was different and the same alcohol, such as Chivas regal, were branded by authenticate labels while the others were not. The purchase price of the alcohol without the authentication label was much cheaper than the others. It was unreasonable. Obviously, the alcohol without the authentication label was adulterated wine.

CONCLUSION

As almost each computer is networked, so it is a key step to investigate the computer network to solve the case. At the same time, the investigation of computer and traditional clues cannot be neglected. They can work together to solve the case effectively.

UDC: 343.123.12:336.722.24
343.53

A STUDY ON A PROACTIVE INVESTIGATING MECHANISM OF CREDIT CARD FRAUD

Yongling Liang[1]
Jing Zou
National Police University of China, Department of Public Security Intelligence, Shenyang,

Abstract: Obtaining credit card information for fake card making and using to carry out fraudulent transactions (hereafter referred to as "illegal make-swipe of credit card") is a serious intrusion to the financial order and it is defined as one of credit card fraud crimes. The activity directly violates the property right of the issuing corporation, the merchants and cardholders. The essay, on the basis of a deep analysis of traditional investigative measures by tracing the money flow after the case is reported and filed where the efficiency of the investigation has been impeded by the problems like cross-regional cashing, virtual identity, time difference in the process of payment and settlement, suggests a large intelligence-led proactive mechanism which aims at detecting suspicious transactions with techniques of credit card fraud detection, cross-searching the information on Internet and public security intranet to ascertain the occurrence of criminal conduct, managing the leads to discover other hidden criminal groups, and obtaining evidence of crime.

Keywords: Credit card fraud, Fraud detection, Proactive investigating mechanism.

Illegal make- swipe of credit card is a common approach of credit card fraud. It manifests as the activity of making and using a fake credit card on card information obtained illegally through the internet. economic loss caused by this activity has reached to several billions every year throughout the world, hence it has become the common concern of police agencies of different countries but up to now the police still lack an effective investigative mechanism to counter the crime. Above all, the complex procedure of judicial assistance and poor intelligence communication system often result in losing the efficacy of leads and chances and push the investigation into a deadlock, especially when confronted with outbound criminal activity. To set up an effective investigative mechanism, a thorough study on the modus operandi of the crime and behavioral features of the criminals involved in the crime should be primarily highlighted.

CHARACTERISTICS OF CREDIT CARD FRAUD IN TERMS OF ILLEGAL MAKE-SWIPE OF CREDIT CARD

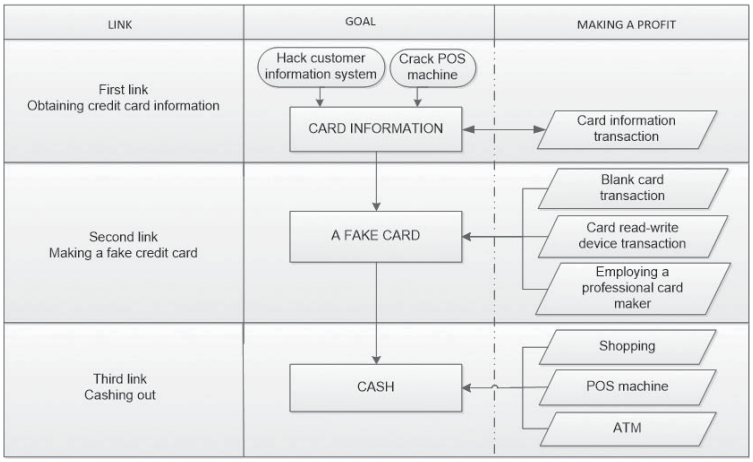
a. Adopting technology-enabled means

Differing from committing other types of fraud crime, criminals of credit card fraud don't contact their cardholder directly, or even their associates. They use hacking techniques to attack websites of banks and online shopping sites, or refit the keyboard with a signal interception equipment and wireless ejector for collecting card information of the clients. As the type and the range of card business develops, the means adopted by criminals also upgrades, which increase the difficulty for investigating department to crack down the case and postpone the investigation.

b. Independent criminal links

Generally speaking, the whole process of credit card fraud includes three stages: obtaining card information, making a card and cashing. Criminals get card information through many ways as logging on a specific website or registering in a chat tool to buy the card information on hacker's websites or from a professional group cracking the POS machine or from the bank staff. Card maker write the stolen information into the track of the magnetic card to make a fake card. In order to cash out, criminals usually buy gold or luxuries in use of time difference created by the payment and settlement system of the bank after the bank closes and the system starts the electronic model. Different steps go relatively independently and each stage has a clearly allocated function. Most of crime groups make profit only involved in one stage, which adds the difficulty for the police to fight against.

1 liang811029@aliyun.com



The criminal links of illegal make-swipe of credit card

c. professional criminal industry chains

Taking the internet as a platform, the criminals join in different communication groups in some real time chatting room to learn the skills, to get in touch with professional crime groups as well as to buy or to sell card information, card read-write device, blank card and POS machine. Thus criminal groups form a cross-regional and cross-professional network with the features of experience sharing, tools cross-regionally selling and homely material receiving. Such features bring about great difficulties for obtaining evidence and locating the criminals.

d. intensive cashing out

The criminals usually take advantage of time difference between payment and settlement. They consume at merchants in shopping mall or withdraw money in a short time and then flee away swiftly before the cardholder, merchant and the bank detect the sanction. Most of the cashing activity takes place abroad and the criminals won't consume at one shopping mall repeatedly, thus it increases the difficulty to trace the fund flow.

DISADVANTAGES OF TRADITIONAL INVESTIGATIVE MEASURES

a. Spatial distance increases time cost

The regular model for investigating the crime is to trace the money flow after the victims report to the police. However, the criminals have a thorough knowledge about payment and settlements of different banks that issue credit card. They explore time and spatial difference to cash out whilst one account may concern several banks in different places. Before the police can trace down the specific spot of cashing out, criminals have already turned the account limit into valuables or cash, and thrown away the fake cards. The leads of the money flow therefore, break off.

b. Frequently altering the telecommunication tools adds difficulty to trace the criminals

Criminals involved in credit card fraud have strong awareness of counter investigation. They contact with each other through internet with the exception of the cashing out period where several criminals consume simultaneously, groups members usually contact through pre-paid phone and dedicated number. Furthermore, they changed mobile phone irregularly or use a phone whose SIM card's home location is in another city. Criminals deliberately set obstacles for the police in investigating and analyzing the traces of telecommunications and therefore gain time for them to flee away before the police can finally locate them.

c. Virtual identity conceals the true identity

Criminals with virtual identity take the internet as a platform of connection and transaction. Most of them have a crime record and have strong awareness of counter investigation, and generally the chat accounts don't contain true personal information, therefore, even the partners engaged in long time cooperation may only know the nickname or the network name. In addition, they log on proxy server in order to hide their own IP addresses. The police can hardly find out the criminal's true identity in such circumstances.

d. Spatial dispersal of the criminals puts the capture in trouble

Criminals of different links disperse in different region or even in different country. Criminals make cards with card information mainly coming from other countries or make cards outbound but cash out domestically. Regular investigation usually points to the criminals on the final link. The ringleaders behind can hardly be apprehended or they can hide themselves soon after they feel something unusual.

e. High awareness of counter investigation makes evidence chain half-baked

As indicated above, criminals on different links or even on the same link communicate with each other through internet, they don't pay much attention to the true identities of each other and they apply jargon to communicate which can hardly be recognized by others, or though the police can understand the meaning of the jargon but can hardly prove it, for instance, they call "inner source" to imply domestic credit card information, "outer source" to imply foreign credit card information and "head information" for the first six numbers of the card number. Some criminals with high awareness of counter investigation even log on internet through a proxy server, and they refuse to send card information in a form of text but via video chat, instead. In such circumstances, obtaining electronic evidence can hardly be realized technically. If, without full preparation, the police carry out a rash action towards the criminals, it will easily alert them and result in the breaking off of the evidence chain, and subsequently affect the effectiveness of the evidence.

A PROACTIVE INVESTIGATING MECHANISM ON THE BASIS OF CREDIT CARD FRAUD DETECTION TECHNIQUES

a. A proactive detective techniques to perceive suspicious money flow

Deferring from traditional investigation, investigating activities in the new mechanism are not initiated by the victims who report the case, but by the detection of suspicious money flow which can be caught promptly though proactively and consistently applying credit card detective method to the transaction data of the bank.

At present, the techniques in detecting credit card fraud which relies on data mining have been developed with growing maturity. Many credit card firms supply anti-fraud service towards credit card's online payment. Those that have been judged to be fraud payments would be refused by the bank. But banks in China have not introduced such techniques so they can't supply anti-fraud service for their customers. Though the detection techniques can't completely prevent the conduct of swiping the fake card, it will help the police to detect the suspicious money flow matching with the credit card fraud pattern if we apply the technique in intelligence system to analyze the transaction record of banks. The application will create chances for preliminary investigation against the possible crime as to greatly save time cost of investigation, and therefore overcome the obstacles like cross-regional inquiry and complex assistance set by criminals and therefore gain opportunities for following work of information sweeping.

b. A proactive mechanism to ascertain the occurrence of criminal conduct

The suspicious money flow can't be seen as the only condition to determine whether there occurs a credit card fraud crime, therefore, we need to set up relevant rules of preliminary investigation so that the police can adopt multiple sources on the Internet and public security intranet to make further investigations against suspicious money flow that happens somewhere frequently in a short period.

A cross comparison among the connected telecommunication trace on foundation of time and space of suspicious money flows, focusing on those phone numbers that come from other areas but disappear after case in question happens can help the police to detect suspicious telecommunication tools, conversation list and account information, etc. In addition, the police can also inquiry information and identify the suspects by exploring such comprehensive information sources as accommodation and flight information, and contact cardholder to make sure if the crime has been committed if they find anyone who is using the card is not cardholder. Once the police are convinced that credit card activity happened the case will then be handed over to the relevant department to file the case and conduct investigation. Meanwhile intelligence department can apply social psychological theory to the analysis of the abbreviation of names, telephone, DOB, license plate number to retrieve on the internet forum and post bar in confirming the identity of the suspect online.

c. A proactive management of the leads to discover other hidden criminal groups

As indicated above, different links on credit card fraud are relatively independent, criminals of each link live or involve in a particular crime in different areas or even different countries. Therefore, the accomplishment of fighting against the kind of crime is usually reflected in the capture of the criminals who are engaged in cashing out whereas information about criminals of other links is hardly to be obtained.

Since proactive mechanism has already started the preliminary investigation while detecting the suspicious money flow, it will greatly help the police take the initiative to make decision how the case would be dealt with before the criminals destroy the trace of connection between different links, that is to say, whether the police need to take actions right away to capture the criminals or they can keep the surveillance to get more information about the case and the criminals.

Through a comprehensive surveillance over the telecommunication tools and online traits and trace of the suspect who is responsible for cashing out, the investigators can acquire the user's name and password and collect the intelligence about the associates as well as the channels of money laundry and cashing out. The police should also highlight the investigation of shipping receipt, the addresses and telephone associated with the suspects. It is quite possible to develop a large scale leads hidden behind in such ways. Furthermore, the advertisement in name of "unsecured loan" and "finance products" actually could be issued by the swiping groups. A cross-comparison between information of the address and telephone number with the existing leads could possibly bring about a final breakthrough for the investigation.

d. A proactive mode to get perfect chain of evidence

Another difficulty in practice is to obtain the evidence to convict the suspect because criminals involved in credit card fraud are usually highly conscious of investigation. They will destroy the communication facilities, credit cards and even laptop computers, so it's necessary to change the investigation direction into proactive mode so as to get the perfect chain of evidence to prove the guilty.

A complete and integrated chain of evidence should contain at least three aspects: the provider (people to steal and provide the credit card information); the maker (people who make the fake card); the user (people who swipe the card on terminal equipment). The investigating department should ascertain the true identity of the criminals before capturing them. Investigators can attack proactively instead of passive investigation in accordance with different situations, contact directly with the criminals through the internet as to dig out the information about when and where card information leaks out and analyze the possible suspect and means of getting information. What is more, the police should estimate the period and place of committing the crime in order to find a practicable chance to conduct the capture in case that they destroy the electronic evidence.

CONCLUSION

The difficulties in investigating credit card fraud in terms of illegal make-swipe of credit card lie in three elements: the concealment of previous links, intellectual means and limited timeliness of the leads. Further element like time cost of traditional investigative mechanism providing the opportunity for the criminals to escape leads to backlog of non-cracking cases. This essay, aiming at solving such problems proposes a proactive mechanism based on the premise of detecting the suspicious money flow proactively, as well as exploiting and digging the suspicious communicating information flow to realize comprehensive detection and complete attack against the crime. The efficiency of this mechanism would undoubtedly rely on the depth and breadth of the information occupied by the police. With the merging of the policing information sources and social controlling information sources and the improvement of investigative consciousness of intelligence officers, this mechanism will function as to fight against credit card fraud in terms of illegal make-swipe of credit card.

REFERENCES

1. Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria, Masoumeh Zareapoor, Seeja.K.R, M.Afshar.Alam, International Journal of Computer Applications (0975 – 8887), Vol.52, No.3, August. 2012.
2. Study on the Fraud Behaviors of Credit-card On-line Crime, Z.H.Xiao, S.GAO, Journal of Nanchang University, Vol.44, No.3, 2013(5).
3. Problems of the crime of stealing, buying and illegally providing credit card information, Q.Wang, Journal of Liaoning Administrators college of police and justice, 2011(1).
4. Applications of Telephone Communication Information in Crime Case Investigation, I. F. Ma, Social Sciences Review 12, 2010.
5. Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, P. N. Grabosky, and R. G. Smith, Federation Press 1998.

UDC: 343.85:[343.533::004
621.395.721.5

ON THE ANALYSIS AND PREVENTION OF CRIME INVOLVING WECHAT

Meng Qingbo[1]
National Police University of China, Cyber Crime Investigation Department, Shenyang
Li Jing[2]
National Police University of China, Basic Study Department, Shenyang

Abstract: Based on the features of difficulty in investigation and positioning of the suspects in crimes involving WeChat, the paper, with a probe into the common means to utilize "shake", "people nearby", "buddy list" and "moments " of the app to commit crime, summarizes the methods of investigation and forensics on account of the accumulated practical experience of locking the suspects with positioning function of the app, taking the chat log as the clue to build up the chain of evidence and faking identity to contact and arrest the suspects, which puts forward the innovative countermeasures to intensify propaganda to strengthen the public awareness, to specify responsibilities of each department to optimize the coordination of supervision, to amend the related law with more explicit electronic evidence system and to stress summarization with coordinated investigation of different police forces, paving a new way and direction for the detection as well as the new theory and technical support for the investigation and crack of the cases involving WeChat.

Key words: WeChat, analysis, investigation, prevention.

WeChat (Chinese: literally: "micro message") is a mobile text and voice messaging communication service developed by Tencent in China, first released in January 2011, which provides text messaging, hold-to-talk voice messaging, broadcast (one-to-many) messaging, sharing of photographs and videos, and location sharing. Up to now, WeChat has more than 800 million registrations, of which 438 million are active users, with 200 million outside of China. As the most downloaded communication software in the world, its influence has spread throughout the Mainland of China, Hong Kong, Taiwan, Southeast Asia as well as the overseas Chinese communities and part of westerners. Meanwhile, with its quality service to the ordinary people, WeChat provides more chances for the outlaws to engage in illegal and criminal activities. As a new type of cybercrime, it has aroused the attention of the whole society and authorities concerned.

THE FEATURES OF CRIME INVOLVING WECHAT

Together with the convenience of communication to mobile phone users brought by WeChat, comes the opportunity for the outlaws to commit crime by the software. The features of the crime are as followed.

1. The suspects are mainly the youth.

As a new thing, WeChat is more popular among the young people, most of whom are more flexible in thought and more introverted in personality. However, this does not rule out the extroverts because some suspects are found rhetoric, witty and humorous, which actually help them win the trust of the victims in a short time.

2. The targets of the crime are mostly women, who are reluctant to report, but the number of male victim has been on the rise.

Owning to the improper attitude towards making friends by WeChat, the victims, without a strong sense of the protection of personal information, are easy to be made use of by others. Along with the development of the crime involving WeChat, some crimes are aimed at specifically for the male victims. By providing false or true sexual services, the suspects invite the male victim to meet them, committing theft, robbery and extortion.

3. Most of the crimes are committed alone but occasionally by complicity.

With strong concealment, the venues of the crime are mostly the hotels, bars, rental housing, leisure clubs and some relatively closed places, where criminal suspects are mainly in a one-to-one relationship with the victims. In recent years, joint crime with WeChat as the means emerge repeatedly, the highlights

1 39411902@qq.com
2 lnsylijing@hotmail.com

of which are the crimes in which the victims are threatened or defrauded to pay the wine with an extremely high price in the bar by the criminal gangs.

4. The time and place to commit the crime is uncertain.

After casting about for the victim and acquiring his or her trust, the suspects can, through the platform of WeChat, commit the crime at any time and place. The means of the crime are always subtle, which make it difficult to find the evidence and detect the crime.

5. The types of the crime are diverse.

Mostly, the cases belong to the violation of property rights, such as theft, robbery, fraud or blackmail. Some cases, such as rape, are the infringement of personal rights. Besides, there is also a possibility for the combination of the types, such as robbery with rape. Recently, prostitution through the channel of WeChat occurs occasionally.[3]

6. The means of the crime are various.

While most of the crimes are committed during the process of the meeting after the suspects has invited the victim to meet, some crimes are committed via sending pictures or other multimedia, in which the suspects has obtained the private photos of the victim with prior trust in advance, and then blackmail the victim by them.

7. Low cost, small risk, but higher success rate.

As long as the suspects can gain the trust of the targets by the sweet words in the WeChat and deceive them to meet him or her outside, the suspects can watch for the chance to commit crime. Many of the targets cannot withstand the test of the words and become the victims. Compared with other crimes, the crime has a low crime cost. Additionally, it is of great difficult for the investigation departments to crack down on the crime in that the suspects won't leave their true names in most cases. The inadequate precaution of the victims contributes to the higher success of the crime as well.

8. It is difficult to fix the evidence.

With the multiple accounts on the internet other than the real name registration, the suspects always won't leave their true information, making it difficult to match the chat record with the corresponding suspects. Plus, network evidence, if not saved permanently, will be overwritten by the new information within a short period of time. Thus, such cases generally require the use of other evidence to support, such as the victim's complaint or the defendant's confession, and part of the circumstances of the crime can't be supported by the evidence. Due to such reasons as being shy to speak out after being defrauded by the love swindler, quite a few victims choose not to report the case to the police, allowing the suspects to become "a fish that slips through the net ".

THE COMMON MEANS OF THE CRIME INVOLVING WECHAT

1. Committing crime through the function of "shake" and "people nearby"

The app is a popular smart phone software, by which you can find people near you using the same software in real time, and the use of "shake " to shake your phone for several times can actually help you find the people using the same function nearby. Criminals tend to utilize these functions to accost the young and inexperienced women inviting her to meet them for recreation or dinner, committing fraud, robbery, rape and other crimes after gaining the trust of them.

2. Committing crime through the function of positioning

The location information is recorded and kept for a period of time in default configuration which exposes some privacy as a serious security hazard when the WeChat users use the "shake" and "people nearby" functions.[4] The outlaws know you accurate location by the positioning function and commit a crime by means of tracking consequently.

3. Committing crime by masquerading as WeChat friends

There are some loopholes of the app.'s identity authentication in that the profile photo and WeChat ID are free to change. Therefore, the outlaws have an opportunity to masquerade as WeChat friends by identity theft. Anyone can replace the profile photo and WeChat ID with official profile photo and " WeChat assistant" ID, which is the official account. Then they can send you all kinds of information, such as checking the privacy issues, committing financial fraud, sending virus link or inducing you to do the corresponding operation without any precaution in the name of WeChat assistant. What's more it's very easy to be entrapped

3 The sequel of the exposure of prostitution by WeChat by CCTV http://news.hf365.com/system/2013/11/19/013562274.shtml.
4 Personal data accessed via WeChat used to aid crimes http://www.zdnet.com/article/personal-data-accessed-via-wechat-used-to-aid-crimes/

when it comes to money, property, meeting and other important matters if the users are forced to pull into some groups (some real acquaintance in them) for malicious intention.

4. Committing crime by embezzling the information on the "moments" of WeChat

According to the default configuration of the "moments", "strangers are allowed to see 10 photos on the moments", which many users are not conscious of and post a lot of pictures of privacy on it. Opening the app to view "people nearby", you will find you can discover the users of WeChat at will within 1000 meters and browse their photo albums freely. It is almost impossible for your friends to guard against such fraud if the outlaws steal your photos on "moments" and substitute your name for their own.

INVESTIGATION AND FORENSICS OF CRIME INVOLVING WECHAT

Generally, the phone and WeChat terminal are taken as the foothold of the investigation by using the advanced analysis techniques and coordinating the use of mobile phone forensics software and social engineering. The forensics anatomy of the crime helps to search for criminal evidence, verify the criminals, and institute legal proceedings accordingly.

1. The use of positioning function helps to directly locate mobile phone and lock the suspects.

The combination of the orientation of mobile base stations and the WIFI positioning are mainly adopted as the WeChat positioning technology. With the support of "location-based services" and GIS platform, the "people nearby" function of WeChat get the location information to provide users with a function of the corresponding service actually through the wireless communication network telecom operators or external positioning way (e.g., GPS). The precision of WeChat positioning function largely depends on the density of the base station where the denser of base station, the higher of the positioning accuracy. Therefore, the police can get the latest location and movement of the suspects by investigating their WeChat account to help narrow the scope of investigation and locate the suspects precisely.

2. The chat log is taken as the clue to build up the chain of evidence.

Through the analysis of the victim and the criminal suspects' chat log, the voice messages, in particular, can be used to roughly analyze the victim' s identity and acquire some valuable information which facilitate the investigation of the case extremely. By analyzing the chat log, the crime scene and the recent movement can be analyzed to accurately find and arrest the suspects through the nearby surveillance video. Although the chat log cannot be directly presented as evidence in court, it is clearly critical for combating crimes eventually by finding clues, unfolding the details of the case and forming a chain of evidence.

3. The "search" function of WeChat could be used to contact and arrest the criminal suspects.

The real-name registration is not adopted by WeChat so that the profile photo and WeChat ID can be modified at any time. Therefore, the investigators can fake identity to win the trust of the suspects by adding the suspects as friends in the detection of the case simultaneously. And the criminal suspects will be ecstatic with less suspicion to take the bait. It is also an effective way that the investigators can lure them out with the excuse of a date for dinner, etc. and arrest them at the location of the appointment.

THE COUNTERMEASURES OF CRIME INVOLVING WECHAT

Effective governance of crime involving WeChat should focus not only on the investigation and forensics of public security organs, but also on tracing the source to fundamentally eliminate the occurrence of this kind of new network crime to kill them in the cradle. Therefore, how to establish and improve the countermeasure system of crime involving WeChat is particularly important.

1. Propaganda Intensified to strengthen the public awareness

The judicial organizations ought to release warning information and admonish the public of the crime involving WeChat in the light of crime circumstance in time. Furthermore, they should remind users of such crime means to strengthen awareness and not to reveal their own state or travel information through the Internet, television, newspapers, text messaging and other media with multi-channel and multi-form.[5] The buddy list of WeChat platform should be filtered and so-called "friends" meeting invitation should be treated with great caution. The users must identify the identity of the other side and guar-

5 Court officials warn of crimes using WeChat app http://www.chinadaily.com.cn/china/2013-07/09/content_16753873.htm

antee its own security before meeting and make sure mobile phone positioning function closed in due time.[6]

2. Clear responsibilities of each department and combined force of supervision

The software publishers should build sound system to develop safety operation procedures. It is urgent for the WeChat service providers to establish users blacklist with a lifetime ban for the suspects involving WeChat crime and ask the users to register by real name or personal identity information of SIM card. Credit rating or blacklist system should be set to ban or restrict the users of illegal acts with the related information as evidence for preparation of judiciary processing. Meanwhile, the MIIT should strengthen the management of new telecommunication services, including WeChat, Twitter, etc. and establish perfect administrative regulations and rules. The reported account should be strictly monitored for pornography or fraud, etc. through the WeChat reporting function.

3. The amendment of legislation with more explicit electronic evidence system

In the present legislation, there is no specific definition for the category of electronic evidence. Therefore, whether the WeChat records can be identified as electronic data evidence relies on the definition of the amendment of criminal procedure law or judicial interpretation. It is high time that the operators established a unified database to prevent the loss of the electronic evidence for mobile phone chat records and other related information such as Wechat, Twitter, QQ through clear judicial interpretation, electronic evidence collection and the security obligation. In addition, the threshold of the registration of the crime involving WeChat should be lowered to properly simplify some legal procedures for timely and effective penalties by the public security organs in avoid of great impact on social stability.[7]

4. Emphasis on the summarization and the joint investigation of different police forces

Basic information should be well collected from the grassroots. The clues and flaws must be left regardless of the kinds of information platform for the suspects to commit crime. All of the investigation and forensics, network investigation methods, the study and judge of suspect activities, etc. need timely summary to broaden the train of thought of investigators. In view of the characteristics of such cases, the public security organs should actively explore collaborative investigation mechanism of multi-cooperation, give full play to the function advantages of each police classification, intensify joint working, and summarize the investigation technology and strategy against the crime involving WeChat to improve the ability to crack down on the new cybercrime.[8]

REFERENCES

1. Aigen, A probe into the ethical problems of communication with WeChat, China Newspaper Industry, 2012
2. Chen Lei, the Feature, Reason and Precaution of WeChat Crime, JOURNAL OF JIANGSU POLICE INSTITUTE, Jan.2014
3. Court officials warn of crimes using WeChat app http://www.chinadaily.com.cn/china/2013-07/09/content_16753873.htm
4. Personal data accessed via WeChat used to aid crimes http://www.zdnet.com/article/personal-data-accessed-via-wechat-used-to-aid-crimes/
5. Spreading rumors on WeChat is a crime, say Chinese internet police https://www.techinasia.com/spreading-rumors-wechat-crime-chinese-internet-police/
6. The sequel of the exposure of prostitution by WeChat by CCTV http://news.hf365.com/system/2013/11/19/013562274.shtml.

6 Spreading rumors on WeChat is a crime, say Chinese internet police https://www.techinasia.com/spreading-rumors-wechat-crime-chinese-internet-police/
7 Aigen, A probe into the ethical problems of communication with WeChat, China Newspaper Industry,2012
8 Chen Lei, The Feature, Reason and Precaution of WeChat Crime ,JOURNAL OF JIANGSU POLICE INSTITUTE, Jan.2014

UDC: 343.533::004

THE TYPES, CHARACTERISTICS AND COUNTERMEASURES OF INTERNET FRAUD CRIME

Qiang Fan[1]

National Police University of China, Network Information Center, Shenyang

Abstract: With the rapid development of computer network technology and communication technology, the number of internet users grows rapidly, and the number of internet fraud also rises sharply. Internet fraud has several characteristics, such as strong concealment, out of space-time limitation, having objects violated wildly, strong timeliness of evidence, which makes the victims violated wildly and brings great harm to the society. This paper analyzes the types, characteristics and countermeasures of internet fraud crime, and makes the writer's opinion, in order to draw people's alert and attention, avoid or reduce the occurrence of such cases.

Keywords: internet fraud; investigative countermeasures; internet security.

When the internet brings digital convenience to people, it gives the criminals opportunities to commit internet fraud crime by using network technology at the same time. Compared with the traditional fraud crime, internet fraud crime makes full use of the network's own characteristics, such as anonymous, transnational, real-time, and has stronger deception and concealment. So internet fraud crime usually makes more economic loss, wider victims group, larger social harm than traditional crime, and it has become a common issue concerned by all countries in the world.

THE DEFINITION OF INTERNET FRAUD CRIME

Internet fraud crime is such behavior, which is committed for the purpose of making profits, that takes the methods of fabricating facts and hiding the truth, in order to swindle public or private money or property in a large amount[2]. This behavior generally refers to any form of fraud behavior, which makes use of some methods, such as network pyramid selling, internet dating, network of win a prize in a lottery, phishing and so on, to make fraudulent temptations to the victims, to guide the fraudulent transactions, to swindle the financial institutions and to use other ways to conduct the internet fraud crime.

THE MAIN TYPES OF INTERNET FRAUD CRIME

In recent years, internet fraud crime is developing fast with various ways and increasing amount. The main types of fraud are as follows:

Network pyramid selling frauds

The essence of network pyramid selling frauds and the traditional pyramid selling activities is the same. However, their characteristics are very different from each other. Network pyramid selling fraud does not only use the internet to sell physical products or make the development of offline, but also commits fraud crime on behalf of high technology, high intelligence, electronic commerce and so on. Thus, network pyramid selling fraud is more deceptive and hidden, has a more wildly spread range and is in the "gray area" of the industry and commerce supervision. What's more, some new types of network pyramid selling are even more harmful.

Network investment frauds

Network investment fraud means that the criminals use false information to obtain the victim's trust, and then obtain their property[3]. Criminals open a web site similar to that of a well-known company, so that

1 58092638@qq.com

2 Xia Qibo, Liu Jingwei. On Legal Regulation of Internet Fraud Crime [J]. Legal System and Society, 2011 (12)

3 Zhou Fengxiang. The Main Methods and Prevention of Internet Fraud [N]. Jiangsu Economic Daily, 2013 (3)

the victims will believe that they are entering a reliable company and make their investment, and obtain the victim's property. There are also some criminals who use the high profits as bait. After collecting shares fees and secret fees, the criminals will return a small fee to get the victim's trust, in order to prompt the victims to make the wrong investment decision, and get more property from the victims.

By using the network access to personal information fraud

By sending deceptive e-mail, establishing false website and other illegal ways, criminals entice internet users to provide credit card accounts, network password, bank account number and other personal information, and then they use the illegally obtained personal information to swindle the victims or they seek illegal interests by other fraudulent activities. By means of untrue information online, this kind of fraud directly defrauds the victim's bank account number and password, which can get more property and cause serious losses.

Internet shopping frauds

Criminals use a fake identity illegally to register an account on the web. At the beginning, they use an internet marketer to obtain high levels of credit rating at a very low price, and then they sell the cost-effective products on the web. After buyers' payment, they obtain benefits, and then disappear without a trace. Some criminals sell real goods through electronic business, but the goods that they sell are far less worth than the money paid by buyers, and the goods are not guaranteed by any sellers. Because the two sides traded on the virtual platform, once the fraud occurs, tracing is extremely difficult.

Network "phishing fraud"

The traditional method of network "phishing fraud" is that the criminals send group messages to the public, and then use the discount preferential measures to induce consumers to log on clone website and steal their account and password. Now the criminals do not simply use fake sites or send fake link, but use the authentic website to deceive. They combine the cross site scripting technology and "phishing" together. When users enter the normal bank website and click on the link, a similar bank website login page will be popped up at the same time. When the fake network window is stealing the user's account number and password, the users' other personal information was also sent out, which provides more details for the criminals to fraud.

Internet credit card frauds

There are several types of this kind of fraud. The first one is through the network settings. When a user logs in the website, their credit card account is asked to be provided at the same time, which is in order to prove their credit rating. When the user input is completed, there will be plenty of fees deducted from the credit card. The second one is to obtain user's credit card account and password through other means. Then the criminals use other people's credit card to consume on the internet. The third one is to use imitated credit cards to consumers on the internet. The fourth one is to refuse to pay the overdraft after consuming.

Internet dating frauds

The criminals establish internet friendship with the victims through the dating sites and real-time communication tools. And after a period time of contact, they will make up some lies, such as home sick, do business and other lies, to cheat the victim's money. Some criminals collude with the young unemployed women, force them to make friends with the victims on the internet, meet with the victims in the reality, and take the opportunity to blackmail the victims, even directly rob the victims.

Network lottery frauds

The criminals send the winning information to the victims through the internet. When the victims believe the information and contact with the criminals, the criminals will require the victims to pay taxes or dues and other expenses to claim the prize, and then achieve the purpose of fraud.

THE MAIN CHARACTERISTICS OF THE INTERNET FRAUD CRIME

Compared with the traditional fraud crime, the internet fraud crime has the following notable features:

Not limited by time and space, regions crossed, more harmful

Internet fraud crime is not restricted by time and space, and with the help of the internet, the information can be sent quickly. The information can quickly reach any place in the world in a few seconds, if there is an internet connection. The victim group is very extensive[4]. There are usually specially appointed persons who are responsible for each link, from the network registration to the opening an account to send fake information and even the extraction of cash and so on. The criminals often take A place to reside, B place to commit fraud and C place to extract money, which makes them flee from one place to another. In addition, compared with the ordinary one-to-one or one-to- several fraud, the internet fraud usually has a large number of victims and greater harm.

Be difficult to discover, fight against and solve

All the information on the internet that is used by the suspects is not real. So when they succeed in committing fraud, they will destroy all the related evidence and disappear rapidly without a trace. Then, they will use another set of virtual identity and fictitious information to commit internet fraud, "return to one's former career", which has strong concealment. Unlike the traditional crime, internet fraud crime has no crime scene. Besides, the contact between the criminals and the victims is very seldom, so there is little information about the criminals that can be provided by the victims. Thus, internet fraud crime is very difficult to investigate and certificate.

The clues and evidence are of strong timeliness

The use of network and communication record, and the suspects' screen names, QQ, MSN, E-mail, accounts and other internet information are the main clues and evidence sources of the internet fraud cases. However, the internet information is easily damaged, and the suspects' screen names, QQ number, MSN number is often changed, so a large number of clues and evidence in the investigation will be easy to lose.

Not contacts

In the usual fraud cases, the criminal suspect and the victims are often face-to-face, namely "person to person" mode. The victims usually have an intuitive impression of the criminal suspect's physical characteristics. However, in internet fraud criminal cases, the criminal subject and object are usually taking the "back to back" contact mode. The two sides do not contact directly but contact through the internet. The criminals usually take the way of bank transfer implementation to commit fraud, which greatly reduces the risks of committing the crime and makes the criminals hard to seize.

INVESTIGATIVE COUNTERMEASURES OF THE INTERNET FRAUD CRIME

Internet fraud crime is increasingly threatening the people's property and safety, and becoming one of the important factors that affect the societal stability. Therefore, decisive and powerful measures should be taken to reduce this kind of crime.

To take the internet fraud crime into Criminal Law, make it an independent crime

In "Criminal Law of the People's Republic of China", the stipulation of internet fraud behavior cannot prevent, combat and punish this crime effectively. Therefore, it's necessary to improve and modify our

4 Liu Shenshi. Characteristics and the Preventive Strategies of the Network Crime[J]. Legal System and Society, 2014(36)

existing computer crimes. If the related law gets perfect, the lawless situation will not appear when internet fraud crime happened. And criminal law will warn the criminals and make them not dare commit fraud.

To strengthen international network coordination and cooperation

The regional concept of the internet fraud crime is very fuzzy. There is often the case: the criminals commit fraud in country A to the victims of country C by using the internet server of country B[5]. In this case, if these three countries do not cooperate with each other, it is very difficult to get this kind of crime punished. To strengthen international coordination and cooperation should contain three respects. The first one is to enhance the coordination of international jurisdiction. The second one is to encourage information sharing among national crime prevention agencies. The third one is that countries should formulate the legal documents on the nature of convention, and make countries' criminal legislation meet the requirements of the convention, so that it is expected to solve the international issue of internet fraud crime.

To improve the network technology and plug up loopholes

The defects of technology development should be overcome by technology; legal norms are only the temporary supplement when the technology does not work. In this sense, advanced science and technology prevention is the most effectual weapon to the internet fraud crime. At present, special attention should be paid to study, formulate and develop all kinds of industry products that are associated with the internet, such as network scanning monitoring technology, data fingerprint technology, data information recovery, network security technology and so on[6]. These will be helpful in the investigation of the internet fraud crime, and also be helpful for the extraction and preservation of the evidence. Therefore, the country should encourage the related investment, research and development. Besides tax preferences, the government should provide more powerful policy support to the technology development and promotion of this field.

To strengthen the network supervision and monitoring

The perfect network management mechanism can greatly improve the internet security. Numerous internet fraud crimes happened because of the network management negligence. Therefore, it is necessary to build up the management of the network. National safe rank system, internet filing system, information media exit declaration system and specialty products sales permit system must be strictly enforced. In addition, some other important systems, such as practitioners' review and appraisal system software and equipment purchase approval system, computer room security management system and network technology development and safety license system, regular inspection and occasional spot checks system and so on, should be established.

To improve the network knowledge level of the public

The society should strengthen the science popularization and propaganda and education of the network knowledge, and make the people understand the network as much as possible. The government should strengthen the disclosure of the internet fraud crime's new form, and increase propagandist strength of the disclosure and prevention of the internet fraud crime, so that the public in the virtual network space will stay alert to the trap, and enhance their self-protection consciousness, ability and level. Of course, to strengthen the crackdown of the internet fraud and make the criminals have no opportunity is the fundamental way. Only in this way, can internet fraud behavior be really reduced. However, the public's prevention capabilities' improvement and vigilance capabilities' increasing, are the most direct and effective methods to prevent the internet fraud crime.

CONCLUSION

Nowadays, it is a fact that internet fraud crime is becoming more and more serious. And with the improvement of the network popularization degree, internet fraud crime is more complicated on its forms

5 Gao Shang. The Difficulties and Countermeasures of Internet Fraud [J]. Journal of Guangxi Police College, 2014(6)
6 Luo Min. Study on the Filing Dilemma and Countermeasure of the Internet Fraud Crime[J]. Journal of Shanxi Police Academy, 2013(4)

and characteristics. Facing the serious situation, we should take several countermeasures to contain internet fraud efficiently. These countermeasures are to make a clear regulation on internet fraud crime in Criminal Law, to strengthen the network supervision and monitoring, to improve the public's self-protection ability of internet fraud prevention and so on, which will give the criminals no place to hide and contain internet fraud efficiently.

REFERENCES

1. Gao Shang. The Difficulties and Countermeasures of Internet Fraud [J]. Journal of Guangxi Police College, 2014(6)
2. Liu Shenshi. Characteristics and Preventive Strategies of the Network Crime[J]. Legal System and Society, 2014(36)
3. Luo Min. Study on the Filing Dilemma and Countermeasure of the Internet Fraud Crime[J]. Journal of Shanxi Police Academy, 2013(4)
4. Xia Qibo, Liu Jingwei. On Legal Regulation of Internet Fraud Crime [J]. Legal System and Society, 2011 (12)
5. Zhou Fengxiang. The Main Methods and Prevention of Internet Fraud [N]. Jiangsu Economic Daily, 2013 (3)

UDC: 343.4/.5:004.738.1

WEBSITE SERVER CLUES INVESTIGATION TAKE "XIN PU JING" GAMBLING CASE FOR EXAMPLE

Xiao Ping[1]
China Criminal Police University, Shenyang

Abstract: The development of Internet technology has introduced website as the most popular information acquiring and publishing platform. At the same time it has assumed a vital role in the publication of false information and fraud. Online gambling events by websites have also emerged in an endless stream, requiring investigators survey the various types of Web server rapidly and accurately digging out important clues or evidence. This paper introduces the working mechanism of the web server, the website architecture, putting forward the ways of obtaining methods of clues in website servers, taking "XIN PU JING" gambling case for example, applying the inspection technology to remote website servers practically.

Keywords: Web server; Gambling site; Investigate web server; Mining clues.

INTRODUCTION

As various kinds of Internet related cases are emerging continually, the website server has becoming the main target of external attacks or criminals profit tool. Due to the difference between platform structures, the clues obtaining and analyzing method of website server are also different. This paper studies the working mechanism of the website server system, and puts forward the online forensics and offline forensics method for different platform web servers. Lastly, these methods were applied to the gambling case "XIN PU JING" for digging out some important clues.

The web server and database server are separated in some medium or large website systems. With the increase of the amount of concurrent access to websites, the website server platform usually uses some specified cache servers in order to improve the customer experience which stores those data accessed by users frequently into the cache server preventing the application server to become the bottleneck of the whole website platform in the accessing peak of the website. In addition, the designer of website system architecture may adopt multiple cache servers according to actual situation including the complex network environment in China, the gap between the response speeds to users in different regions. Large web server platforms adopt CDN (Content Delivery Network) to enhance the user access experience to websites, which deploy CDN nodes in some main ISP (Internet Server Provider) data center room, so the access users can obtain data from the nearest CDN node physically when they send a webpage request to a website [1] .The CDN architecture is shown in figure 1.

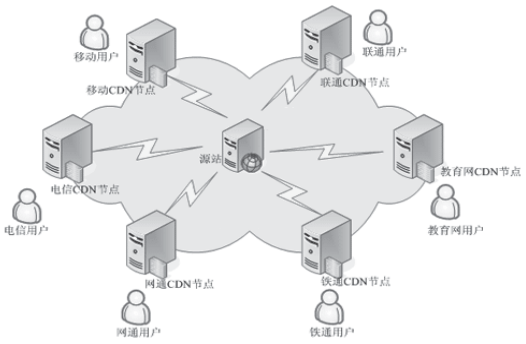


Figure 1 *CND Architecture*

1 18940177780@126.com

THE THEORETICAL BACKGROUND

As far as a personal or small website is concerned, a host assumes the roles including web server, application server and database server in general. The web server is responsible for receiving and responding to the http request from clients, the application server is responsible for executing and interpreting dynamic scripts of server, database server is responsible for storing and managing the background data of website system, the platform structure is shown in figure2.

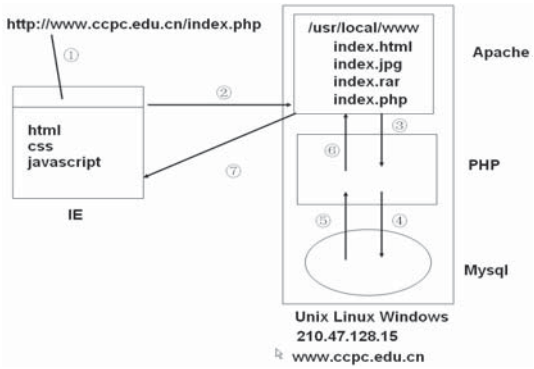


Figure 2 *Request Process by Server Platform*

Take a user request "http://www.ccpc.edu.cn/index.php" for example, on the website server, the specific processing flow for this request is shown as following:

– When an user inputs "http://www.ccpc.edu.cn/index.php" in the browser and presses the "Enter" button, it sends a request browsing the webpage "index.php" to the server.

– After the APACHE server receives the dynamic webpage request, it searches the webpage "index.php" in the main directory of the website, and forwards the document "index.php" to the PHP application server according to the file suffix ".php".

– The PHP application server will process the PHP program codes in the "index.php" file, translate them into the corresponding HTML, JavaScript, CSS code, and generate the HTTP packet, and respond to the client. If the PHP application server finds some SQL statements, then it connects to the specified database server, sends these SQL statements to the database, then to the forth step.

– If the request is the dynamic query, the PHP application server will obtain the data from the database according to the query conditions in the webpage program; if the request is the database store or update operation, the PHP application server inserts these received data into the database or updates the corresponding data, and the operation result returns to the PHP application server at last.

– The PHP application server will arrange the query data or operation results returned by the database forming a table delivering to the APACHE server. In short, the PHP application server translates the PHP codes into some HTML, JavaScript, and CSS codes.

– The Apache server will respond the "index.php" file translated by the PHP application server to the client having send the "http://www.ccpc.edu.cn/index.php" request.

– After the client browser receives the HTTP response package, it interprets and executes the HTML, JavaScript codes in the package resulting the elegant page displaying to the user accessing the website.

From the above data processing flow, we can only see the static webpage translated by the website server consisting of JavaScript, HTML, and other client codes, not the dynamic webpage including database and file operation codes in client browsers. To view the website business logic, database implementation codes, we must find out those website program files in the website publishing main directory.

THE CLUE INVESTIGATION OF WEB SERVER

Web server is a common platform for information dissemination. Some criminals set up their own web server in the LAN, through the relevant network technology, providing illegal services to Internet users, such as gambling, pornography, etc. In addition to providing illegal service by setting up website server, some hackers attack some small website servers to obtain account numbers, passwords and other personal

information through phishing website, webpage linked to malicious program, etc, and web server as an intermediate springboard for the implementation of network theft behavior. In practice, the clue investigation method of web server can be divided into two categories, one is server hard disk forensics, and the other is web server online forensics.

Server hard disk forensics

Website release clues

An important clue in server hard disk is website release information. For the website of ASP or ASP.NET type, web server is powered by Microsoft's own IIS (Internet Information Service), which will display publishing information derived from the configure file "Metabase.xml", including the published website domain name, IP address, etc[2]. So we can fix publishing clues through the configuration file "Metabase.xml" in server hard disk.

```
<IIsWebServer   Location ="/LM/W3SVC/9034674@"
                AuthFlags="@"
                LogFileDirectory="C:\web1log"
                LogFileLocaltimeRollover="FALSE"
                LogFilePeriod="1"
                LogFileTruncateSize="20971520"
                LogPluginClsid="{FF160663-DE82-11CF-BC0A-00AA006111E0}"
                ServerAutoStart="TRUE"
                ServerBindings="192.168.253.128:80:www.shop.com"
                ServerComment="WEB1"
        >
</IIsWebServer>
<IIsWebVirtualDir       Location ="/LM/W3SVC/9034674@/root"
                AccessFlags="AccessRead | AccessScript"
                AppFriendlyName="默认应用程序"
                AppIsolated="2"
                AppRoot="/LM/W3SVC/9034674@/Root"
                AuthFlags="AuthAnonymous | AuthNTLM"
                DefaultDoc="Default.htm,Default.asp,index.htm,Default.aspx,index.asp"
                DirBrowseFlags="DirBrowseShowDate | DirBrowseShowTime | DirBrowseShowSize | DirBrowseShowExtension |
                Path="C:\Shop"
        >
</IIsWebVirtualDir>
<IIsWebVirtualDir       Location ="/LM/W3SVC/9034674@/root/image"
                AccessFlags="AccessRead | AccessScript"
                AppFriendlyName="image"
                AppIsolated="2"
                AppRoot="/LM/W3SVC/9034674@/Root/image"
                DirBrowseFlags="DirBrowseShowDate | DirBrowseShowTime | DirBrowseShowSize | DirBrowseShowExtension |
                Path="C:\新建文件夹"
        >
```

Figure 3 *Example of "Metabase.xml"*

From the configuration script shown in Figure 3, we can dig out the publishing clues including the site's domain name "www.shop.com", IP address "192.168.253.128", and the listening port 80, the directory "c:\web1log" where the log files are located, the home directory " c: \ shop " where the website codepages are located, and so on.

For the website of PHP type, Web server is powered by Apache, we can fix publishing clues through the configuration file "httpd.conf" in server hard disk. At first, it should be determined if the configuration file "httpd.con" includes the virtual host configuration file "httpd-vhosts.conf", if it is included, then the website publishing clues in the configuration file "httpd-vhosts.conf", otherwise in the configuration file "httpd.conf".

Figure 4 *Example of "httpd.conf*

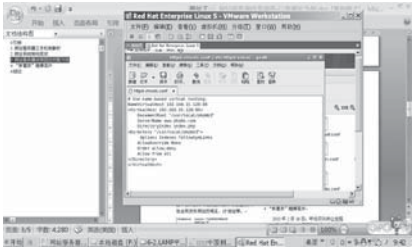


Figure 5 *Example of "httpd-vhosts.conf*

As shown in figure 4, the configure file "httpd.conf" has included the configure file "httpd -vhosts.conf". We can dig out the publishing clues from the configure segment of "httpd -vhosts.conf" shown in figure 5 , which comprises the site's domain name " www.phpbb.com", IP address "192.168.15.128", and the listening port 80, the home directory "/usr/local/phpbb3 " where the website codepages are located, and so on.

WEBSITE DISPLAY EFFECT CLUES

During the examination, fixing the display effect of involved website scripts in server hard disk is also an important aspect, which can support the event that suspects the set up of an illegal website. A browser is not able to explain and implement those website server side scripts. We can fix the display of the server side scripts only when they are published in the corresponding web service platform. For example, the webpage

of ASP or ASP.NET will be published in the platform "Windows IIS ASP SQL Server" and the webpage of PHP will be published in the platform "Linux Apache PHP MYSQL"[3]. During the website rebuilding, in order to fix the corresponding display, we must shield the operation codes linked database in the webpage. The display of rebuilt "ZhenQian Game navigation" website is shown in figure 6.

Figure 6 *"Zhen Qian Game navigation" Website*

After browsing the above website in client, we can find that it has many linkages to the address "http://www.28365365.com/zh-CHS/?affiliate=365_044536". After verification, the "http://www.28365365.com" website is an offshore gambling site. So investigators can dig out the clues pointing out the behavior for offshore gambling site promotion by fixing webpage display effect.

WEBSITE ADMINISTRATION SOFTWARE CLUES

Administrators may be used to utilize some third-party software to maintain website including monitoring software, promotion tools, and so on. The third-party software that we found in the given samples is shown in figures 7 and 8.

Figure 7 *Example1 of Third-Party Software*

Figure 8 *Example2 of Third-Party Software*

Figure 9 shows the clues that the administrators monitored and managed the website "http://www.baode88.com" and other gambling sites. The email auto-sending software, which is shown in figure 10, can promote some gambling websites by auto sending emails.

WEBSITE SYSTEM DATA CLUES

Most dynamic information for all types of websites displayed by webpage is stored in the database, such as membership information, betting records and betting methods in gambling website system. So the interrelated database files need be fixed in the process of examination. Common website system database has ACCESS, SQL Server, MYSQL and so on. The surveying methods of different database are similar. The key database files need to be fixed and reconstructed, so that inspectors can browse table data to find more case clues. The key files of each database are reported as following:

The key data suffix of a file of ACCESS database is "MDB". After installing the correct access database version in system, the inspector can view the content of data tables by double click on "MDB" files [4].

The primary data suffix of a file of SQL Server database is "MDF" and "LDF". The inspector can view the content of data tables by selecting "MDF" file to attach database as shown in figure 9.

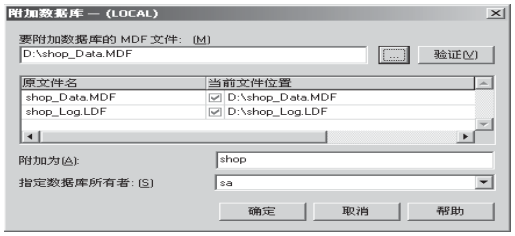


Figure 9 *Attaching Database*

The related data files of MYSQL database are stored in DATA subfolder under the default installation directory. Each database table is matched to three types of data files, where the "FRM" file represents the structure of the database table, the "FRM" file is the data of the database table, and the "MYI" file is the index included in the database table. The inspection process requires the fixation of the above three types of files timely [5-6]. In order to view the content of database tables, inspectors can carry out the operations as following:

Firstly, they can install MYSQL database system software on other computers with the version in accordance with the sample.

Secondly, they can create the database with the same name to the sample.

Lastly, they can copy the above three types of files to the database folder auto created in the DATA subfolder under the database installation directory and cover the original database files.

Web server online forensics

if the involved target website can be visited normally, inspectors should fix the webpage by visiting the target website timely. The inspector should pay attention to check the time consistency and video, i.e. the whole operation process that preserves the screenshot of display effect through accessing the target website.

HOST ADDRESS AND PORT CLUES

Generally, we should locate the web server IP address information by the domain name IP translation function through some tools such as "ping", "nslookup" or websites such as "www.ip138.com", and so on. If the web server is located in the domestic, inspectors can seize the web server according to the details of the case; otherwise they should find clues from the maintaining client to the web server. If inspectors can obtain the information such as administrator's name, password, etc. by interrogating suspects, then we can obtain clues by a remote desktop tool going to online inspection [7]. As soon as connecting the target website, inspectors need to fix the information including IP address and listening port by some commands such as "ipconfig", "netstat ", and so on.

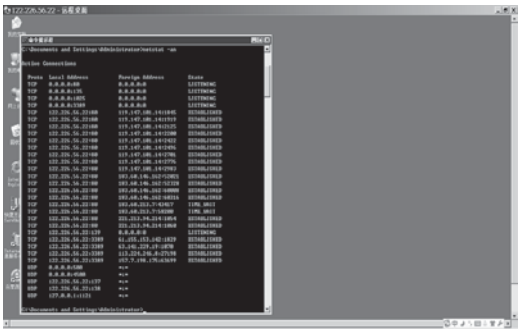


Figure 10 *Result of "Netstat" Command*

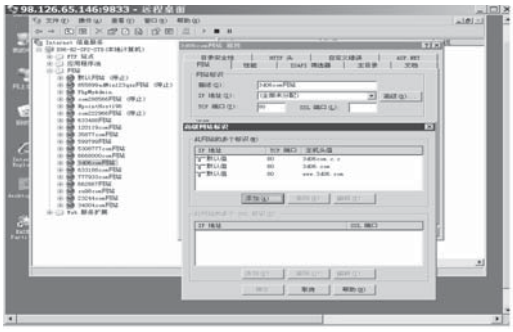


Figure 11 *"3d06com" Website Properties*

WEBSITE IDENTIFICATION CLUES

The website for the ASP type is generally published through IIS. Inspectors can fix website identification information through IIS manager window. As shown in figure 11, the target server starts fifteen website including "3d06com", "35877com" and so on. For more specific identification information, inspectors should open "advanced website identification" window by click "advanced" button in the "website identification" item. For the website "3d06com", the IP address is "default value" denoting local host, the port is 80, and the domain is "3d06com.c.c","3d06.com" and "www.3d06.com" as shown in figure 11.

WEBSITE PROGRAM FILE CLUES

The website program file for a network gambling case, which offers gambling function or promotes agents gambling website, has an important meaning for the conviction and sentencing the crime of opening casinos. After fixing the website identification in a remote inspection process, switch to the "main menu" tab in website properties window as shown in figure 12, all program files of website "3606com" are stored on "d:\www\3d06com\web" directory in the target server. Turn to the folder "d:\www\3d06com\web" and open the default document "index.html", some function source codes are shown in figure 13.

Figure 12 *Main Directory of "3606com*

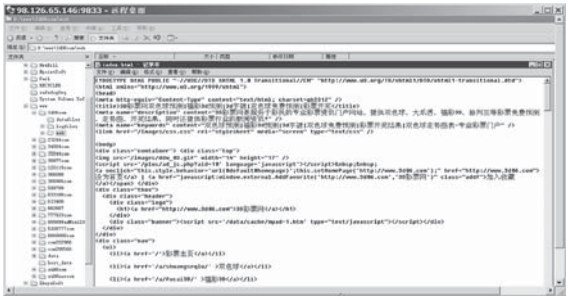


Figure 13 *Source Code of "index.html*

WEBSITE ACCESS LOG CLUES

When going to an online examination, inspectors can confirm if the website starts log record function, the log formats and other information in "website properties" window, as shown in figure 14. More specific information can be mined in "log properties" dialog box showing the log file directory and file name information in figure 14[8], where all log files are located in "C:\WINDOWS\system32\LogFiles\W3SVC722942227" folder, and the file name is associated with the date according to the naming rule, such as "ex120304.log" denoting the log file created in March 4, 2012.

Figure 14 *"Log Properties" Dialog Box*

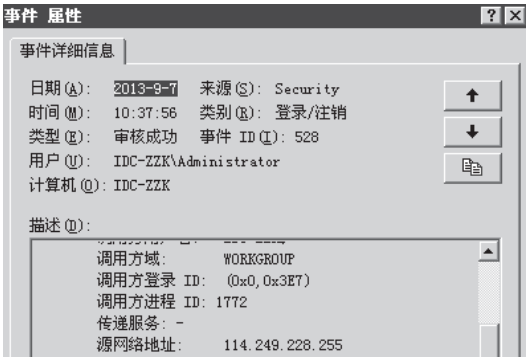


Figure 15 *Event Property 1 of System Log*

SERVER SYSTEM LOG CLUES

System log, also known as host log, is generated automatically by operating system, and is related to the user behavior closely , which records various events occurred in the system, such as user login, logout and other events. Generally, the suspects administrate target server by remote connection. So in the course of examination, mining the "login/logout" event information from involved system log is particularly important. As shown in figure 15, the terminal having IP address "114.249.228.255" logged the inquest host in the "2013-9-710:37:56" moment.

"XIN PU JING" NETWORK GAMBLING CASE

February16, 2013, Public Security Detachment Hulunbeir Yakeshi received a report by Zhang. Zhang said that he registered a user at a gambling website "www.pj1188.com" involved in gambling. Up to report time, he had lost more than one hundred thousand yuans. After conducting reconnaissance of the site found that the situation was true, Public Security Detachment Hulunbeir Yakeshi decided to file on 17 February, 2013.

The target site 'http:// www.pj1188.com " can be visited normally, so first the website display effect should be fixed by visiting the site in client, preserving screenshot of each site column content , and the whole process need to be videoed. Through this step, we inspected the target site containing 33 online gambling projects including "sports betting", and so on.

LOCATE THE TRANSIT SERVER

After the pre inspection, we found that the IP addresses of gambling site, payment platform and online customer service were located overseas. But in order to attract more people to access gambling sites and participate in gambling, suspects usually set up a number of transit servers at home to promote the gambling sites. How to locate these transit servers accurately is one of the core steps for network gambling cases.

In order to check the promotion and proxy effect of a site, suspects often use third-party site or software to view site access traffic. In this case, through analyzing the "XINPUJING "index file source codes which is shown in the figure 16, we found that the site used a third-party site "log properties" dialog box www.51yes.com" to conduct traffic statistics.

```
</script><script language="javascript" src="http://count32.51yes.com/click.aspx?id=3269958(
charset="gb2312"></script>
```

Figure 16 *Part Source Code of "index.html"*

Questioning the suspects, we obtained the username and password of "XINPUJING" registered at "www.51yes.com" site. Logging to "www.51yes.com" site and selecting "Source Statistics" menu, start date for 2013-10-31, end date for 2014-01-05, the statistical result is shown in figure 17.

Figure 17 *Source Statistics Result*

Figure 18 *Released Website Information*

The statistics result shows that the top-ranking addresses are 118.26.226.104, 118.26.226.102 and 42.62.24.51, which accounted for more than 60%. It is clear that the above three addresses conduct promotion for "XIN PU JING" site. After investigation, the hosts corresponding above three IP address belong to "Beijing Ouyi time-space network technology Co., Ltd.".

TRANSIT SERVER REMOTE ONLINE EXAMINATION

Checking the remote online examination of domestic transit server (IP address 118.26.226.104), the inspectors found that the server released three sites, namely "2288sun", "pj1188" and "ld1188", as shown in Figure 18.

Through the further inspection to "pj1188" site, we found that the site's domain name includes "www.pj1188.com", "pj1188.com", "xin22222.com" and "www.xin22222.com", as shown in Figure 19. The "pj1188" site is just the gambling site visited by the above informant. The main directory of the site stored only one file "default.htm". The source code of "default.htm" is shown in Figure 20, which forwards all requests to the site "www.pj938.com".

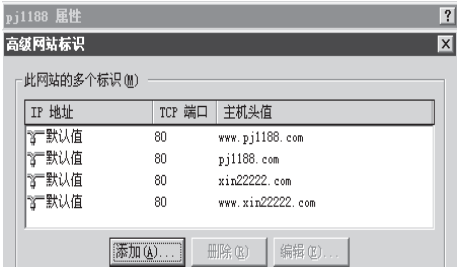


Figure 19 *Domain of "pj1188"*

Figure 20 *Source Code of "default.htm"*

FIXING IP ADDRESS LOGGED TO THE TARGET TRANSIT SERVER

The system host logs for forensic analysis showed that the client setting up IP address 14.249.228.255 conducted the login or logout operation on "2013-9-7 10:37:56", and the client setting up IP address 121.54.175.102 conducted the login or logout operation on "2013-9-10 15:32:40", as shown in Figures 21 and 22.

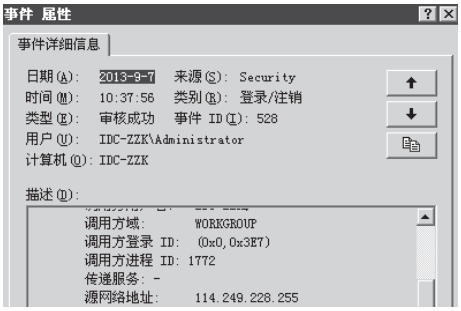


Figure 21 *Event Property 2 of System Log*

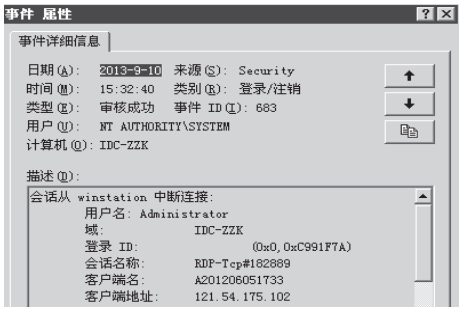


Figure 22 *Event Property 3 of System Log*

CONCLUSION

The paper has presented the clue investigation method of web server including online web server forensics and web server hard disk forensics, and has verified the extraction method of critical information within web server by actual cases to help investigators fix the relevant evidence for locating the attacker tracking or illegal user accurately. These investigation methods are refined from real cases, especially the third-party traffic statistics site "www.51yes.com" playing a key role for detection in "XIN PU JING" network gambling case. The fixing and inspection methods of web server clues should be further improved with the advance of network technology.

REFERENCES

1. Wang Gang: "On the public security organs for reflections on the investigation of network gambling cases" Journal of Legal Latitude 2011:34(1):89-90
2. BenNa Zhou: "Further analysis of Internet gambling cases" Journal of Case Analysis 2013:10(8) 62
3. WeiGang Jiang: "Analysis of dynamic website core technology based on ASP" Journal of Fujian computer 2012:21(5): 120-121
4. Wan Feng: "Study on MS SQL Server database data recovery" Journal of Computer Engineering 2009:56(6):90
5. Liu Bing: "Research on the security strategy of SQL database Server" Journal of The examination Week 2010:23(54): 37-38
6. XiongTao Gong: "Study on the recovery technology of SQL Server database" Journal of Science and technology information 2009:5(27): 210-211
7. Xiao Ping: "Investigation of Common Application Server Clues in LAN" Journal of Information network security 2014:89(4):90-95
8. Wenhua Luo: "The Application of Reverse Analysis on Digital Investigation" Journal of Computer Applications 2011;31(11):S2975-2978

UDC: 343.4/.5:621.395.721.5

RESEARCH ON THE CHARACTERISTICS, TRENDS AND DETACHMENT COUNTERMEASURES OF THE TELECOM FRAUD CRIME

Wang Yahong
Wu Zhaomei
China Criminal Police University, Shenyang

Abstract Telecom fraud crime which can be divided into telecommunication fraud and transaction fraud is a new form of fraud crime. Telecom fraud crime has many characteristics, such as being well-organized and having clear division, costing low but involving large, involving many people and spreading to wide range, the criminals' age being low but the culture level being high. Telecom fraud crime also has a lot of new trends, including continuous upgrading of fraud means, committing crime snugly, intelligent degree being higher, cross-border crime being more obvious. There are also many difficulties to detect and prevent telecom fraud crime. So we should comb investigation clues, obtain evidence, infer criminal identity, determine the suspects, dig more crimes and partners in detection, and perfect laws, strengthen propaganda, consolidate the construction of the public security information, collaborate intimately with related departments, reinforce international and interregional criminal judicial assistance in prevention.

Keywords: Telecom fraud crime, Characteristics, Trends, Detachment countermeasures.

With the rapid development of the financial, telecommunications and the Internet, telecom fraud crime emerged, grew and spread rapidly in China. Especially in recent years, the "non-contact" crime which is implemented with the aid of SMS, telephone, Internet and other means of communication has been showing a high incidence of multiple state, making people suffer great losses, causing strong psychological trauma to the crowd and also posing a grave threat to social harmony and stability. Therefore, summarizing the characteristics of the crime in time, predicting the trends of the crime scientifically and constructing countermeasures of the crime systematically are of practical significance.

THE CONCEPT AND FORMS OF TELECOM FRAUD CRIME

As to the concept of telecom fraud crime, different scholars tend to draw widely divergent conclusions because of different research perspective and route. However these different conclusions can be attributed to two kinds of different opinions, i.e., is telecom fraud crime a new type of crime, or only a new form of traditional crime of fraud? The author thinks that, as a kind of "non-contact" criminal activities, although telecom fraud crime has a lot of new forms and features, it is not enough to make it become a new types of crime, because they are not typical, it will not set new crime regulation and they can still be included by the evaluation model of traditional crime of fraud- "fabricate the facts or conceal the truth", and they are not enough to set up new crime. Therefore, telecom fraud crime refers to, fabricating the facts or concealing the truth for the purpose of illegal occupation, diddling large amount of public or private property by sending text messages, dialing telephone, Internet or other means of communication.

Since telecom fraud crime having various forms, different scholars have made different conclusions (about it). For example, the forms of the crime are summarized as ten types, i.e., slotting card and consuming fraud, tax refund fraud, fake lottery fraud, seducing the remittance fraud, telephone charges owed fraud, fictional first aid fraud, defrauding telephone charge fraud, pretending to be leader fraud, high pay recruitment fraud, fabricating litigation fraud and so on[1]. The author believes that the method listed above can reflect the forms of telecom fraud crime, but this method also has defects, such as the standard not being unified, types being too much, lack of flexibility, and so on. So, the author agrees with this kind of classification, namely the forms of telecom fraud crime can be divided into two categories-- telecommunication fraud and transaction fraud-- according to the means of fraud. Telecommunication fraud is that the criminals send the fraud information actively to the victims through telephone, SMS, fax, E-mail, Internet chat tools, communicate with the victims through these means, and make the victims misunderstand and dispose of the property "voluntarily". These types of fraud contain all kinds of winning the lottery fraud, fraud of pretending to be acquaintances, public service institutions and state organs, refunding tax fraud,

donation for the disaster area fraud, travel opportunities fraud and medical rescue fraud. Transaction fraud mainly occurs in the online trading. The object of this kind of fraud is the consumers or businessmen in the network transaction. The offender usually doesn't send fraud information to the no specific people, but issues false trading information through self-built website, BBS, QQ group or uses third-party trading platform with certain credibility or network game platform to release information, or makes false purchases and sales by taking various means to bypass the third party supervision, using a loophole in the trading platform or using the victim's weakness to defraud others' property. [2]

THE CHARACTERISTICS AND TRENDS OF TELECOM FRAUD CRIME

The characteristics of telecom fraud crime

First, being well-organized and having clear division. Telecom fraud crime is usually an organized and premeditated crime. Therefore, gangs inside are well-organized and have clear division. Gang members are generally divided into three layers, namely the upper, the middle and the lower, which present "pyramid" structure. Gang members can also be classified into several groups according to different responsibilities, which include telephone answering group, mass message sending group, card opening group and withdrawal group. In order to reduce risk, the members of different groups or even the same group don't know each other.

Second, costing low but the amount involving large. First of all, its inputting cost is low and it can be learned easily. In general, simple telecom fraud crime can be completed just by ordinary equipments such as phone, credit cards and group message sender, which can be obtained easily and at a low cost. Even the complex crime, whose input may be higher because of hiring employees and renting the VOIP phone, is still cheaper compared to its high return. Second, the illegal cost is low and the fluke mind is serious. Because telecom fraud crime is a "non-contact" crime which means it's difficult to obtain the clues and evidences, and the legal punishment has not the death penalty, the criminal's fluke mind trying to obtain high profits and escape punishment is more obvious.

Third, involving many people and spreading to wide range. On the one hand, because the crime is the gang crime and the cross-regional crime, the number of the suspects may be larger and the region involved may be wider. On the other hand, because criminals tend to choose non-specific people as object, commit crime on the Internet and release lots of fraud information in a very short time, so the violating range is wide and the number of the victims is numerous.

Fourth the criminals' age being low but the culture level being high. According to materials from the public security organs in various regions, the criminals' age is low but the culture level is high. According to a survey of the suspects somewhere, 65 people are above high school level, accounting for 63.1%, in which 49 people accounting for 47.6% are high school level, 13 people accounting for 12.6% are technical secondary school level and 3 people accounted for 2.9% are above college degree; 38 people are junior high school level, accounting for 36.9%. From the age structure of the suspect, they are concentrated in 18 to 28 years old, mainly in around 20 years old, in which 49 people accounting for 47.5% are under the age of 18 to 20, 44 people accounting for 42.7% are under the age of 21 to 25, 10 people accounting for 9.8% are under the age of 26 to 28.

The trends of telecom fraud crime

First, fraud means upgrading continuously, fraud ways renovating ceaselessly. With the enhancement of the crackdown to the crime by the judicial organs and the improvement of people's awareness, the means and ways of the telecom fraud crime have been upgraded and renovated. The crime has developed from the initial "guess who I am" to winning the lottery, to pretend to be public service agencies or national law enforcement agencies. And the crime becomes more confusing and more harmful to the society.

Second, committing crime snugly and the counter-investigation ability enhancing. Within the organization, members often contact each other in single line, which means there can not be any contact with other group or other person except the "superior". Each group commits crime alone. To avoid the punishment of the judicial authorities, criminals usually open bank accounts with false identity or by hiring others to open. The account information provided to the victim is also not real, so the criminal can hide his true identity. When one member is arrested, other members will be notified to change the contact way immediately, to block the further investigation by the judicial organs. [3]

Third, technological intelligent degree being higher. The tools of the crime experienced a series of changes, from the early use of group messaging device, to the Internet, to the network proxy server, to the wireless adapter, any significant number software, manufacturing background sound on demand. These changes embody that the crime's intelligent level becomes more and more advanced.

Fourth, cross-border and cross-regional crime being more obvious. In recent years, the tendency of committing crime cross-regional and cross-border becomes more and more apparent. Criminals choose a range of telephone numbers to send messages or call, so the victims are not specific and the range involved is quite wide. Moreover, criminals often commit cross-regional or cross-border crimes by making the best use of financial services such as online banking and modern communication network. In the crime, each link such as commanding, dialing, transferring and withdrawing may occur in different regions or even different countries. The characteristic of cross-regional and cross-border is more and more obvious.

THE DIFFICULTIES IN DETACHMENT OF TELECOM FRAUD CRIME

The difficulties of investigation

First, being difficult to obtain clues. On the one hand, victims in a considerable amount of cases are cheated because of coveting interest, so many of them prefer not to report to the police for the face if the amount is not big, so that the judicial organs lose the chance to gain clues early. On the other hand, criminals not only use false bank account information, but also change phone number frequently in order to escape punishment, so it is difficult for the judicial organs to obtain valuable clues.

Second, being difficult to investigate. On the one hand, because telecom fraud crime is a remote and non-contact crime, criminals can complete the crime in a very short time with the aid of modern communication technology. But the information left in the telephone or the account during the crime is always false, so it's bad for forensic. On the other hand, the site feature of crime is not obvious, so it is very difficult for the traditional technology of inspection to play an important role. While the electromagnetic marks such as SMS, web pages, bank card is easy to be encrypted, removed, or tampered with, even if not encrypted, removed, or tampered with, it is difficult to preserve and fix, which also adds difficulty to the forensic work.

Third, being difficult to dig crime deep. From the current cases detected, the case in which all members were arrested is a minority. In the vast majority of cases, only members at the intermediate level or at the bottom were captured, who were responsible for sending SMS, dialing telephone, opening bank account, withdrawing money, etc, and knew little about the organizers at the higher level. Even gang members told the organizers behind the scenes in some cases, it was still difficult to arrest them at the same time, because they often hid overseas and they contacted each other in a single line.

Fourth, being difficult to recover the money in time. Because telecom fraud crime is a cross-regional, cross-border crime, when the crime succeeds, criminals will shift money to overseas with the fastest speed, or transfer money quickly by putting it into multiple accounts, spreading the money to more than one card in a relatively short period of time and then extracting the money from different locations respectively, so it's difficult to recover the money.

The difficulties of prevention

First, laws and regulations being not enough. The lack of related laws and regulations makes the prevention and attack of the crime lack corresponding legal basis. Compared to combating and punishing the crime, preventing and controlling the crime is more important. While preventing and controlling the crime requires the support of the corresponding laws and regulations, only in this way it can be legal. However, the reality is that there is a quite lack of the early laws not only spam messages cannot be regulated by law, but also personal information security cannot be protected by law.

Second, loopholes existing in the management of telecom departments. First, there are large amounts of secret phone cards in society. Since these cards are not registered, they can hide the criminal's real identity, therefore, it is easy to be used by criminals as tools for the crime. Second, group messaging devices lack effective supervision. Due to the lacking of supervision by the relevant institutions, criminals can buy the devices easily, leading to the proliferation of telecom fraud crime. Third, the VOIP phones (also called network phones) lack effective regulations. As the mixing of the Internet and telecommunication network, VOIP service is widely used. However, the service provider doesn't monitor and regulate its users effectively, so criminals can forge special identity, number location by modifying the information and commit crime. [4]

Third, blind areas existing in the management of financial institutions. On the one hand, the real-name system is not completely implemented in opening bank cards. Owing to the vicious competition between commercial banks, some banks handle the card in auditing relatively loosely, to strive for more business and attract more customers, so that the criminals have the opportunity. On the other hand, banks lack emergency measures to the crime. Although banks have emergency stop system, the examination and approval procedures are cumbersome. Even if the money has not been removed, banks will not freeze the account on the grounds that the procedure is not complete, resulting in a greater loss. [4]

Fourth, some people's precaution awareness being weak. The crime has close relationship with the lacking of precaution awareness. Some victims don't know much of fraud methods and lack the necessary vigilance, carelessly and thoughtlessly, so they can be deceived easily. Some victims have certain ability to identify the crime and are alert enough in advance, but they are unwilling to give up "pertain" profits, so they contact with criminals and finally fall into the trap set by the criminals.

THE DETACHMENT COUNTERMEASURES OF TELECOM FRAUD CRIME

Investigation countermeasures[5]

First, accepting cases timely, combing investigation clues fully. When the crime happens, investigators should not only accept the case in time, but also inquire the reporter carefully to get first-hand information as much as possible, to extract and fix information related. According to the ways of crime, we should retrieve, collide and find similar information from the database which the investigation organs have grasped, so as to determine the direction of investigation.

Second, strengthening the department cooperation, obtaining the evidence of crime. Because there is no positive contact between criminals and victims, crimes are committed by the mobile phone, group messaging device, fixed telephone, network, communications and financial instruments such as bank card. And the messages, phone records, computer storing information and related data from financial institutions are important evidence of crime. Therefore, the investigation organs must strengthen the cooperation with the communications, finances, network supervisor departments and so on to gain evidence in time.

Third, analyzing the case, inferring the criminal's identity. When criminals commit crimes to satisfy their desires by modern communications and financial instruments, there will also be a large amount of the corresponding marks and information left in the crime at the same time. Investigators must be good at mining and using these tracks and information. They can also retrieve and obtain the information attached in these departments through investigating from mobile service providers and Internet service providers to infer the criminal's identity synthetically, delimit the scope of investigation scientifically, and control the investigation direction accurately.

Fourth, tracking money flows, determining the suspects. Prior to the crime, criminals generally register bank account in financial institutions by using false identity information or hiring others in advance. When the victim is deceived, the money will be remitted to the designated account, and then transferred or withdrawn to another place immediately. So investigators can obtain, query the related records of financial institutions, and find, track the real suspects through the identity information left in the financial institutions. In addition, criminals' appearance information may be recorded by the monitoring system of financial institutions, when they transfer or withdraw cash after crime. Therefore, the investigation organs may find and determine the suspects by the surveillance video from the financial system.

Fifth, using interrogation tactics neatly, digging more crimes and partners. For cases in which evidence is sufficient and facts are relatively simple, investigators can use more straight and cut to the chase interrogation tactics, hunting down the criminal, until making them confess all the crimes and partners. For cases in which evidence is sufficient but facts are relatively complex, investigators can use evidence and let the criminal write a personal statement at the same time to avoid excessive exposure of information. For cases without sufficient evidence, investigators need to take corresponding interrogation tactics flexibly according to different psychology, but it's unfavorable to use evidence or show the crucial evidence at the time.

Prevention and control countermeasures

First, perfecting the relevant laws and regulations, strengthening the legal regulation. Not only attacking crime but also preventing and controlling crime all need perfect laws and regulations. According to the judicial practice, the following questions need to publish relevant laws and regulations urgently: First, the connotation and denotation of crime need to be clear, at the same time, the cognizance of the accomplice

and the evidence censorship also need the guidance of corresponding laws and regulations. Second, the jurisdiction of telecom fraud crime needs to be clear in different levels and different areas of the public security organs, thus reducing the repetition work, and avoiding the loopholes in jurisdiction. Third, the regulatory responsibility or even the criminal responsibility of the telecom operators and financial institutions such as bank also needs to be clear, so the survival soil of crime can be cut off from the source.

Second, strengthening the propaganda, raising the public awareness. Related departments should make good use of radio, television, newspapers, the Internet and other media to educate the masses, making people have a general understanding of the crime and its methods. Meanwhile, the judicial organs should also take advantage of a large number of vivid, typical cases to make further education for the masses, making them discern, deal with all kinds of crimes and giving no chance to criminals by ensuring "don't believe, transfer, remittance". [6]

Third, reinforcing the construction of information of public security organs. improving the ability to prevent crimes. With the improvement of intelligent level of the crime, reinforcing the construction of the public security's information to enhance the ability of preventing and cracking down on crimes is the inevitable choice. First, we should attach more importance to researching, developing and utilizing the products related to computer network, as well as the telephone positioning and tracking technology. Second, we should strengthen the construction of crime personnel database, realizing nationwide network, region linkage. Third, the public security organs should make good use of the existing technique and combine it with traditional detection method to collide, identify and sift lots of suspicious clues, striving to kill the crime in the bud.

Fourth, enhancing the collaboration with telecoms, banking and other departments, improving prevention effect. To strengthen the cooperation with telecommunication departments, we can easily identify and sift the sensitive number and sensitive messages, we can also monitor and track the fraud message and the fraud call, improving the efficiency of investigation and arrest. To strengthen the cooperation with banks and other financial institutions, we can establish and improve the mechanism of the quick query, freezing and bank transferring, and strengthen the monitoring and management of the bank account. Therefore, we cannot only prevent and reduce the economic losses of the victim, but also improve the ability to recover the money.

Fifth, strengthening the international and interregional judicial cooperation, dispelling the fluke mind of criminals. To deal with cross-border telecom fraud crime effectively and dispel the fluke mind of criminals, strengthening the international and interregional criminal judicial assistance is particularly important. In recent years, lots of multinational and cross-border cases have been detected by the police from the mainland and other areas. These are the shining example of international and interregional judicial assistance and cooperation, and worthy of summary and promotion.

REFERENCES

1. Liu Ji-min. Suggestions on Control Measures and Analysis of Telecom Fraud Crime in Information Society [J]. Policing Studies, 2011. 6. 19-20(in Chinese).
2. Ge Lei. Research on Legislation of Telecom Fraud Crime [J]. Hebei Law Science, 2012. 2. 108-109(in Chinese).
3. Yang Fan, Chen Haili. Characteristics, Difficulties and Control Countermeasures of Telecom Fraud Crime [J]. Journals of Colleges in Guangxi, 2012. 6. 21-22(in Chinese).
4. Hu Xiangyang, Research on Control Countermeasures of Telecom Fraud Crime [J]. Journals of the Chinese People's Public Security University (social science edition), 2010. 5. 93-94(in Chinese).
5. Wu Zhaomei. The Characteristics and Interrogation of Telecom Fraud Crime [J]. Journasl of Liaoning Police Collage, 2010 3 33-34(in Chinese).
6. Zhang Xuan. Investigation Difficulties and Countermeasures of Telecom Fraud Crime at Present [J]. Nomocracy Forum, 2010 4 149(in Chinese).

UDC: 343.57:004

INTERNET-BASED DRUG-RELATED CRIMES INVESTIGATION PROBLEMS AND SOLUTIONS

Zhang Ruzheng [1]
Duan Zhuoting
National Police University Of China, Shenyang

Abstract: Currently, cracking down Internet-based drug-related crimes is a new situation and requirement of anti-drug work. In practice, Internet-based drug-related crimes constitute a huge threat to public security that is so important and difficult for drug investigation because of the following features: extensive distribution, obvious concealment, and hard collection of evidence. We should improve the laws, rules, regulations, technology to curb the development and spread of Internet-based drug-related crimes.

Keywords: Internet-based drug-related crimes; drug crimes; crack down crimes.

INTRODUCTION

At present, with the development of the network technology and the popularity of Internet application, Internet-based drug-related crimes present new features and situations with an increasing number. For these reasons, the public security organs carry out a series of actions against Internet-based drug-related crimes. In the second half of 2013, the Ministry of Public Security launched a special campaign against online drug-related activities that arrested 2,120 criminal suspects, destroyed 11 secret drug-producing sites and confiscated 268 kilograms of illicit drugs, 22 guns, 719 bullets and 7.93 tons making drugs tools in just 8 days.[2] Internet-based drug-related crimes constitute a huge threat to public security that is so important and difficult for drug investigation because of the following features: extensive distribution, obvious concealment, and hard collection of evidence.

INTERNET-BASED DRUG-RELATED CRIMES – CURRENT SITUATIONS AND DAMAGE

Internet-based drug-related crimes include all drug-related criminal activities with Internet technology. In comparison to traditional drug-related crimes, Internet-based drug-related crimes have the following types:

1. Transaction Internet-based drug-related crime

With the development of e-commerce and logistics industry, illicit trafficking in drugs and making drugs tools actions have spread on the Internet. In June 2011, Guangxi police cracked an Internet-based drug-related trafficking case. In this case, these criminals were to be found using the Internet as a trading platform to conduct sales in the name of "perfume".[3] They first created a site and contacted buyers through chatting in online chatting rooms which are inaccessible for outsiders finally delivering the drugs with online payment system and the logistics company.

At present, there are two main modes for trafficking and transporting drugs through the Internet. The first one is "sales online + the third-party payment platform + delivery & logistics services". The second one is "release news through Weibo/Weixin (a kind of social networking web platform which is similar to Twitter in the US) + delivery & logistics services + cash on delivery". The criminals release some news on Weibo/Weixin in their own words that could be understood by themselves. These virtual exchanges allow more and more drug addicts and dealers to purchase illegal drugs comfortably.

2. Instigation and gathering Internet-based drug-related crime

In October 2011, China's police arrested 12,125 suspects during the battle against Internet-based drug-related crime that was led by the Ministry of Public Security. Police destroyed 22 secret drug-pro-

1 jotinduan@163.com
2 http://news.youth.cn/gn/201306/t20130619_3390193.htm
3 http://v.ku6.com/show/fgcaKZSmPaByJLVC.html

ducing sites and confiscated 308 kilograms of illicit drug. These criminals were getting and selling drugs through the online chatting room. Newcomers were just allowed to enter the chatting room after being introduced by acquaintances. They gathered drug addicts to perform drug-addiction through the online video. Criminal suspects use the Internet for drug addiction and instigation.[4]

INVESTIGATION DIFFICULTIES AGAINST INTERNET-BASED DRUG-RELATED CRIMES

Fighting trouble

Now, most of the network platforms do not require the users' real-name registration. A person can register more than one user name with different accounts logging in at the same time. These circumstances make drug-related crimes completely anonymous. The virtual drug crimes give police tremendous obstacles for fighting against Internet-based drug-related crimes.

Collecting evidence trouble

Internet-based drug-related criminals use online payment to complete transactions. It is easy to destroy the online evidence and transfer online property. In some cases, criminals hire special technical person to destroy and update criminal data with encryption and maintenance of the network, increasing the difficulty of the police for investigation and collection evidence.

Litigating trouble

Internet-based drug-related crimes trouble filing cases that mainly exist in cyberspace with regional network. Police cannot investigate without evidence, however, most of the drug addicts do not report. There is a lower level of legislation and weakened enforcement mechanism for Internet-based drug-related crimes. Without sufficient evident, perfect legal framework, charges over the drug crimes will hardly lead to conviction.

COUNTERMEASURES FOR CRACKING DOWN INTERNET-BASED DRUG-RELATED CRIMES

1. Legal countermeasures

Consummating the law

Buying and selling drugs on the Internet could be a crime resulting in criminal charges of illegal drug trafficking or gathering a crowd of drug addiction. But, sometimes we had some realistic obstacles such as insufficiencies of legal support and incompleteness of supervision, which is caused by imperfect laws and regulations. Drawing lessons from other countries' experience, we should improve the laws, rules and regulations. We make great effort to accelerate the laws and improve their quality.

Adding new type of criminal charge

Internet-based drug-related crimes become more and more desperate; they increased the damage degree all over the world. While discussion of Internet-based drug-related crime often focuses on blocking drug advertisement, the greatest danger may lurk in chat rooms on the Internet. The people who tempt, abet and deceive someone into drug addiction through online chatting room shall be investigated for criminal responsibility according to the law (or the new type of criminal charge).

Strengthen International Cooperation

Recognizing combating Internet-based drug-related crime is a global problem. It is imperative to strengthen international cooperation dialogue and in this regard, address both the symptoms and root causes of Internet-based drug-related crimes. By now, it is hard to form boundary of the standards for measuring punishment and convicting criminals. For example, Sibutramine was considered a kind of drug in Russia; however, it is marked and prescribed as added ingredients for the treatment of obesity. We should stipulate the extent of prescribed punishment minutely and define the standard of sentence by the judicial interpretation clearly. China firmly denounces and opposes all kinds of crimes, and makes efforts to make stronger international links, signing extradition treaties with other countries.

2. Technology countermeasures

Monitoring network

4 http://news.xinhuanet.com/2011-10/30/c_111133054.htm

Supervisory person could filter out related topics and words to delete these unlawful contents. Police could shut down the website through locating the suspected specified server.

Building firewall

A network firewall stands between the web server and the network. It is playing an important role in the area of fighting against Internet-based drug-related crime. Government regulatory authorities could block some drug information or news with the firewall ensuring the Internet security.

Tapping communication line

Tapping in this paper is the monitoring of telephone or Internet lines by the third party (Government regulatory authorities) with covert methods. Police affected by the law would have to provide access to tap or intercept communication lines through the network. Tapping communication line could be used in such criminal cases. Unfortunately, communication lines are not yet absolutely safe. It is hard to use this method in Internet-based drug-related crime, but it can become an effective method in investigation and increased working efficiency.

3. Management countermeasures

Stepping up web monitoring

Strengthen the web monitoring of network operators and Internet service providers who are the first manufacturers of network information. Do not underestimate the force of the broad Internet users. Government regulatory authorities search social media, such as Weibo/Weixin (Twitter, Facebook in other countries) as part of their law enforcement efforts, responding to the drug criminals using the Internet to release news, process online transaction and so on. Establish drug offence-reporting system with publishing email address, messages, and telephone numbers for public supervision. All governments would call for new treaties to govern the regulation of the Internet to curb the development and spread of Internet-based drug-related crimes.

Stepping up logistics monitoring

One of the main reasons for Internet-based drug-related crimes develop rapidly is in the loopholes of management and absence of management of logistics. Logistics companies do not require verifying ID. Keep monitoring the whole logistics system must be enforced. The real-name registration system would help investigations and crackdown the Internet-based drug-related crimes.

CONCLUSION

Solving the combating Internet-based drug-related crime we should carry on comprehensive treatment through all kinds of ways in the whole space of network. To crack down Internet-based drug-related crimes, consummating the law is the premise and the foundation; the improvement of the technology countermeasures is the important method, the perfect legal framework and management policies are the effective guarantee. At the same time, the real-name registration system would help curb the surging number of Internet-based drug-related crimes. The international community including all governments and police from various countries are determined to insist on waging resolute struggle against internet-based drug-related crime.

REFERENCES

1. Drug Law of the People's Republic of China.

2. Peng, Song. New Trends and Rules of Drug Crimes In the Internet Age, Journal of Henan Institute of engineering, 2014, (1).

3. Report on Drug Control in China.

4. Wang, Ruiyuan. Analysize of INTERNET-BASED DRUG-RELATED Behavior [J]. Journal of Shanghai University of Political Science & Law, Vol. 29, No.5 Sep., 2014.

Topic VIII

INNOVATIVE TECHNIQUES AND EQUIPMENT IN FORENSIC ENGINEERING

UDC: 343.983:623.445.1

BALLISTIC PROTECTIVE EQUIPMENT – FORENSIC ENGINEERING ASPECTS

Radovan V. Radovanovic[1]
Marko Z. Ristic[2]
Jelena V. Milic[3]
The Academy of Criminalistics and Police Studies, Belgrade

Abstract: Tendency of modern society to achieve maximum security of the individual is supported by the adequate levels of equipment of the members of the security services in modern instrumentality for the purposes of the personal protection. Instrumentalities for the purpose of the personal ballistic protection are inevitably part of the equipment used by the police and military service. Respectively, all the individuals whose life could be vitally endangered by the projectiles and explosive projectile fragmentation must have ability to have next to the protective purpose necessary mobility and efficiency to its users, as well. Namely, modern protective equipment has to provide to all of its users high protective performance, comfort, flexibility and undisturbed complex movement while providing assistance and aid to the jeopardized ones or while performing different operative tasks. Technological advancement and economic power of the society are the ones that dictate the level of the protective equipment of the security service units. In order to achieve high levels of national security and security of its structured security service personnel, it is necessary to analyze forensic engineering aspects of the protective ballistic equipment and its protective elements.

Keywords: protective equipment, protective elements, security, ballistics, forensic engineering.

INTRODUCTION

Constant changes in the world global security are caused by changes in approach to the concept of combat operations, which are becoming more frequent and more extensive in urban areas. It became especially important in populated areas which are the key areas of contemporary armed conflicts. Converting complete cities and populated areas into the "epicenter" of combat operations has raised the issue of protection of the civilian population.

More frequent acts of terrorism and attacks on civilian objects has resulted in the engagement of specially trained police units, which are composed of a small team of people entering into close combat with the terrorists. These units, armed with special weapons and equipment, on the field are exposed to different types of ammunition and splashed mines and explosives devices.

Members of special police units during the execution of the tasks suffer great physical and psychological stress, partly responsible for that is the heavy protective equipment that is necessary to be worn. In order to increase the chances of survival in the field, contemporary policeman is forced to wear a bulletproof protective equipment and clothing. Due to that fact, great attention has been given in to the development of ballistic protective equipment, whose use is not been limited to the special teams units, but it is a fundamental part of the modern police officers and soldiers equipment. This type of protection has shown to be needed in the structures outside the state services as well; from the person whose life has been threatened by the various criminal groups to the journalists, also various private security agencies, further on health workers and Red Cross aid workers operating in the territories affected by the war conflict.

1 *Full Professor, Ph.D., E-mail: radovan.radovanovic@kpa.edu.rs;*
2 *Ed.S. Candidate, MSc., E-mail: markoffh@yahoo.com;*
3 *Ed.S. Candidate, MSc., E-mail: jelenamilimbf@hotmail.com.*

CHARACTERISTICS OF THE PROTECTIVE BALLISTIC EQUIPMENT

Modern protective equipment must provide to its customers a high degree of self–protection, comfort, flexibility and enabling of the movement freely, while providing assistance to the wounded and during the execution of the tactical security tasks. Particular care must be taken in making protective equipment intended for the fairer sex in order to allow maximum possible comfort.

Characteristics of ballistic protective equipment generally depend on: (i) the demands of the users, whether they be individuals or institutions; (ii) the level of protection of the ballistic and surface equipment; (iii) the weight of equipment and additional elements (collars, protection for groin and shoulders, etc.).

Good anti–ballistic protection represents a compromise between the level of protection, comfort and weight. Insertion of ballistic plates increased the level of protection, but it also increased the mass, which again reflects on the comfort and mobility. One of the major problems in ballistic protective equipment is the heat dissipation of the user's body. Furthermore, increased secretion of sweat, loss of strength and endurance members of the special security forces depends on climatic and meteorological conditions. The situation becomes even worse when members of special police units are in the vehicle where the temperature is considerably higher than outside, while space for accommodation is much narrower. These kinds of problems are usually solved by installing air conditioners in vehicles and/or by placing the cooling system under the protective vests, which operate on the principle of circulating fluid or ventilation air. In recent types of vests this problem is solved by inserting a special material named *"Outlast"*[4] (Figure 1), which regulates heat.

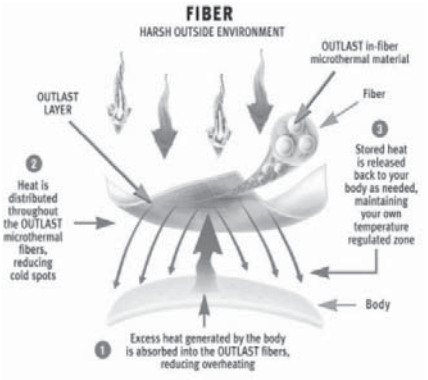


Figure 1 *Outlast® technology*

Protective ballistic equipment of contemporary members of the special security forces (Figure 2) are mainly composed of:

1) protective vest;
2) ballistic plates;
3) protective belts;
4) ballistic pants;
5) helmet with visor;
6) protective goggles;
7) protective guards for neck, elbows and knees;
8) tactical shields, as well as the covers for explosive devices and other protective devices.

The most commonly used pieces of equipment are protective vests with/without inserted ballistic plates and protective helmet with a visor. Also, it is possible to set the model of the missiles effects at the target[5] and to test the degree of sensitivity and destructiveness of protective equipment on the basis of their prominent characteristics for anti–ballistic protection which will be the topic of further research.

4 Outlast Adaptive Comfort material is developed by NASA to regulate extreme temperature changes which astronauts are exposed to. (available at: http://www.thetechnicalcenter.com/features/Assets/KA_Outlastfall02.pdf)
5 Radovanović, R., Ristić, M., Milić, J. (2014). Forenzički značaj određivanja parametara dejstva pištoljskih projektila. U Lj. Mašković (ur.), *Kriminalističko–forenzička obrada mesta krivičnih događaja: tematski zbornik radova II* (str. 149–162). Beograd: Kriminalističko–policijska akademija.

Figure 2 *Parts of ballistic protective equipment, respectively*[6] *(numerated in the text)*

CLASSIFICATION OF THE PROTECTIVE BALLISTIC EQUIPMENT

In general, there is a wide range of potential threats depending on the types of weapons combined with different types of ammunition. Consequently, protective ballistic vests can be divided into six different categories and seventh level as a special type of protective vests[7].

- **Level I** (*.22 LR*; *.380 ACP*): Protects from gunshot leaded beads 5.56 mm caliber with a rounded tip, with nominal masses of 2.6 g and impact velocity of less than 320 m/s and with a 9 mm full metal jacketed and rounded tip, the nominal mass of 6.2 g and the impact velocity of less than 312 m/s.
- **Level II–A** (*9 mm*, *.40 S&W*): Protects against the 9 mm grain which is full metal jacketed with a rounded top and a nominal mass of 8.0 g, impact velocity of less than 332 m/s and 10 mm grain caliber with total metal–coat, with nominal masses of 11.7 g and impact velocity of less than 312 m/s. Also, it includes protection from all types of ammunition from class I.
- **Level II** (*9 mm*; *.357 Magnum*): Protects against the 9 mm grain which is full metal jacketed with a rounded top and a nominal mass of 8.0 g, impact velocity of less than 358 m/s and .357 caliber Magnum with a soft jacket, with nominal masses of 10.2 g, impact velocity of less than 427 m/s. Also, it includes protection from all types of ammunition from Class I and II–A.
- **Level III–A** (*High Velocity 9 mm*; *.44 Magnum*): Protects against the grain 9 mm full metal jacketed with a rounded top and a nominal mass of 8.0 g, impact velocity of less than 427 m/s and the .44 Magnum grain with a blunt tip of nominal masses of 15.6 g, impact velocity of less than 427 m/s. Includes protection from all types of ammunition from a class I, II–A and II. Ballistic vests this level of protection[8] is the most often choice of the police and security services.
- **Level III** (*Rifles*): Protects from 7.62 mm bullets, with full metal jacketed and with nominal masses of 9.6 g, as well as impact velocity of less than 838 m/s. This type includes protection from all types of ammunition from a class I, II–A, II, and III–A.
- **Level IV** (*Armor Piercing Rifle*): Protects from gun armored 7.62 mm grain of nominal mass of 10.8 g, impact velocity of less than 869 m/s. Includes protection from all types of ammunition from classes I, II–A, II, III–A and III. Level IV represents the highest level of protection; to halt bulletproof grain it is necessary to insert a ceramic plate. It can provide protection against single shot because of the nature of ceramics materials.
- **A special type of body armor:** It is manufactured mainly upon request of customers, and it differs from the above mentioned types by the fact that customer himself defines the level of protection from the exact type of ammunition and a minimal impact speed, which proves that this standard is in front of all the other types in all the aspects.

6 Images were taken from the following web sites: *http://www.bodyarmour.co.za/poltactical.htm*, *http://www.blackhawk.com/Products/Gloves-Protective-Gear/Protective-Gear/Armor/Plates/Ballistic-Ceramic-Plate-Level-IV-Stand-Alone.aspx*, *http://crossfire.com.au/shop/shapeshifter-duty-belt/*, http://www.derbycycles.com/cgi-bin/eShop/index.cgi?pid=1310, *http://senkenprotection.en.alibaba.com/collection_product/police_helmet/1.html* , *http://www.copsplus.com/safetyglasses-goggles.php*, *http://spanish.alibaba.com/product-gs/single-police-equipment-tactical-elbow-and-knee-supporte-693617241.html*, *http://www.civil-defence.co.uk/helmet1.html*, *http://www.act-sales.com/products/tactical-equipment/ballistic-shields/intruder.php*, *http://forums.gamersfirst.com/topic/347545-riot-shields/*

7 *Ballistic Resistance of Body Armor–NIJ Standard–0101.06.* (2008). Washington: National Institute of Justice.

8 http://www.aleksarmor.com/pitanja.html

REQUIREMENTS THAT MUST BE FULLFIELD BY THE PROTECTIVE BALLISTIC EQUIPMENT

Protection levels I, II–A, II, and III–A must stop the penetration of six bullets per panel, two on the entire sample (front and back panel, Figure 3a) with a specific velocity and location for the two types of ammunition. Moreover on every six shoot bullets, two must hit an angle of 30° (Figure 3b). Deformation of the inside material must not exceed a value of 44 mm. The deformation is measured on each panel, specifically, and in all locations, depending on the collision speed. The protective vest must meet these requirements even in humid condition[9].

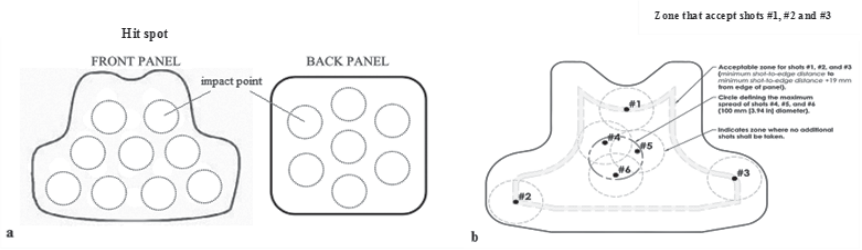


Figure 3 *a) Protective ballistic vests panels, b) Hit zones*

Protection level III must meet all the requirements set out in the previous paragraph, except that it uses just one type of ammunition, furthermore all six cartridges must be tested while hitting the surface at right angles.

Protection level IV must stop the penetration of one type of ammunition (bulletproof grain) and prevent deformation greater than 44 mm of the body armor material on the inner side in one hit. Two samples are being tested.

Protective levels III and IV are obtained by inserting protective ballistic plates. These protective plates are made of titanium, steel, or ceramics. Ceramic plates are manufactured by sintering at high temperature and pressure, on the basis of oxide ceramics. Commonly they are made on the basis of aluminum oxide (Al_2O_3), or a non–oxide ceramic, the carbide or nitride–based (to be used silicon carbide). The plates are usually made in small sizes, and later glued to the basis of composite materials made of ballistic cloth. This solution avoids the main negative feature of ceramic, which is the absorption of impact energy throughout the volume, resulting in the destruction of large areas of homogeneous material. Ceramics are used in the form of large thick plates as the basic element of protection of modern combat vehicles, helicopters and even tanks, consisting of a sandwich–armor. Basic physical properties that make them suitable for ceramics installation in armor elements of protection are firmness, which is achieved due to the special structure of the material, with homogeneous and compact crystal structures, as well as small specific weight. High hardness allows the destruction of armor missiles.

Level of achieved protection of the protective plates is shown in Table 1, according to the applicable standards referred to in (NIJ Standard 0101.06)[10]

Table 1 *The levels of protection for the protective plates*

Level of protection	Type of bullet	Velocity (m/s)
III	*7.62 mm NATO M–80 steel jacket*	838
	7.62 mm NATO M–80 (FMJ)	838
	30,06	824
	.30 (FMJ)	595
	.12 rifle grains	473
	.223 (5.56) FMC	938
	7.62 x 39 mm	732
IV	*30-60 AP M–2*	868
	7.62 mm NATO AP (.308)	838
	.223 (5.56 mm)	942
	7.62 x 54R B32	778

9 *Stab Resistance of Personal Body Armor–NIJ Standard–0115.00*. (2000). Washington: National Institute of Justice.
10 *Ballistic Resistance of Body Armor–NIJ Standard–0101.06*. (2008). Washington: National Institute of Justice.

Safety helmets are designed to protect the head from different types of projectiles fired from different small arms armaments, fragmentation of the hand–bombs, grenades, mines and blows with a blunt object. Their mass ranges from 1100 to 2500 g. Modern safety helmets are made of the combinations of multi–layer synthetic fabrics, such as aramids and high molecular weight polyethylene, glass fibers, and lightweight. Mostly, safety helmets are made from Kevlar composite, by the method of forming the impregnated layers. They enable protect from missiles fired from small arms whose initial rate do not exceed 685 m/s. Protective helmets cover the surface of the head and neck from 1100 to 1300 cm^2 and exhibits resistance to temperatures up to 190°C . Furthermore, they are usually produced in several colors (olive, black, UN blue, etc.). Safety helmets are made in various sizes on which depends their weight. Modern helmets are coated with ABS–film emulsion, which provides protection from observations with infrared and thermal imaging equipment. Their level of protection is usually covered in type III and IIIA[11] (according to NIJ).

There are two types of protective ballistic vests: protective vest with hard (*Hard–shell body armor*, Figure 4a) and soft shell (*Soft–shell body armor*, Figure 4b).

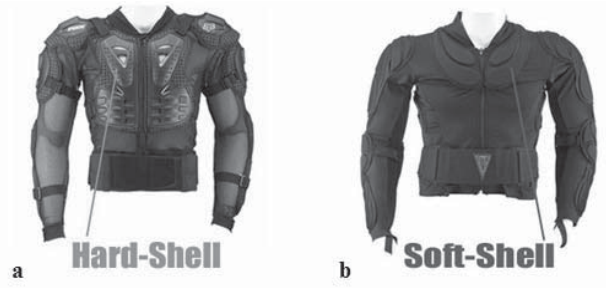


Figure 4 *The protective ballistic vest: a) with a hard shell and b) soft–shelled.*

Soft–shell body armor is designed to protect its users from bullets fired from the pistols and revolvers, and provides protection up to level III–A. Also, they are designed to be inconspicuous in the form of jackets, vests or other parts of the wardrobe. Whereas, hard–shell body armor is usually worn in tactical situations if there is a need for the highest protection level, III–A and IV. They are designed by inserting additional ballistic plates of steel, titanium or ceramic vests in soft–shelled.

The protective vest with soft shell is designed to protect the user from the bullets fired from the pistols and revolvers, and provides the protection until level III–A. Also, they are designed to be inconspicuous in the form of jackets, vests or other parts of the wardrobe. On the other hand, protective vests with a hard shell are usually worn in tactical situations where there is need for the highest protection level III–A and IV.[12] They are made by inserting in the Soft-shell body armor additional ballistic plates of steel, titanium or ceramic.

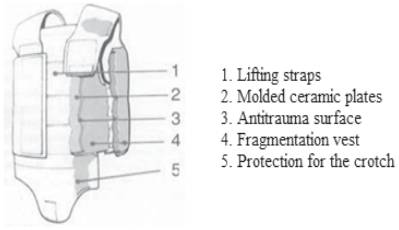


Figure 5 *Schematic view of the protective ballistic vest*

DESIGN AND MANUFACTURING TECHNOLOGY OF PROTECTIVE BALLISTIC EQUIPMENT

In the process of designing the ballistic protective equipment it is necessary to determine the level of danger, select the material or combination of materials that will withstand hazards and determine the number of layers of materials in order to prevent outbreaks and "blunt" injuries of the organs. The final weight of protective equipment is one of the most important factors that must be taken into consideration when

11 Azrin Hani, A. R. *et al.* (2012). Body Armor Technology: A Review of Materials, Construction Techniques and Enhancement of Ballistic Energy Absorption. *Advanced Materials Research Vols. 488–489*, 806–812.
12 Azrin Hani, A. R. *et al.* (2012). *Advanced Materials Research*, *488–489*, 806.

selecting material for making equipment. The aim is to find a compromise between the choice of materials, in order to achieve the required level of protection and on that way provide maximum comfort and free movement of its user.

Numerous factors determines the degree of danger posed on the protective equipment, such as caliber, grain geometry and the materials from which the grain was made, grain weight and initial velocity of the projectile. Consequently, the protective equipment that provides protection against one missile speed does not provide protection against missiles of the caliber that has greater speed and different structural characteristics. However, there are other types of threats that users are exposed to, which are significantly different from previously mentioned ones, such as exposure to the stabbing with knifes or other sharp object. According to the standards of the American National Institute of Justice 0115.00[13], protective equipment is divided into to two categories based on the type of threat that equipment must provide protection from. The first category "edged blade"[14] is designed to provide protection from high–quality sharp edges such as kitchen knives or other cold sports weapons. The second category provides protection against improvised sharp objects that are made of inferior materials (NIJ Standard 01.01.06).

Protective equipment is constructed by connecting multiple layers of materials in the form of a protective plate. The role of these layers is that when the missile strikes, it gets "caught" between the layers of fibers, which are able to stop, deform and absorb its energy. The protective plate is inserted into conventional garments, which are made of synthetic fibers or cotton. Furthermore, protective plates could be sewn together with clothing or they could be removable. There are a wide range of fabrics and materials that manufacturers install in order to improve the level of protection and reduce the weight of it. The way of merging the layers depends on the manufacturers. Namely, some of the protective plates are made by stitching the layers, while the other layers are bonded on to one another which increase the performance of protective equipment.

MATERIALS USED IN PRODUCTION OF PROTECTIVE BALLISTIC EQUIPMENT

There are many different manufacturers involved in the development and production of the materials which are used in production of the protective ballistic equipment. Ballistic protection is mainly based on multilayer synthetic fabrics that are made from polyethylene[15], aramid[16] or other types of artificial fibers. These types of fibers are several times stronger than steel of the same weight[17].

One of the first materials, developed in 1965 is Kevlar (*Kevlar*®). Namely it was developed by the American Chemical Company *DuPont*[18]. Kevlar is a lyotropic liquid crystalline polymer it has golden yellow color and belongs to the class of para–aramid synthetic fibers. Furthermore it possess characteristics of high strength, low weight, high chemical resistance, high resistance to cutting, resistance to the temperature change[19] and water impact. *Kevlar® 29* represents the first generation of synthetic fibers that were introduced in the production of ballistic protective equipment**.** *DuPont* has developed a second generation of Kevlar fiber called *Kevlar® 129* in 1988th. This generation had increased ballistic resistance including resistance towards 9 mm grain with a full metal jacket (FMJ). Moreover, in 1995, *Kevlar®* fibers *Correctional™* was developed, which provided protection against stabbing. The latest generation of *Kevlar®* fiber is *Prothero*, which is characterized by low weight, flexibility and significantly greater ballistic protection. Molecular

13 *Stab Resistance of Personal Body Armor–NIJ Standard–0115.00*. (2000). Washington: National Institute of Justice.

14 NIJ Ballistic, *Edged Blade, and Spike Levels*, http://www.safeguardclothing.com/articles/nij-levels/

15 Polyethylene is non–toxic thermoplastics, odorless and tasteless, resistant to oil, grease and many chemicals. It is flexible and lightweight thin–layer of translucent and transparent. They have great toughness and flexibility even at relatively low temperatures. Low density polyethylene (LDPE) and high density polyethylene (HDPE) can be easily processed and can be painted. (Nedic, Vesić, Vasiljevic, 2008, 130)

16 Polyethylene and aramid fibers are among the most powerful and highly modular fibers with special applications and they present the basic material for the production of ballistic protective equipment. High performance polyethylene fiber can be obtained in two ways: by extracting fibers from the surface of mild solution called gel drawing (smooth surface). Polyethylene (PE) fiber is steadily against most organic solvents at room temperature and also has good biological compatibility and does not cause adverse reactions in contact with living tissue. The only drawback is that it is not applicable on high temperatures (it melts already at about 1500°C). Thanks to its excellent impact resistance and ability to absorb energy, polyethylene fibers are suitable for making lightweight bulletproof ballistic vests and other clothing, protective helmets, as well as various structural elements. (Lukkassen, Meidell, 2007, 72–74; Maksimović, Divjaković, 1996, 1–9)

17 Compared to the steel it shows better flexibility and good resistance to fatigue and it can be easily processed by twisting and weaving in textile plants.

18 The aim of researchers at *DuPont* Company is to create a combat suit that will be bulletproof, light, comfortable and equipped with communication systems, autonomous controller with health status and devices that increase mental and physical abilities of its user.

19 At lower temperatures it expresses stronger properties, while at higher temperatures at around 250°C eventually loses its firmness in one hour by 10% . For example, kevlar fiber has a glass transition temperature of about 300 °C, while it is decomposed at a temperature of 550 °C. (Utracki, 2010, 6–11)

structure of its fiber is responsible for good characteristics. *Prothero* fiber has increased tensile strength (3,620 MPa) and energy absorption which is accomplished by developing new ways to twine fibers**.**

This patented technology enabled production of armors which have abilities to protect against gunfire, commercially–produced knives and other stab means.

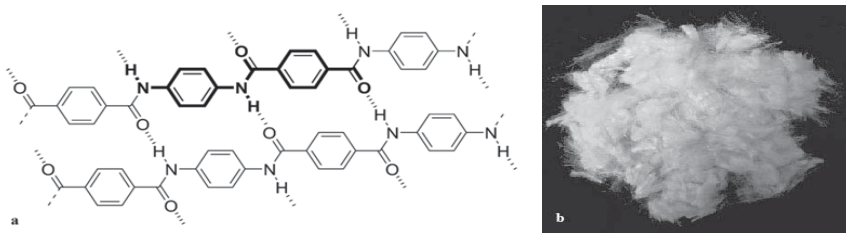


Figure 6 *Chemical structure (a) and tamed fibers of Kevlar® Protera (b)*

Spectra® fibers are produced by the *Honeywell* manufacturer. These fibers are polyethylene fibers that possess very high strength (Figure 7).

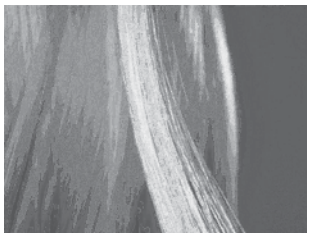


Figure 7 *Spectra® fiber*

Spectra® fibers express high resistance to tearing, they have extremely high chemical resistance and very low resistance to cutting.

Honeywell Company patented *Spectra Shield*® fibers, based on these fibers. *Spectra Shield*® fibers consists of two layers of *Spectra*® fibers, which cross each other at an angle of 90° and which are connected with flexible resins (Figure 8). The result showed an incredibly strong, light and flexible fabric, which has excellent ballistic protective qualities.

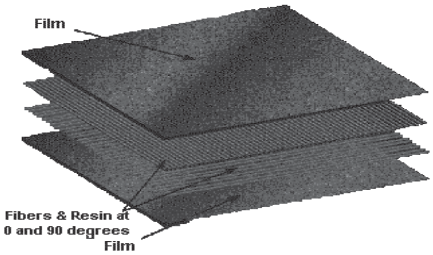


Figure 8 *Layers of Spectra Shield® fiber connected with a flexible resin*

Taming and merging of aramid fibers in combination with *Spectra*® fibers aroused in even better modifications, such as *Gold Flex*® fibers (Figure 9). Furthermore, these fibers are used for production of helmets, protective ballistic plates and vehicle armor.

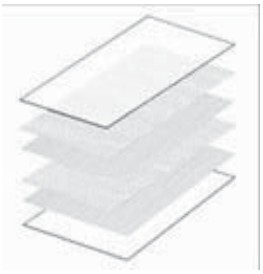


Figure 9 *Gold Flex® layers of fibers*

Dutch firm *AKZO* developed a para–aramid synthetic fiber named *Twaron*®. This fiber consists of 1,000 finely tamed threads that acts like a sponge by absorbing bullet energy and dissipating it in adjacent fibers, providing on that manner increased comfort and flexibility. Protective equipment made of *Twaron*® fibers is characterized by a significantly lower weight and high resistance to tearing and cutting.

Currently, in the world the strongest commercially available fiber is *Dyneema*®[20] (Figure 10). In addition to, it is polyethylene fiber which offers maximum strength combined with low weight and not only that it showed to be up to fifteen times stronger than quality steel, but also 30–40% lighter and stronger than aramid fibers. Due to the high specific gravity it floats on water and it is very resistant to moisture, chemicals and ultraviolet light.

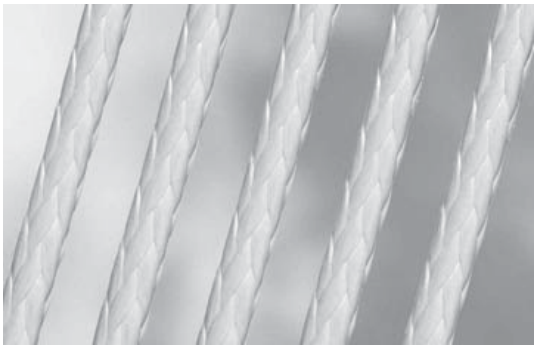
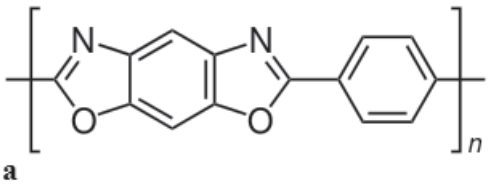


Figure 10 *Microscopic appearance of Dyneema® fibers*

Protective equipment made of *Dyneema*® fibers provides protection against firearms and bladed weapons and has twice longer warranty in contrast to the aramid fibers. This type of fiber is characterized by very high strength (for example, rope made of this fiber in 1 mm diameter can withstand the load of up to 240 kg) and great ability to absorb energy. *Dyneema*® *Soft Ballistic* solution has been developed for the purpose of manufacturing protective ballistic vests and has the ability to provide protection from pistol ammunition, fragments and knives. However, *Dyneema*® *Hard Ballistic* solution is manufactured in the form of ballistic plates in order to provide protection from the rifle projectiles and fragments at high speed.

Zylon®[21] is a type of synthetic–based polymer[22] fiber developed by the Japanese company *Toyobo Corporation* (Figure 11).



a

b

Figure 11 *a) The chemical structure of Zylon® fibers (n – number of monomer units in the polymer chain), b) set of Zylon® fibers*

20 Radonjić, V *et al.* (2014). Unapređenje balističkih karakteristika i održavanja zaštitnih balističkih prsluka. *Vojnotehnički glasnik*, *62* (4), 89–103.

21 Trade name; This complete name of an isotropic liquid crystal polymer according to IUPAC is poly-benzo–bis–oxazole [poly(*p*–phenylene–2,6–benzobisoxazole], abbrev. (PBO). (Utracki, 2010)

22 Polymers represent a broad and diverse group of natural and synthetic materials. The polymer is actually in a condensed state of the matter, the structure consists of long–chained macromolecules that arise from the synthesis of small and medium–molecular monomers, in the processes of polymerization (anionic, cationic, radical, equilibrium etc.), polycondensation or polyaddition, under the action of increased temperature, electromagnetic radiation or catalysts. During polymerization, monomers (from a few hundred to a million) are united in the polymer. In the polycondensation, a macromolecule formed from a monomer of different composition while separating the by-products (water, gas, acid, etc.). Polyaddition is a process between the polycondensation and polymerization and it consists in merging of different molecules without separation of byproducts. (Nedić, Vesić, Vasiljević, 2008, 85–86)

It is characterized by high performance, outstanding technical properties and two times higher tensile strength (5.8 GPa) than conventional para–aramid fibers (according to Figure 12 and Table 2).

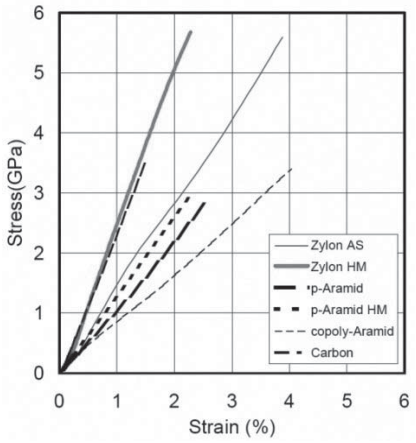


Figure 12 *Mechanical and technological features of fiber: Zylon® AS; Zylon® HM; p-aramid (HM); m-aramid; steel fibers; HS-PE; PBI; Polyester*

Table 2 *Mechanical and technological features of fibers*

	Tenacity		Modulus		Elongation	Density	Moisture Regain	LOI	Heat Resistance*
	cN/dtex	*GPa*	*cN/dtex*	*GPa*	*%*	*g/cm³*	*%*		*⁰C*
Zylon® AS	37	5.6	1150	180	3.5	1.54	2.0	68	650
Zylon® HM	37	5.8	1720	270	2.5	1.56	0.6	68	650
p–Aramid (HM)	19	2.8	850	109	2.4	1.45	4.5	29	550
m–Aramid	4.5	0.65	140	17	22	1.38	4.5	29	400
Steel Fiber	3.5	2.8	290	200	1.4	7.8	0		
HS–PE	35	3.5	1300	110	3.5	0.97	0	16.5	150
PBI	2.7	0.4	45	5.6	30	1.4	15	41	550
Polyester	8	1.1	125	15	25	1.38	0.4	17	260

*Melting or Decomposition Temperature

However, there are various controversies about the warranty period in which protective equipment made of *Zylon®* fiber is rapidly lost the protective properties. There were cases where protective vests that were used couple of months under a warranty failed to stop 9 mm grain, and the manufacturer was forced to withdraw its products from the market.

Protective helmets are developed mainly by using thermoplastics based on ABS (Acrylonitrile Butadiene Styrene) polymers[23] (Figure 13). The most important technical characteristics of ABS is that's resistant to shock and chemicals, also shows very high strength and firmness.

23 ABS belongs to the so–called, *technical plastics*. These are materials whose properties are such that they can be used as structural elements or as a replacement for metals. Their features are high toughness and stiffness in a wide temperature range, as well as dimensional stability. It is stronger than polystyrene, shows better resistance to high temperatures and chemicals. It is usually opaque and may be colored in the mass or on the surface. Processing temperatures is between 200°C and 260°C. Processing ways could be: injection molding, extrusion, blow molding and depressurization. Good processing is gained by grinding, milling and embossing. It also has property of very little absorption of moisture, and even relatively low moisture content makes it difficult to process, causing errors on the product surface and difficult dosage. Therefore, pre-drying in a layer of 3–4 cm thick in an aluminum casserole on a hot air at a temperature of 80–90°C , is recommended. (Nedić, Vesić, Vasiljević, 2008, 133–134)

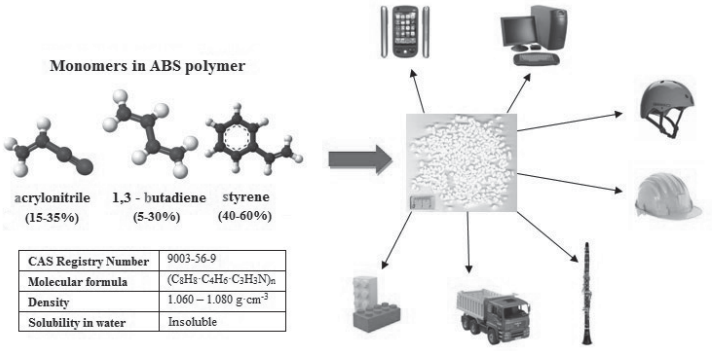


Figure 13 *Production Technology of the thermoplastics based on ABS polymers*

Important innovation in production of the ballistic protective equipment is introduction of new materials that are currently being developed by the United States Army. In fact, it is the Liquid body armor which is characterized by great flexibility and allows its user to move freely. Key component of this material is STF (Shield-Thickening Fluid)[24], which represents a combination of a solid and a liquid phase (colloidal silica nanoparticles) (Figure 14) and polyethylene glycol. Liquid phase is highly filled with the solid colloidal particles, which give excellent performance to the material in terms of strength and projectiles energy drainage.[25]

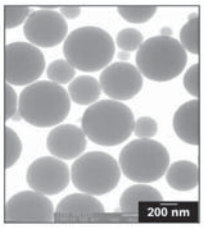


Figure 14 *Micrograph of colloidal silicon nanoparticles*

Under normal conditions body armor possess liquid state, but when it hit with the missile it becomes firm and prevents further penetration of the projectiles (Figure 15).

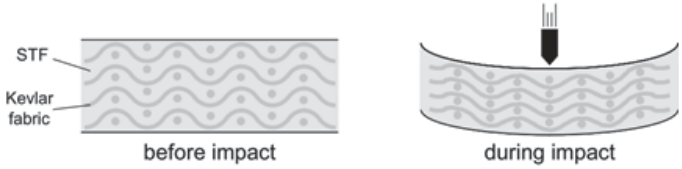


Figure 15 *Schematic behavior of the STF component reinforced materials before and during the impact of the projectiles*

During manufacturing, Kevlar is well soaked in STF (Figure 16), and furthermore such fabric can then be tailored and drenched as any other fabric.

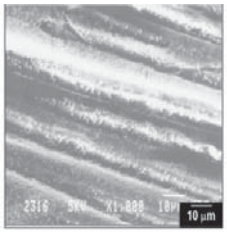


Figure 16 *Micrograph of Kevlar fibers impregnated with STF*

24 See also: http://www.ccm.udel.edu/STF/
25 Lee, Y. S et al. (2002). Advanced Body Armor Utilizing Shear Thickening Fluids. 23rd Army Science Conference, Orlando, FL.

Liquid armor is more resistant to stabbing in contrast to the conventional armors. Whereas, ceramic or titanium inserts are unnecessary here since liquid body armor shows protection of the internal organs from trauma as well. In summary, new body armor is lighter and more flexible, which in turn reduced user's fatigue. It could be used to drench parts of the equipment which are not covered by the armors or larger covered areas to neutralize the effects of explosive devices[26].

CONCLUSION

This paper presents the need of modern society and the members of Security Services for ballistic protective equipment, which will allow its users a high degree of self–protection, comfort, flexibility, or the smooth movement in the execution of security and operational tasks.

In the process of designing ballistic protective equipment it is necessary to determine the degree of potential danger, select the material or combination of materials accordingly, and also optimize the total weight of protective equipment.

Ballistic protection is mainly based on the multilayer synthetic fabrics that are made of polyethylene, aramid or other types of artificial fibers. One of the first materials that have been developed is *Kevlar*® fiber. Kevlar fiber belongs to the class of para–aramid synthetic fibers. Furthermore it possesses high strength, low weight, high chemical resistance, also resistance to cutting, temperature changes and the water impact. Anti–ballistic resistance is provided by the development of improved generation of these materials, which enabled protection from firearms, knives and stabbing.

Spectra® fibers are type of polyethylene fibers, which are extremely resistant to tearing, and have extremely high chemical resistance and very low resistance to cutting.

Dyneema® fiber is commercially polyethylene fiber that is currently the strongest fiber in the world. Besides, it offers maximum strength combined with low weight and protection from firearms and bladed weapons, or protection of pistol ammunition, fragments and knives.

In the process of manufacturing of the protective helmets, thermoplastics based on ABS polymers are used, which enabled impact and chemicals resistance.

Liquid body armor is an important innovation, which represent the combination of solid and liquid phase material. In addition to that it provided excellent properties in terms of strength and projectile's draining energy as well as the flexibility and smooth movement of its users.

Further development of the materials in the forensic industry is directed towards higher levels of optimization and improvement of nano–fiber, synthetic and biological materials, which provide a high level of protection, maximum comfort and minimal weight, as well as smooth movement of its users, both to civilians and for officials.

Throughout review of the materials used in the manufacturing of the ballistic protective equipment this paper is primarily intend to point out performances and thus give future guidance on improvements of the equipment that will be used in security services.

REFERENCES

1. Azrin Hani, A. R. *et al.* (2012). Body Armor Technology: A Review of Materials, Construction Techniques and Enhancement of Ballistic Energy Absorption. *Advanced Materials Research Vols. 488–489*, 806–812.

2. Ballistic Resistance of Body Armor–NIJ Standard–0101.06. (2008). Washington: National Institute of Justice, https://www.ncjrs.gov/pdffiles1/nij/223054.pdf

3. Egres, R. G. Jr. *et al.* (2004). Stab Resistance of Shear Thickening Fluid (STF)–Kevlar Composites for Body Armor Applications. *Proceedings of the 24th Army Science Conference*, Orlando, FL.

4. Henderson, J. (2008). *Ballistic Body Armor: Protecting the Protectors*. CMGT 564 Strategic Standardization.

5. Inženjersko tehnički priručnik (1976). U D. Papadopolos (ur.), *Materijali*: šesta knjiga. Beograd: Izdavačko preduzeće „Rad".

6. Lee, Y. S. *et al.* (2002). Advanced Body Armor Utilizing Shear Thickening Fluids. *23rd Army Science Conference*, Orlando, FL.

26 Egres, R. G. Jr. *et al.* (2004). Stab Resistance of Shear Thickening Fluid (STF)–Kevlar Composites for Body Armor Applications. *Proceedings of the 24th Army Science Conference*, Orlando, FL.

7. Lukkassen, D., Meidell, A. (2007). *Advanced Materials and Structures and their Fabrication Processes (Book manuscript)*, Narvik University College, HiN, Norway.
8. Maksimović, R., Divjaković, V. (1996). The application of high performance polyethylen fibers in manufacturing protection equipment for the security service. *NBP: Journal of Criminalistics and Law*, *1*(1), 1–9.
9. Maksimović, R. *et al.* (1995). Struktura i sastav savremenih antibalističkih prsluka. *Zbornik radova Policijske akademije*, (1), 111–117.
10. Nedić, B., Vesić, N., Vasiljević, D. (2008). *Boja, kolorimetrija i plastične mase*. Kragujevac: Mašinski fakultet.
11. Radovanović, R., Ristić, M., Milić, J. (2014). Forenzički značaj određivanja parametara dejstva pištoljskih projektila. U Lj. Mašković (ur.), *Kriminalističko–forenzička obrada mesta krivičnih događaja: tematski zbornik radova II* (str. 149–162). Beograd: Kriminalističko–policijska akademija.
12. Radonjić, V. *et al.* (2014). Unapređenje balističkih karakteristika i održavanja zaštitnih balističkih prsluka. *Vojnotehnički glasnik*, *62* (4), 89–103.
13. Spasova, S., Srebrenkoska, V. (2011). Dizajn zaštitne odeće. *Zbornik radova sa konferencije*. Štip: Univerzitet „Goce Delčev", http://eprints.ugd.edu.mk/2506/1/P-36%20trud.pdf
14. *Stab Resistance of Personal Body Armor–NIJ Standard–0115.00*. (2000). Washington: National Institute of Justice, https://www.ncjrs.gov/pdffiles1/nij/183652.pdf
15. Utracki, L. A. (2010). *Rigid ballistic composites (Review of literature)*. Advanced Materials Design, Industrial Materials Institute, National Research Council, Canada.

UDC: 543.068:582.635.38
343.983.2:613.83

CHEMOMETRICS AS POWERFUL TOOL FOR DETERMINATION OF THE ORIGIN OF CANNABIS SAMPLES

Slavica Razic[1]
University of Belgrade, Faculty of Pharmacy, Department of Analytical Chemistry
Natasa Radosavljevic-Stevanovic[2]
The National Crime-Technical Centre, Ministry of Interior of the Republic of Serbia

Abstract: The plant species of *Cannabis sativa,* produced illegally, in indoor or outdoor conditions, is a very common forensic sample. Police forces are usually faced with the lack of information about the particular place of its production. In order to conduct the characterization of such samples, the TLC and GC-FID techniques were applied for determination of organic fraction. Determination of inorganic fraction was conducted by AAS techniques. The obtained results were subjected to the chemometric evaluation, together with the results of soil analysis where plants were cultivated. The conclusions of this study could be used for determination of origin of cannabis and its production and thus be an instrument for law enforcement officers.

Keywords: cannabis production, TLC, characterization, forensics, examination.

INTRODUCTION

The police authorities usually seize a large quantity of illicit drugs. The majority of the drugs are samples of *Cannabis sativa* plants produced illegally. This plant is widely produced all around the world in indoor and outdoor conditions. Production, possession and smuggling of this material is prohibited according to the law regulative in Serbia.

This material is also widely consumed by the population in each country and therefore establishing of a system for classifying the origin of this plant can be a challenge for scientists and a great benefit for the police authorities. For this reason, many attempts have been made recently in the different domains of science: biology, chemistry, forensics, and statistics with the mutual aim of classifying the geographical origin of *Cannabis sativ*a samples.

For the forensic purposes, the most significant compounds in Cannabis samples are cannabinoids, terpenophenolic compounds unique to cannabis[3] . For the forensic practice, the most important cannabinoids are: Δ^9-tetrahydrocannabinol (Δ^9-THC), cannabinol (CBN) and cannabidiol (CBD) (Figure 1). The first compound, Δ^9-THC is psychoactive component, while the other two mentioned cannabinoids are not.

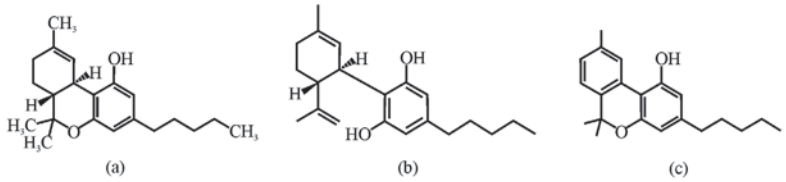


Figure 1 *Structures of cannabinoids: a) Δ^9-THC (−)-(6aR,10aR)-6,6,9-trimethyl-3-pentyl-6a,7,8,10a-tetrahydro-6H-benzo[c]chromen-1-ol, b) CBD 2-[(1R,6R)-6-isopropenyl-3-methylcyclohex-2-en-1-yl]-5-pentylbenzene-1,3-diol, c) CBN 6,6,9-trimethyl-3-pentyl-benzo[c]chromen-1-ol*

1 slavica.razic@pharmacy.bg.ac.rs
2 natasa.radosavljevicstevanovic@mup.gov.rs
3 Pate DW. 1994. Chemical Ecology of Cannabis. J. Int. Hemp Ass. 2(29):32-37.

Transition metals are important for plant growth and they are distributed in different cells, in certain concentrations due to the established homeostasis. Hemp has the ability to tolerate and accumulate heavy metals; the highest concentrations of the metals Cd, Pb, Ni, Cu and Zn were found in leaves[4],[5],[6].

Bearing in mind the lack of literature on possible correlations between content of cannabinoids in Cannabis plants and metals in both Cannabis samples and soil where the plants were cultivated, multivariate methods were applied aiming to assist in determination of origin of cannabis and its production.

EXPERIMENTAL

Young plants of *Cannabis sativa* species were seized by the Police authorities as material planted by the criminal groups on different locations in Serbia. The plants were grown illegally under controlled indoor conditions by applying certain levels of temperature, humidity and intensity of light. The plants were randomly selected from the plantations in the early growing stage for the purpose of forensic analyses. The rhizosphere soil from the root zone at a depth of 5-10 cm was sampled. The plant samples were further separated into roots, stems and leaves. The root parts were cleaned from traces of soil, washed with deionised water and dried. The Cannabis leaves were dried and grounded to a powder. The samples were prepared for the TLC method[7]. In further process the 20 mg of each sample were dissolved in 5 mL methanol, shaken in an ultrasonic bath for 30 min, filtered and evaporated to dryness. The residue was reconstituted with 2 mL of methanol. 1 μL of the resulting solution for each sample was injected into the GC-FID system in order to analyse the content of cannabinoids. For the purpose of elemental analysis, the sampled soils, roots, stems and leaves were subjected to microwave-assisted acid digestion, according to a known procedure[8].

SOLUTIONS AND REAGENTS

All reagents for both elemental and cannabinoid content analyses were of analytical grade and double distilled water was used for preparation of all solutions. Methanol, n-hexane and diethyl-ether were purchased from Merck (Germany) and reference materials of cannabinoids were purchased from Lipomed (Austria): a solution of Δ^9THC 50 mg/mL in ethanol, CBD and CBN in the solid state with purity of 99.090±0.199 % and 99.337±0.018 %, respectively. Stock solutions of cannabinoids in methanol, were prepared in concentrations of 0.1, 0.05, 0.025, 0.01 and 0.005 mg/mL for Δ^9THC, CBD and CBN. Stock solutions of Cu, Zn, Fe, Mn, Cr, Ca and Mg salts (1 g/L) were purchased from Merck (Germany). Working solutions were made by dilution of the corresponding stock solutions with 2.5 % nitric acid (HNO_3). Nitric acid (65 %, v/v) was provided by Merck and a solution of H_2O_2 (30%, v/v) was provided by Zorka Pharma Šabac (Serbia).

INSTRUMENTAL AND OPERATING PARAMETERS

The determination of the cannabinoids by thin layer chromatography (TLC) with plates made of aluminium and covered with silica gel with fluorescence indicator of UV254 was performed by conducting the semi quantitative analyses[9].

The determination of the cannabinoids was performed using an Agilent GC System, Model 7890A, fitted with a Flame Ionization Detector. The conditions were as follows: column HP-5 (30 m × 320 μm × 0.25 μm), injection temperature: 250 °C, splitless mode, oven program: initial temperature 150 °C for 0 min, heating rate 15 °C/min to 300 °C and held for 5 min, nitrogen flow rate: 46 mL/min.

The determination of the Cu, Zn, Mn, Fe, Ca and Mg was done using a Perkin-Elmer Model 5000 atomic absorption spectrophotometer, operated under optimized measurement conditions using suitable

4 Linger P, Müssing J, Fischer H, Kobert J. 2002. Industrial hemp (*Cannabis sativa* L.) growing on heavy metal contaminated soil: fibre quality and phytoremediation potential. Ind. Crop. Prod. 16:33-42.
5 Clemens S. 2001. Molecular mechanisms of plant metal tolerance and homeostasis, Planta. 212:229-248.
6 Küpper H, Lombi E, Zhao FJ, McGrath SP. 1999. Cellular compartmentation of zinc in leaves of hyperaccumulator Thlaspi caerulescens. Plant Physiol. 119: 305-312.
7 Determination of tetrahydrocannabinol in C*annabis sativa* plant and its products by semi quantitative method of Thin Layer Chromatography, ЦЈ-01-(03,04,05)/01-03-22, 2013, The National Criminalistic-Technical Centre, Ministry of Interior of the Republic of Serbia, Belgrade.
8 Razic S, Djogo S, Slavkovic L. 2006. Multivariate characterization of herbal drugs and rizosphere soil samples according to their metallic content. Microchem. J. 84: 93-101.
9 Determination of tetrahydrocannabinol in C*annabis sativa* plant and its products by semi quantitative method of Thin Layer Chromatography, ЦЈ-01-(03,04,05)/01-03-22, 2013, The National Criminalistic-Technical Centre, Ministry of Interior of the Republic of Serbia, Belgrade.

hollow cathode lamps[10]. The determination of the Cr was accomplished using a Perkin-Elmer Model 5000 atomic absorption spectrophotometer with a graphite furnace HGA 400 Automatic Burner Control, with pyrolytic graphite tubes[11].

Statistical analysis was performed using SPSS 11.0 (SPSS Inc., Chicago, IL) and Minitab 13.20 (Minitab Inc., State College, PA), for Windows software packages.

RESULTS AND DISCUSSION

Since the roots contain only trace amounts of these substances while the stems, branches and twigs have less than the leaf material, the cannabinoid content was measured only in the leaves[12].

For the purpose of comparison of the cannabinoid content in the young plants and the mature one the semi quantitative method of the TLC was conducted and the difference in the cannabionid content was detected. Figure 2 shows the TLC plate with the spots of the reference materials and the examined samples. The levels of three cannabinoids are low in young plants (the level of THC is below 0.3%) and much higher in mature (the level of THC is over 0.3%). The CBN is visible in a small concentration in the sample "M" since it is a plant analyzed three years after the harvest and therefore the psychoactive THC was degraded into CBN. The sample "Mc" contained only THC, since it was analyzed immediately after harvesting.

Figure 2 *TLC plate with certified reference materials of cannabinoids (CBN: cannabinol, THC: tetrahydrocannabinol, CBD: cannabinol), young plants samples (8, 12, 16, 20, 24, 28) and mature plants samples (M u Mc)*

The cannabinoid content in the leaves of the examined cannabis plants was determined by external calibration. The values varied from 0.03 to 1.47 mg/mL for THC and from 0.11 to 1.12 mg/mL for CBN. The lowest levels were from 0.003 to 0.06 mg/mL for CBN, what is reasonable since the level of this cannabinoid, as degradation product of THC, increases with time during storage of cannabis plants. Different factors influence these variations: the genetic characteristic of the seeds[13],[14], the environmental conditions such as light, temperature, moisture and oxygen [15], [16] and the maturity [17].

Quantification of metals was performed by external calibration. The accuracy of the methods was checked by analysis of a standard reference material, NIST SRM 1547 – Peach Leaves and NIST SRM 2711 - Montana II Soil, when satisfactory recoveries (90.06 – 115.35 %) were obtained, (Table 1).

Table 1 *Analyses of metals in standard reference material for Peach leaves and Montana Soil*

	NIST SRM 1547 PEACH LEAVES			NIST SRM 2711 MONTANA SOIL		
	Found	**Certified**	**Recovery %**	**Found**	**Certified**	**Recovery %**
Cu [mg/kg]	3.2±0.9	3.7±0.4	86	96±10	114±2	84
Fe [mg/kg]	197±6	218±14	90	3.8±0.1	2.89±0.06	131
Mn [mg/kg]	70.5±0.9	98±3	72	398±13	638±28	62
Zn [mg/kg]	15±1	17.9±0.4	84	317±12	350.4±4.8	90
Cr [mg/kg]	2.85±0.03			22±2	47	47
Ca [%]	1.01±0.07	1.56±0.02	65	1.34±0.09	2.88±0.08	47
Mg [%]	0.456±0.007	0.432±0.008	106	0.725±0.009	1.05±0.03	69

10 Razic S, Onija A, Slavkovic L, Popovic A. 2005. Determination of metal content in some herbal drugs - Empirical and chemometric approach. Talanta. 67:233-239.
11 Razic S, Djogo S, Slavkovic L. 2006. Multivariate characterization of herbal drugs and rizosphere soil samples according to their metallic content. Microchem. J. 84: 93-101.
12 Pate DW. 1994. Chemical Ecology of Cannabis. J. Int. Hemp Ass. 2(29):32-37.
13 Bouquet JR. 1950. Cannabis. Bull. Narcotics. United Nations Publ. II:14–30.
14 Taylor BJ, Neal JD, Gough TA. 1985. The physical and chemical features of cannabis plants grown in the United Kingdom of Great Britain and Northern Ireland from seeds of known origin – Part III: third and fourth generation studies. Bull. Narcotics. United Nations Publ. XXXVII:75–81.
15 Mechoulam R. 1973. Cannabinnoid Chemistry: In Marijuana, Chemistry, Metabolism, Pharmacology and Clinical effects. Academic Press, New York.
16 Nahas G. 1978. Symposium on Marijuana. Bull. Narcotics. United Nations Publ. XXX: 23–3.
17 Baker PB, Fowler R, Bagon KR, Gough TA. 1980. Determination of the distribution of cannabinoids in cannabis resin using high-performance liquid chromatography. J. Anal. Toxicol. 4: 145–152.

In general, the obtained values for measured metals in soils were within their expected ranges[18]. The copper values ranged from 8.0 to 54.6 mg/kg; the concentrations of iron were low: from 1026 to 7626 mg/kg; the values of manganese were lower than expected and varied from 67 to 1729 mg/kg: the zinc values were also lower, ranging from 30-161 mg/kg, chromium varied significantly from 5 to 74 mg/kg. The values for calcium and magnesium were from 15283.63-38195700 mg/kg and 2284.09-12045.13 mg/kg, respectively.

Finding patterns to classify the geographical origin of cannabis plants has already escalated in recent years; a number of 15 elements were measured from the cannabis leaf and correlated with soils and the cannabinoids content[19]. Carbon and nitrogen isotopic ratios are related to plant growth and could be useful as indicators of origin[20]. Despite its potentiality, the use of this technique to determine the origin of cannabis plant has not yet been practically applied[21].

The chemmometrics as a powerful method is widely applied in forensic analyses. In connection with the chromatographic methods, it was a comprehensive tool to conduct drugs profiling procedures[22].

The objective of this study was to analyze the correlations of seven metals and three main cannabinoids using multivariate methods of analysis. Firstly, the Ryan-Joiner test was applied for testing the distribution of the data. Then, the outliers were detected by the Grubbs test and discarded in a few cases to avoid interruption of the further modelling. The basic data matrix was composed of samples as rows, and organics and metals as columns. The correlation analysis was assessed by the Pearson's coefficient and the results are presented in Table 2.

Table 2 *The correlation matrix of the elements and cannabinoids data (Pearson correlation)*

	Cu	**Fe**	**Mn**	**Zn**	**Cr**	**Ca**	**Mg**	**THC**	**CBD**
Fe	-0.344								
	0.505								
Mn	0.484	-0.134							
	0.331	0.800							
Zn	0.201	-0.675	0.496						
	0.702	0.142	0.317						
Cr	-0.097	0.628	-0.097	-0.775					
	0.855	0.182	0.855	0.070					
Ca	0.452	0.464	0.443	-0.224	0.649				
	0.368	0.354	0.379	0.670	0.163				
Mg	-0.724	0.272	-0.176	-0.148	-0.190	-0.622			
	0.104	0.602	0.739	0.780	0.719	0.188			
THC	0.061	-0.379	0.791	0.618	-0.373	-0.145	0.285		
	0.909	0.459	0.061	0.191	0.467	0.784	0.584		
CBD	-0.113	-0.411	-0.331	0.596	-0.659	-0.378	-0.176	-0.209	
	0.831	0.418	0.522	0.212	0.155	0.460	0.379	0.691	
CBN	0.332	-0.602	0.813	0.802	-0.545	-0.111	0.000	0.929	0.011
	0.520	0.206	0.049	0.055	0.263	0.835	1.000	0.007	0.984

The concentration data were subjected to principal component analysis (PCA) in order to highlight any relations between the elements. With PCA, the data reduction was realised by transforming the data into orthogonal components that are linear combinations of the origin variables. The initial statistics of Eigen analysis of the correlation matrix was realised and the corresponding scree plot is presented in Figure 3[23].

18 Kabata-Pendias A, Pendias H. 2001. Trace elements in soils and plants: Soils Constituents. 3rd ed. Boca Raton FL: CRC Press.
19 Coffman CB, Gentner WA. 1975. Cannabinoid profile and elemental uptake of *Cannabis sativa* L. as influenced by soil characteristics. Agron. J. 67:491-497.
20 Denton TM, Schmidt S, Chritchley C, Stewart GR. 2001. Natural Abundance of stable carbon and nitrogen isotopes in *Cannabis sativa* reflects growth conditions. Aust. J. Plant Physiol. 28 (10):1005-1012.
21 Shibuya EK, Sarkis JES, Negrini-Neto O, Martinelli LA. 2007. Carbon and nitrogen stable isotopes as indicative of geographical origin of marijuana samples seized in the city of Sao Paulo (Brazil). Forensic Sci. Int. 167:8-15.
22 Dufey V, Dujourdy L, Besacier F, Chaudron H, 2007, A quick and automated method for profiling heroin samples for tactical intelligence purposes, Forensic Science International, 169 108–117.
23 Kaiser HF.1960. Educ. Psychol. Meas. 20(1):141–151.

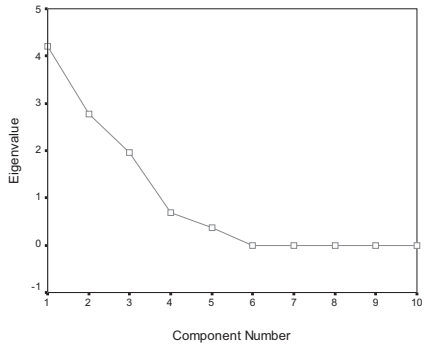


Figure 3 *Scree plot*

According to the Kaiser Criterion, only the first three PCs should be retained as the subsequent eigenvalues are all less than one. It can be seen that four principal components (PCs) appeared to account for 89.42% of the variance of the data. Hence, the reduced dimensionality of the descriptor space is three.

One of the main objectives of PCA is to identify factors that are meaningful. PCA is based on the assumption that the direction of the largest variance in the data carries most of the information. The results of the principal components factor analysis of the correlation matrix produce the first unrotated component matrix, which gives the first insight into factors solutions. To obtain a better insight into the latent structure of the data, the principal component extracted correlation matrix was subjected to Varimax orthogonal rotation. Rotation of the coordinate system of factors will not affect the position of the objects relative to each other but will simplify the structure of the factors (Table 3). For better visualization, Figure 4 is presented to illustrate a principal component plot in rotated space (Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization; rotation converged in 5 iterations).

Table 3 *Rotated component matrix*

	Component		
	1	2	3
Cu	0.258	-0.091	0.842
Fe	-0289	0.790	-0.177
Mn	0.912	0.123	0.345
Zn	0.548	-0.765	0.129
Cr	-0.266	0.878	0.194
Ca	0.071	0.601	0.721
Mg	0.142	0.115	-0.965
THC	0.966	-0.134	-0.191
CBD	-0.334	-0.851	0.021
CBN	0.920	-0.380	0.081

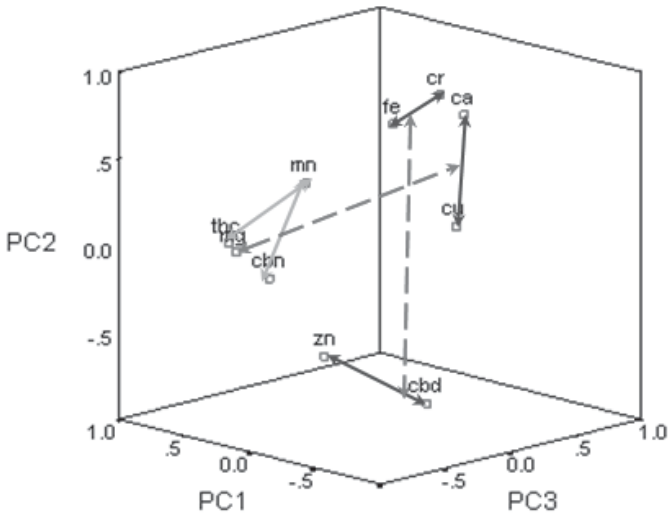


Figure 4 *Component plot in rotated space*

Features with high positive or negative loadings essentially determine the factor. A rule cannot be made about the minimum amount of loadings which can be interpreted. These factors are related to the sources of the elements and cannabinoids in the studied samples.

If a limit of 0.7 for a coefficient is kept, except for the first, all other factors express the importance of single elements. Although the correlations between some elements indicate that they arise from the same source, some additional sources have to be considered for the others. The first factor comprises Mn, THC and CBN with high loadings. A correlation like this indicates that they arise from the same sources.

Fe and Cr show significant positive loadings in the second factor and are negatively correlated with Zn and CBD with high negative loading. The third factor is dominantly loaded by Cu as an essential element; a constituent of co-enzymes important for a plant cycle. It is also correlated with Mg, with a high but negative loading. These correlations led to the consideration of the biosynthesis of cannabinoids and the involvement of metals as cofactors in the enzymatic catalyzed synthesis cycles. An enzyme CBDA synthase, an oxidoreductase was identified, as the one responsible for synthesis of CBDA from CBGA, assuming that no coenzymes or cofactors are involved[24]. The enzyme responsible for the synthesis of THCA was identified as THCA synthase[25]. Cannabinoids are synthesized in their acidic form as cannabinoic acids, which are converted into their neutral forms during storage of the plant material[26]. Despite the synthesis previously suggested [27](Figure 5),

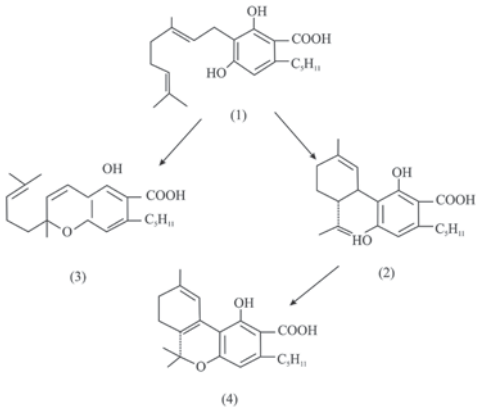


Figure 5 *Biosynthesis of cannabinoid acids: 1 = cannabigerol (CBG); 2 = cannabidiol (CBD); 3 = cannabichromene (CBC); 4 = delta-9-tetrahydrocannabinol (THC)*

a new biosynthetic pathway was proposed, which starts form geranylpyrophosphate giving CBCA, CBDA and THCA *via* CBGA[28]. Further, THCA synthase is an FAD-dependent enzyme and catalyzes the oxidative cyclisation of CBGA into THCA[29]. This reaction requires molecular oxygen for re-oxidation of the coenzyme and also produces hydrogen peroxide in a 1:1 molar ratio to THCA. Such a produced amount of hydrogen peroxide would be toxic[30]. CBDA synthase is the enzyme responsible for CBDA synthesis, which is also an FAD-dependent enzyme. Reduced flavin is reactivated by forming the hydrogen peroxide. THCA synthase and CBDA synthase catalyze the oxidative cyclisation of CBGA to form THCA and CBDA, respectively, while THC and CBD are generated from THCA and CBDA by non-enzymatic decarboxylation. The proposed synthesis reactions are given in Figure 6.

24 Taura F, Morimoto S, Shoyama Y. 1996. Purification and characterization of cannabinolic acid synthase from *Cannabis Sativa* L. J. Biol. Chem. 271:17411-17416.
25 Taura F, Morimoto S, Shoyama Y. 1995. First direct evidence for mechanism of delta-1-tetrahydrocannabinolic acid biosynthesis. J. Am. Chem. Soc. 38:9766-9767.
26 De Meijer EPM, Bagatta M, Carboni A, Crucitti P, Moliterni VMC, Ranalli P, Mandolino G. 2002. The inheritance of Chemical Phenotype in *Cannabis sativa* L. Genetic. 163:335-346.
27 Pate DW. 1994. Chemical Ecology of Cannabis. J. Int. Hemp Ass. 2(29):32-37.
28 De Meijer EPM, Bagatta M, Carboni A, Crucitti P, Moliterni VMC, Ranalli P, Mandolino G. 2002. The inheritance of Chemical Phenotype in *Cannabis sativa* L. Genetic. 163:335-346.
29 Sirikantaramas S, Morimoto S, Shoyama Y, Ishikawa Y, Wada Y, Taura F. 2004. The gene controlling marijuana psychoactivity: molecular cloning and heterologous expression of Δ1-tetrahydrocannabinolic acid synthase from *Cannabis sativa* L. J. Biol. Chem. 279:39767–39774.
30 Sirikantaramas S, Taura F, Tanaka Y, Ishikawa Y, Morimoto S, Shoyama Y. 2005. Tetrahydrocannabinolic Acid Synthase, the enzyme controlling marijuana psycho-activity, is secreted into the storage cavity of glandular trichomes. Plant Cell Physiolol. 46(9):1578-1528.

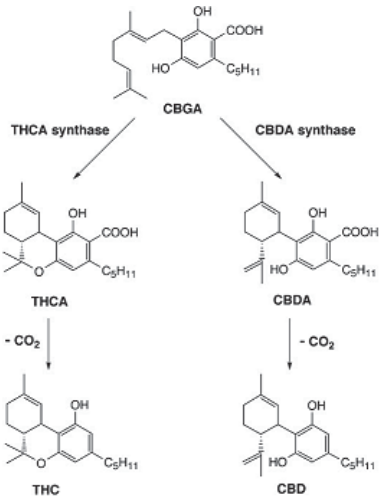


Figure 6 *Biogenesis of THCA and CBDA and decarboxylation to THC and CBD*

The toxic hydrogen peroxide is further converted into water and dioxygen by catalases containing haem iron groups or dimanganese centre[31]. Considering the facts stated above, an attempt was made to explain the positive correlation of manganese, THC and CBN. It was assumed that the catalase that decomposes the hydrogen peroxide derived from the synthesis of THCA contains a Mn(III) centre. Conversion of the peroxide into water and dioxygen, via red-ox reaction between manganese peroxide enables the cofactor to be again active[32].The mentioned reactions are energetically favoured, since $\Delta G < 0$[33].

The positive correlation of Mn and CBN was expected since CBN is the primary degradation product of THC.

The negative correlation of Fe and Cr to CBD can be explained by the hypothesis that catalase responsible for the conversion of the peroxide derived from CBDA synthase reaction might have haem iron groups. Although the complete mechanism of such catalase has not yet been confirmed, the predicted mechanism has the transition state: O=Fe(IV)–Enzyme(+) [34] which is energetically unstable and thus the reactions are unfavourable[35].

Since Cr and Fe occur together in nature as a complex oxide, the negative correlation of Cr to CBD is explained with the mutually positive correlation of Fe and Cr.

The negative correlation of Mg with Cu may arise from the fact that the radii of their ions are similar and thus they could be competitive metals during plant uptake.

CONCLUSION

This work is conducted in order to determine weather the metals content in rhizosphere and *Cannabis* plants can affect the levels of three important cannabinoids. Using the results obtained by the instrumental techniques and applying the chemmometrics, we have come to the conclusion that available manganese makes the synthesis of THC favourable while the synthesis of CBD is not favourable by iron present in the *Cannabis sativa* plants. The role of other elements, like Mn and Cr were highlighted too. The levels of metals in rhizosphere and *Cannabis sativa* plants could be a good indicator for the content of cannabinoids important for the forensic investigation. This work can be useful for forensic scientists and further for the intelligence service since it represents the basis for determination of the origin of the *Cannabis sativa* plants.

31 Wu AJ, Penner-Hahn JE, Pecoraro VL. 2004. Structural, spectroscopic, and reactivity models for the manganese catalases. Chem. Rev. 104:903–938.

32 Wu AJ, Penner-Hahn JE, Pecoraro VL. 2004. Structural, spectroscopic, and reactivity models for the manganese catalases. Chem. Rev. 104:903–938.

33 Radosavljevic-Stevanovic N., Markovic J., Agatonovic-Kustrin S., Razic S., Metals and organic compounds in the biosynthesis of cannabinoids: a chemometric approach to the analysis of Cannabis sativa samples, Natural Product Research: Formerly Natural Product Letters (2014) DOI: 10.1080/14786419.2014.880912.

34 Boon EM, Downs A, Marcey D, Proposed Mechanism of Catalase, Catalase: H_2O_2: H_2O_2 Oxidoreductase: Catalase Structural Tutorial. Retrieved 2007-02-11. Available from: http://biology.kenyon.edu/BMB/Chime/catalase/frames/cattx.htm#Proposed%20Mechanism%20of%20Catalase.

35 Radosavljevic-Stevanovic N., Markovic J., Agatonovic-Kustrin S., Razic S., Metals and organic compounds in the biosynthesis of cannabinoids: a chemometric approach to the analysis of Cannabis sativa samples, Natural Product Research: Formerly Natural Product Letters (2014) DOI: 10.1080/14786419.2014.880912.

REFERENCES

1. Baker PB, Fowler R, Bagon KR, Gough TA. 1980. Determination of the distribution of cannabinoids in cannabis resin using high-performance liquid chromatography. J. Anal. Toxicol. 4: 145–152.
2. Boon EM, Downs A, Marcey D, Proposed Mechanism of Catalase, Catalase: H_2O_2: H_2O_2 Oxidoreductase: Catalase Structural Tutorial. Retrieved 2007-02-11. Available from: http://biology.kenyon.edu/BMB/Chime/catalase/frames/cattx.htm#Proposed%20Mechanism%20of%20Catalase
3. Bouquet JR. 1950. Cannabis. Bull. Narcotics. United Nations Publ. II: 14–30.
4. Clemens S. 2001. Molecular mechanisms of plant metal tolerance and homeostasis, Planta. 212:229-248.
5. Coffman CB, Gentner WA. 1975. Cannabinoid profile and elemental uptake of *Cannabis sativa* L. as influenced by soil characteristics. Agron. J. 67:491-497.
6. De Meijer EPM, Bagatta M, Carboni A, Crucitti P, Moliterni VMC, Ranalli P, Mandolino G. 2002. The inheritance of Chemical Phenotype in *Cannabis sativa* L. Genetic. 163:335-346.
7. Denton TM, Schmidt S, Chritchley C, Stewart GR. 2001. Natural Abundance of stable carbon and nitrogen isotopes in *Cannabis sativa* reflects growth conditions. Aust. J. Plant Physiol. 28 (10):1005-1012.
8. Determination of tetrahydrocannabinol in C*annabis sativa* plant and its products by semi quantitative method of Thin Layer Chromatography, ЦЈ-01-(03,04,05)/01-03-22, 2013, The National Criminalistic-Technical Centre, Ministry of Interior of the Republic of Serbia, Belgrade.
9. Dufey V, Dujourdy L, Besacier F, Chaudron H, 2007, A quick and automated method for profiling heroin samples for tactical intelligence purposes, Forensic Science International, 169 108–117.
10. Fonseca BM, Costa MA, Almada M, Correia-da-Silva G, Teixeira NA, 2013, Endogenous cannabinoids revisited: A biochemistry perspective, Prostaglandins and Other Lipid Mediators, 102-103. 13-30.
11. Hill AJ, Williams CM, Whalley BJ, Stephens GJ, 2012, Phytocannabinoids as novel therapeutic agents in CNS disorders, Pharmacology & Therapeutics, 133, 79–97.
12. Kabata-Pendias A, Pendias H. 2001. Trace elements in soils and plants: Soils Constituents. 3rd ed. Boca Raton FL: CRC Press.
13. Kaiser HF. 1960. Educ. Psychol. Meas. 20(1):141–151.
14. Küpper H, Lombi E, Zhao FJ, McGrath SP. 1999. Cellular compartmentation of zinc in leaves of hyperaccumulator Thlaspi caeulescens. Plant Physiol. 119: 305-312.
15. Linger P, Müssing J, Fischer H, Kobert J. 2002. Industrial hemp (*Cannabis sativa* L.) growing on heavy metal contaminated soil: fiber quality and phytoremediation potential. Ind. Crop. Prod. 16:33-42.
16. Mechoulam R. 1973. Cannabinnoid Chemistry: In Marijuana, Chemistry, Metabolism, Pharmacology and Clinical effects. Academic Press, New York.
17. Nahas G. 1978. Symposium on Marijuana. Bull. Narcotics. United Nations Publ. XXX: 23–32.
18. Pate DW. 1994. Chemical Ecology of Cannabis. J. Int. Hemp Ass. 2(29):32-37.
19. Radosavljevic-Stevanovic N., Markovic J., Agatonovic-Kustrin S., Razic S., Metals and organic compounds in the biosynthesis of cannabinoids: a chemometric approach to the analysis of Cannabis sativa samples, Natural Product Research: Formerly Natural Product Letters (2014) DOI: 10.1080/14786419.2014.880912.
20. Razic S, Djogo S, Slavkovic L. 2006. Multivariate characterization of herbal drugs and rizosphere soil samples according to their metallic content. Microchem. J. 84: 93-101.
21. Razic S, Onija A, Slavkovic L, Popovic A. 2005. Determination of metal content in some herbal drugs - Empirical and chemometric approach. Talanta. 67:233-239.
22. Shibuya EK, Sarkis JES, Negrini-Neto O, Martinelli LA. 2007. Carbon and nitrogen stable isotopes as indicative of geographical origin of marijuana samples seized in the city of Sao Paulo (Brazil). Forensic Sci. Int. 167:8-15.
23. Sirikantaramas S, Morimoto S, Shoyama Y, Ishikawa Y, Wada Y, Taura F. 2004. The gene controlling marijuana psychoactivity: molecular cloning and heterologous expression of Δ1-tetrahydrocannabinolic acid synthase from *Cannabis sativa* L. J. Biol. Chem. 279:39767–39774.
24. Sirikantaramas S, Taura F, Tanaka Y, Ishikawa Y, Morimoto S, Shoyama Y. 2005. Tetrahydrocannabinolic Acid Synthase, the enzyme controlling marijuana psychoactivity, is secreted into the storage cavity of glandular trichomes. Plant Cell Physiolol. 46(9):1578-1528.
25. Taura F, Morimoto S, Shoyama Y. 1995. First direct evidence for mechanism of delta-1-tetrahydrocannabinolic acid biosynthesis. J. Am. Chem. Soc. 38:9766-9767.

26. Taura F, Morimoto S, Shoyama Y. 1996. Purification and characterization of cannabinolic acid synthase from *Cannabis Sativa* L. J. Biol. Chem. 271:17411-17416.

27. Taylor BJ, Neal JD, Gough TA. 1985. The physical and chemical features of cannabis plants grown in the United Kingdom of Great Britain and Northern Ireland from seeds of known origin – Part III: third and fourth generation studies. Bull. Narcotics. United Nations Publ. XXXVII: 75–81.

28. United Nations Office on Drugs and Crime (UNODC), Recommended Methods for the Identification and Analysis of Cannabis and Cannabis Products, (2009) http://www.unodc.org/documents/scientific/ST-NAR-40-Ebook.pdf (retrieved October 2009).

29. Wu AJ, Penner-Hahn JE, Pecoraro VL. 2004. Structural, spectroscopic, and reactivity models for the manganese catalases. Chem. Rev. 104:903–938.

UDC: 343.983.2:662.3

DETERMINATION OF FALSE POSITIVES IN GSR EXAMINATIONS

Nilgün Şen[1]
Forensic Science Institute of Turkey, Instanbul
Taner Bora[2]
Ankara Criminal Police Laboratory
Çağdaş Aksoy[3]
Diyarbakır Criminal Police Laboratory
Fırat Aydın
Dicle University, Faculty of Science, Diyarbakır

Abstract: Transferring of gunshot residue (GSR) from fabrics via adhesive types is a rapid, easy, cheap, and effective method. However, false positives due to the presence of antimony in the seat fabrics swabs cause some problems in GSR examinations, especially with graphite furnaced atomic absorption (GFAAS) spectrometry. In this study, we aimed to determine the reason of false positives by examining the adhesive tape swabs taken from 100 seats of fifty different automobiles. Examinations are carried out by GFAAS. Types of the seat fabrics were determined by Fourier transform infrared (FTIR) spectroscopy. Results of GFAAS and FTIR examinations indicated that the entire seat covers containing antimony were of polyester. Examination via FTIR before elemental analysis is proposed as a new method to prevent false positives caused by antimony.

Keywords: GSR, Antimony, GFAAS, ATR-FTIR, Seat covers.

INTRODUCTION

GSR evidence is one of the most common and most heavily scrutinized sources of trace evidence examined in violent crime investigations [1]. GSR are composed of unburned and partially burnt propellant powder, particles from the ammunition primer, smoke, grease, lubricants, and metals from the cartridge as well as the weapon itself. Organic compounds mainly originate from propellant and firearm lubricants, taking the form of unburned and partially burned gunpowder particles, some products of their transformation, and hydrocarbons . Inorganic residues such as nitrates, nitrites, and metallic particles originate from the primer and propellant as well as the cartridge case, the projectile jacket or its core and from the weapon barrel itself [2]. The explosion of a cartridge produces a heterogeneous population of GSR particles that contain different chemicals. Many of them contain elements found in the primer mixture that eventually recombine with other metals from the cartridge case and from the barrel [3].Lead (Pb), barium (Ba), and antimony (Sb), possibly with one or more of the following elements: aluminum, silicon, phosphorus, sulphur (trace), chlorine, potassium, calcium, iron (trace), nickel, copper, zinc, zirconium, and tin are admitted as characteristic GSR elements [4].

In real cases, typically only a few particles of interest are found on the hands of living suspects and with some cartridges SEM- EDS can be unsatisfactory, failing to distinguish between an environmental particle and a particle produced by a gunshot [5].The Scanning Electron Microscope equipped with an Energy Dispersive X-ray Spectrometer (SEM-EDS) is currently considered in court to be the most powerful tool to analyse inorganic GSR particles [6].The analytical approach based on SEM-EDS gained widespread success in the field, mainly because when the technique was introduced in the seventies in Europe and the USA, the majority of cartridges on the market had primer mixtures containing lead styphnate, barium nitrate and antimony sulphide [7].

Detection and identification of primer residues are of paramount importance in the forensic setting. These investigations can be performed by several methods which involve atomic absorption spectroscopy (AAS) either with flame (FAAS) or electrothermal atomic absorption spectrometry (ETAAS), neutron ac-

1 nilgunsen2001@yahoo.com
2 Director of Ankara Criminal Police Laboratory.
3 Police Chief of Chemical Section.

tivation analysis (NAA), scanning electron microscopy/energy dispersive X-ray (SEM/EDX) spectroscopy, component analysis employing Xray fluorescence (XRF), proton induced X-ray emission technique (PIXE) which are methods for GSRs detection and identification on suspects of shooting, on clothing items, and on objects [8–9].

The adhesive tape method which is currently used as GSR sampling method in Turkey provides a rapid, easy, cheap, and effective way to collect GSR from surfaces and is widely used by crime scene investigators [10-11-12-13]. Because of low persistence of GSR on the hands, in some cases sampling of the suspect's clothes, goods or vehicles is needed. Vehicle seat cover provides a useful area to collect long lived GSR. After all analyzes of clothes and fabric surfaces via SEM/EDX usually needs carbon/gold coating which significantly increases the analyze time [14]. Thus determination of GSR elements, Sb, Pb, and Ba with GFAAS is rapid, easy, and cheap way for clothes and goods. However, the analysis of GSR with GFAAS does not take into account the morphology of individual particles and therefore the possibility of false positive results is much greater. In order to prevent false positives, identification of their sources is a crucial issue.

Main goal of this study is determining an average ratio of false positives on seat covers and what cause these false positives. For that reason 100 seat cover samples analyzed and their raw materials were determined via FTIR which is a very useful method for defining materials and their chemical structures. FTIR examinations also do not damage the chemical structure of the analyzed material, produce results quickly and cheap.

EXPERIMENTAL

A PerkinElmer® AAnalyst™ 600 atomic absorption spectrometer, equipped with Zeeman background corrector, graphite furnace with THGA™ pyrolytically coated graphite tubes, and a PerkinElmer AS-800 autosampler, were used (PerkinElmer, Inc., Shelton, CT, USA). The operating conditions and analytical parameters are optimized before [15], are listed in Table I.

Table 1 *Instrumental Operating Conditions for Antimony Analysis*

Lamp: Perkin Elmer Lumina Sb
Wavelength: 217.6 nm
Slit: 0.5 nm
Dispensed sample volume: 20µl

Step	Temperature (°C)	Ramp Time (s)	Hold Time (s)
1	110	1	20
2	130	15	20
3	1000	10	15
4	2100	0	5
5	2450	1	3

Total program time: 90 s

A Thermo® Nicolet 6700 model FTIR (USA) with diamond ATR (Attenuated total reflection) kit (Smart Orbit, USA) was used to identify the raw materials of the fabrics.

Sb standard solution of 1.000 mg L−1 for AAS was purchased from E. Merck (Darmstadt, Germany). Distilled water was produced with a NS-104 system (Nüve Co., Turkey). Working standard solutions of 5, 10, 20, 30, and 40 µg L−1 Sb in 1% nitric acid were prepared by dilution of the 1000 mg L-1 Sb standard. Nitric acid (65%, Merck) was of analytical purity.

Medical fabric adhesive tapes (Seyitler Kimya Co., Turkey) were used for sampling because of their good recovery results [15]. Each adhesive tape was cut into 25 cm2 parts in order to simulate samples normally submitted by crime scene investigators. A hundred adhesive tape swabs were collected from fifty different vehicles of ten different companies which correspond to more than eighty percent of total automobile sales in Turkey. Sampled vehicles, cleaned with a vacuum-cleaner, were selected randomly from three different regions of Turkey, Ankara, Antalya and Diyarbakir. The polystyrene sample boxes were of 2.5 cm bottom diameter and 4 cm height (LP Italiana Spa, Italy).

A 9 mm Beretta FS92 pistol (Italy) with MKE 9x19 mm parabellum cartridges (Turkey) was used to simulate a firing in the vehicle.

The analytical method still used as one of the GSR detection methods in Turkish Police Forensic Laboratories was the quantitative elemental detection of antimony via GFAAS [16]. The samples were put into boxes and shaken for 45 minutes with 4 mL 8% nitric acid (v/v).

Fabric samples were directly analyzed with ATR-FTIR to determine the raw material used. Swabs from the surface of vehicle seats were taken a day after firing.

RESULTS AND DISCUSSION

The confidence parameters were based on the relative standard deviation (%RSD), limit of detection (LOD), and limit of quantitation (LOQ) values obtained by GFAAS from the calibration curves shown in Table II.

Table 2

Confidence Parameters Based on the Calibration Curve

S (Standard deviation)	0.0004 (for 10 μg L^{-1}, 15 samples)
m (slope)	0.0013
n (slide)	0.0029
Linear range	5-40 μg L^{-1}
R^2	0.9982
LOD	0.92 μg L^{-1}
LOQ	3.08 μg L^{-1}

In the five samples numbered 7 (left-right), 26 (left-right), and 30 (left), the mean antimony concentrations were 93.6, 143.7, 71.4, 137.4, and 65.6 μg L-1, respectively, so samples were four times diluted before analyze. The mean antimony concentrations of 23 samples from 12 different vehicles were higher than 5.0 μg L-1 and high enough to cause false positives. All positive results are listed in Table III.

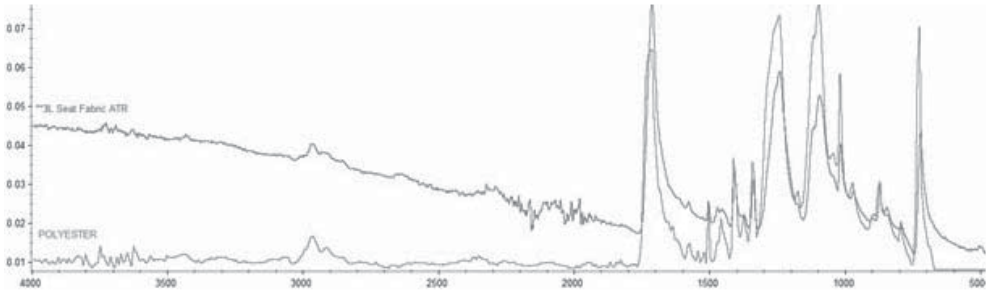
Table 3

GFAAS Analyze Results of Seat Swabs Detected Antimony*

Vehicle Code	City	Seat Major Raw Material	Mean Sb Conc. (μg L^{-1})	
			Left Seat	Right Seat
3	Ankara	Polyester	13.4	5.7
4	Ankara	Polyester	11.5	11.1
5	Ankara	Polyester	19.0	6.4
7	Ankara	Polyester	93.6	148.7
16	Antalya	Polyester	5.0	16.8
21	Antalya	Polyester	15.7	13.3
25	Antalya	Polyester	10.7	<LOQ
26	Antalya	Polyester	71.3	137.3
27	Antalya	Polyester	6.5	17.4
30	Antalya	Polyester	65.6	21.9
47	Diyarbakir	Polyester	6.0	10.3
48	Diyarbakir	Polyester	9.8	16.2

* Only samples that contain antimony (12 vehicles) are shown. Sample concentrations below LOQ (38 vehicles) are not shown.

All fabric samples were examined via ATR-FTIR. According to FTIR spectrums, three major raw materials, leather, nylon, and polyester, were determined in the fabrics. The spectrum of a fiber sample identified as polyester is shown in the next figure.



ATR-FTIR spectrum of a seat fabric and polyester identification.

In our study, antimony was not detected in the leather and nylon seat swabs via GFAAS. Antimony was detected only in some polyester seat fabric swabs. Moreover repeated GFAAS examinations of the same polyester seat fabric showed similar results.

It was known that antimony compounds are used as catalyst in polyester fiber production. Mean antimony content in commercial polyester fibers is in the range of 200 to 300 ppm [17]. In connection with this information, it was assumed that antimony was within the structure of the polyester fibers.

Swabs taken from the vehicle seats of three different raw materials after single shooting were analyzed to establish the efficiency of the swabbing method and make a comparison of swabs among seat types. The antimony concentrations in the leather seat swabs were found higher than the others. The mean concentrations of antimony depending on the seat material type are listed in Table IV.

Table 4

Comparison of determined Sb concentrations with seat material

Vehicle	Raw material included in the seat fabric	Mean Sb Concentrations ($\mu g\ L^{-1}$) (n=3)	
		Before shooting	After shooting
2	Leather	< LOQ	85.5
4	Polyester	11.5	55.9
18	Nylon	< LOQ	47.9

CONCLUSION

The identification of gunshot residue optimally requires a combination of visualizing the morphological features along with identification of the chemical components by SEM/EDX. But collecting samples from clothing or fabrics using tape lifts may also create problems with fibers and other debris. This detritus is likely to be nonconductive and may hold charge during SEM analysis. Carbon-gold coating of the sample may therefore be required which involves extra time and expense [14-19].To prevent these expense and time consumption, detection of unique GSR elements, Sb, Pb and Ba, via non-visualizing techniques like GFAAS are used. However, the effectiveness of AAS in term of GSR analysis was further brought into question by Ivanović [18], who criticized the method on the basis of the large number of false results it has been shown to produce (about 40%).

In this study, for the first time in Turkey a detailed sampling of vehicle seats and their GFAAS analyses were made to determine the reason of false positives encountered in GSR determination. Antimony was detected in twenty-three percent of all examined vehicle seats. Polyester was the common trait of these seat's raw materials. Higher antimony concentrations were detected for more sheddable fabrics. Because antimony was present only in polyester fibers and comparable results were obtained in each analysis, it was assumed that antimony was within the structure of polyester fibers.

As a result, it was seen that GSR determination via GFAAS isn't a suitable method on polyester fabrics and antimony contamination is likely. In addition, this study confirms the strength of SEM/EDX in the analysis and characterization of gunshot residue on polyester fabrics.

Identification of raw material used in fabric by FTIR before GFAAS analysis is proposed to prevent antimony contamination. Fabrics' FTIR analysis with ATR is fast and cheap. In case of determination of polyester fiber, examination by SEM/EDX is crucial to determine GSR in real cases.

ACKNOWLEDGMENTS

The authors are grateful to Turgay Tekinay (Gazi University, Research Laboratory, Turkey).

REFERENCES

1. A. J. Schwoeble, D. L. Exline. "Current Methods in Forensic Gunshot Residue Analysis". New York : CRC Press LLC, 2000.
2. O. Dalby, D. Butler, J.W. Birkett. "Analysis of gunshot residue and associated materials"—a review, J. Forensic Sci, 55 (2010) 924–943.
3. S. Charles, B. Nys, N. Geusens. "Primer composition and memory effect of weapons – some trends from a systematic approach in casework",Forensic Sci. Int, 212 (2011) 22–26.
4. J.W.Warmenhoven. "A New Procedure in the Forensic Analysis of Gunshot Residue Using Integrated Ion Beam Analysis in Conjunction with Multivariate Canonical Discriminant Function Analysis" University of Surrey, U.K., Thesis (2013) 2-20.
5. F.S. Romolo, M.E. Christopher, M. Donghi, L. Ripani, C. Jeynes, R.P. Webb, N.I. Ward, K.J. Kirkby, M.J. Bailey. "Integrated Ion Beam Analysis (IBA) in Gunshot Residue (GSR) characterization" , Forensic Science International, 231 (2013) 219–228.
6. American Society for Testing and Materials. "Standard guide for gunshot residue analysis by scanning electron microscopy/energy dispersive X-ray spectroscopy" in: Annual Book of ASTM Standards, ASTM, International, West Conshohocken, PA, USA, 2010, E 1588-10.
7. J.I. Thornton, "The chemistry of death by gunshot", Anal. Chim. Acta, 288 (1994) 71–81.
8. S.S. Krishnan, "Firing distance determination by atomic absorption spectrophotometry", J. Forensic Sci,19 (1974) 351–356.
9. A. Zeichner, "Recent developments in methods of chemical analysis in investigations of firearm-related events", Anal. Bioanal. Chem,. 376 (2003) 1178–1191.
10. R.L. Singer, D. Davis, and M.M. Houck. "A survey of gunshot residue analysis methods", J. Forensic Sci, 41(2) (1996)195-8.
11. M. Tassa, N. Adan, N. Zeldes, and Y. Leist. "A field kit for sampling gunshot residue particles", J. Forensic Sci., 27 (1982) 671-676.
12. H.A. Wrobel, J.J. Millar, M. Kijek. "Comparison of properties of adhesive tapes, tabs, and liquids used for the collection of gunshot residue and other trace materials for SEM analysis", J Forensic Sci, 43(1) (1998)178– 81.
13. D.K. Shaffer, K. Yi. "A comparison of particle transfer efficiencies of two collection methods for the identification of gunshot residue on fabric surfaces using scanning electron microscopy-energy Dispersive spectrometry" ,Scanning Conference, 21 (2) (1999) 99–100.
14. V. Mastruko. "Detection of GSR particles on clothing of suspects, in: Proceedings of the 3rd European Academy of Forensic Science Meeting" , Forensic Sci. Int., 136 (2003) 153–154.
15. Ç. Aksoy, Z.O. Ergün, Y. Akman, U. Üzek, F. Aydin. "Determination of Antimony in GSR Using GFAAS and SEM/EDX, At. Spectrosc." 34(5) (2013) 170-174.
16. Report.Method validation of antimony determination by atomic absorption spectrometry in gunshot residue, Ankara Police Forensic Laboratory (2007) KPL-GP-021.
17. K. Lacasse, W. Baumann. "Textile Chemicals". Dortmund: Springer Science & Business Media (2004).
18. A. Ivanović. "Is There a Way to Precisely Identify That the Suspect Fired from the Firearm. Proceedings of the Third European Academy of Forensic Science Meeting, Istanbul, Turkey. Forensic Science International Special Issues, September 22-27, (136) (2003) 158-159.
19. F.S. Romolo , M.E. Christopher, M. Donghi, L. Ripani, C. Jeynes, R.P. Webb, N.I. Ward , K.J. Kirkby, M.J. Bailey . " Integrated Ion Beam Analysis (IBA) in Gunshot Residue (GSR) characterization", Forensic Science International, 231 (2013) 219–228.

UDC: 343.982.3:641

RECENT DEVELOPMENTS AND APPLICATIONS OF ENZYME-LINKED IMMUNOSORBENT ASSAYS IN FORENSIC FOOD ANALYSIS

Bojana Vidovic[1]
University of Belgrade, Faculty of Pharmacy
Nikola Milasinovic[2]
The Academy of Criminalistic and Police Studies, Belgrade

Abstract: The development of efficient, sensitive and cost/effective techniques for forensic food analyses is of great importance to ensure safety, quality, and traceability of foods in compliance with the legislation and consumers' demands. In recent years, advances in enzyme-linked immunosorbent assays (ELISA) technology have led to rapid development of different commercial immunoassays kits used in the food analysis. The simplicity of the test and the short time required for the analyses make the ELISA methods suitable for food screening tests of a large number of samples. However, there are few disadvantages of the ELISA technique that will be discussed in this paper, as well. The present paper focuses on recent developments and applications of the ELISA in determining food ingredients and food contaminants such as residues of pesticides, toxins, veterinary medicine residues, allergens and other contaminants in food derived from food processing and storage.

Keywords: ELISA, Antibodies, Food Forensics, Immunoassay.

INTRODUCTION

With a growing interest in healthy eating, the food industry sets a global requirement for the production of the nutritious, safe, environmentally sustainable, and affordable foods. In addition, macro- and micronutrients and non-nutritive components of the food, responsible for its organoleptic characteristics, nutritive and biological values and many other substances that are more or less harmful to health can be found in foods. This primarily includes microorganisms and their toxins, additives (i.e. colorants, flavourings, and preservatives), contaminants (i.e. dioxin, polychlorinated biphenyls, melamine, and phthalates) and veterinary medicine residues (i.e. hormones, antibiotics). Detection of these substances and their determination present the basis of the food safety control.[3] Additionally, with the greater awareness of food safety and quality, consumers increasingly demand reassurance regarding the origin and content of the foods, while manufacturers need to be able to confirm the authenticity of components of their products and comply with government legislation.[4]

Immunochemical assays are powerful bioanalytical techniques with application to several areas in food forensic analysis, including microbiology, safety, quality, authenticity, as well as food process control. Immunochemical techniques require little or no sample pre-treatment, making these analytical procedures relatively rapid. Due to its relative low cost, immunoanalytical assays provide attractive tools for the food analyst who requires either inexpensive qualitative screening tests or reliable quantitative methods with a high degree of sensitivity.[5]

This paper examines some methodological issues associated with the wide use of enzyme-linked immunosorbent assay in forensic food analysis.

1 bojana@pharmacy.bg.ac.rs
2 nikola.milasinovic@kpa.edu.rs
3 *Mirić,* M., *Šobajić,* S., *Zdravstvena ispravnost namirnica*, Zavod za izdavanje udžbenika, Beograd, 2002.
4 Sun, D.-W., (Ed), Modern Techniques for Food Authentication, Academic Press / Elsevier, San Diego, California, USA, 720 pp., 2009, ISBN: 978-0-12-374085-4.
5 Gazzaz, S.S., Rasco, B.A., Dong, F.M., Application of immunochemical assays to food analysis. Critical Reviews in Food Science and Nutrition, 32(3):197-229, 1992.

ENZYME-LINKED IMMUNOSORBENT ASSAY

Enzyme-linked immunosorbent assay (ELISA) represents one of the most widely used immunochemical techniques that involve an enzyme to detect the presence of an antibody or an antigen in a sample. An antigen is any molecule that induces the formation of antibodies. To stimulate the immune system for generation of specific antibodies the antigen should have a molecular weight of at least 3000-5000 daltons. The development of specific antibodies for low-molecular weight compounds (<1000 daltons) can be obtained through the use of a larger carrier immunogenic molecule such as albumin proteins from a different species.[6] The linked form of the small molecule is known as *hapten*. Antibodies are glycoproteins, also known as immunoglobulins (Ig) produced by animals in response to protein antigens or haptens. These proteins bind the particular antigen responsible for their induction. The specific region on an antigen that an antibody recognizes and binds to is called the *epitope*, or antigenic determinant. An epitope is usually 5-8 amino acids long on the surface of the protein. The reversible binding between an antigen and an antibody is mostly due to non-covalent bonding and includes: hydrogen bonds, electrostatic, hydrophobic and van der Waals interactions. Antibodies used in analytical methods can be obtained directly from an animal immunized with the antigen of interest. The immune response to an antigen generally involves the activation of multiple B-cells all of which target a specific epitope on that antigen. As a result numerous antibodies are produced with different specificities and epitope affinities these are known as *polyclonal antibodies*. Polyclonal antibodies are preferred for the detection of denatured proteins because they offer broad recognition of different epitopes and more tolerance to small changes, such as denaturation and polymerization of antigens.[7] However, assay performance can often be improved by the preparation of *monoclonal antibodies* that exhibit greater specificity for the target antigen, due to their binding for only a single epitope.[8]

There are different formats of ELISA. The solid support is typically a 96-well plate or a polystyrene strip of 8-12 wells, but other materials such as polyvinylidene difluoride or nitrocellulose membrane can serve this function. Two antibodies are involved in ELISA. The primary antibody, usually produced in rabbits or mice, binds specifically with the antigen and determines specificity of the assays. A secondary antibody is enzyme-labelled goat anti-rabbit or goat anti-mouse immunoglobulin G (IgG), depending on the origin of the primary antibody. An enzyme-linked secondary antibody that reacts with a chromogen is added, producing a colour change to detect the antigen.[9]

The most common enzyme used as labels for ELISAs are horseradish peroxidase (HRP), calf intestine alkaline phosphatase, and *E. coli* β-galactosidase. These enzymes meet most, if not all, of the criteria necessary to produce a sensitive, inexpensive, and easily performed assay. These criteria include stability at typical assay temperatures (4°C, 25°C, and 37°C), greater than six months shelf life when stored at 4°C, commercially available, capable of being conjugated to an antigen or antibody, inexpensive, easily measurable activity, high substrate turnover number, and unaffected by biological components of the assay.[10]

A standard ELISA protocols involve the stepwise addition and reaction of reagents to a solid phase-bound substance, through incubation and separation of bound and free reagents using washing steps. An enzymatic reaction is utilized to yield colour and to quantify the reaction, through the use of an enzyme-labelled reactant.[11] These can be summarized as follows:

1) Adsorption of the antigen or antibody to the plastic solid phase;
2) Addition of the test sample and subsequent reagents;
3) Incubation of reactants;
4) Separation of bound and free reactants by washing;
5) Addition of enzyme-labelled reagent;
6) Addition of enzyme detection system (colour development), and
7) Visual or spectrophotometric reading of the assay.

6 Bonwick, G.A., Smith, C.J., Immunoassays: their history, development and current place in food science and technology. International Journal of Food Science & Technology, 39:817-827, 2004.
7 Asensio, L., González, I., García, T., Martín, R., Determination of food authenticity by enzyme-linked immunosorbent assay (ELISA). Food Control, 19:1-8, 2008.
8 Hsieh, Y-H.P., Immunoassays. Ch. 17. In: Nielsen, S.S. (Ed) Food analysis, 4th edn. Springer, New York, 2010.
9 Chen, J., Contemporary monitoring methods. In: Schmidt, R.H., Rodrick, G.E. (Eds.), Food safety handbook (chapter 11). Hoboken, NJ: John Wiley & Sons, Inc. 2003.
10 Rakshit, S.K., Diagnostic enzymes. In: Pandey, A., Webb, C., Coccol, C.R., Larroche, C. (Eds), Enzyme Technology; New York: Springer, pp.685-696. 2006.
11 Crowther, J.R., *The ELISA Guidebook*. 2nd edition. New York: Humana Press, 2009.

TYPES OF ELISA

ELISAs can be performed in many different formats (direct, indirect, capture, competitive, etc.) The two most common forms of ELISA used for food analysis are the indirect and the sandwich ELISA (Figure 1). In the indirect ELISA two antibodies are used: one binds to a specific antigen and the other couples to an enzyme that converts a substrate into a coloured product. The amount of colour produced is proportional to the amount of secondary antibody that was bound. A disadvantage of the indirect ELISA is that cross-reactivity occurs with the secondary antibody, resulting in strong non-specific signals. On the positive side, sensitivity is increased because each primary antibody contains several epitopes that can be bound by the labelled secondary antibody, allowing signal amplification.[12]

However, if antigen is present at low levels or does not adhere well to the plastic, than the sandwich ELISA may be used. This type of assay is named since the antigen is bound between two antibodies: the capture antibody and the detection antibody. The detection antibody can be coupled to an enzyme or can bind the conjugate (enzyme/linked antibody) that will produce the biochemical reaction.[13] Major advantages of this technique are that the antigen does not need to be purified prior to use, due to its high specificity. A disadvantage is that not all antibodies can be used.

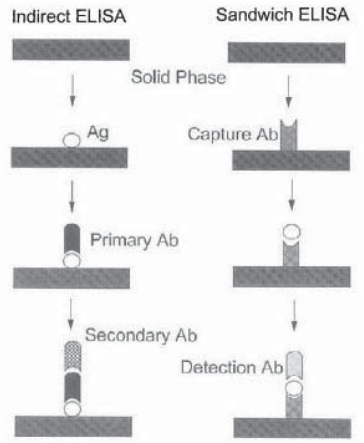


Figure 1 *Principles of ELISA (adapted from Chen, 2003)*[14]

This assay format can be further divided into competitive or non-competitive, depending on whether capture antibody has to compete for the antigen with antibodies added to the sample extract. In a non-competitive assay, the concentration of the analyte is directly proportional to the intensity of the developed colour. In the case of a competitive assay, the colour development is inversely proportional to the concentration of the analyte.

ELISA tests can be obtained either in qualitative or quantitative formats. While qualitative ELISA provides either positive or negative results, the quantitative ELISA determines antigen concentration by interpolating optical or fluorescence intensity into a standard curve generated by a serial dilution of targets.[15]

COMMERCIAL ELISA

In the last years, ELISA system has become more popular assay that can be used as a rapid test for screening large number of routine samples. Many commercialized immunochemical diagnostic kits from different companies are available. A commercial ELISA may contain some or all of the following components: coated plates (solid and/or strip plates), sample diluents, controls, wash concentrate, conjugate, substrate and stop solution.[16]

12 De La Guardia, M., Gonzalez Illueca, A., Food Protected Designation of Origin: Methodologies and Applications. Comprehensive Analytical Chemistry, 60:2-773, 2013.
13 Goldsby, R.A., Kindt, T.K., Osborne, B.A., Kuby, J., Immunology, 5th Edition, W.H. Freeman and Company, New York, New York, 2003.
14 Chen, J., Contemporary monitoring methods. In: Schmidt, R.H., Rodrick, G.E. (Eds.), Food safety handbook (chapter 11). Hoboken, NJ: John Wiley & Sons, Inc. 2003.
15 Goldsby, R.A., Kindt, T.K., Osborne, B.A., Kuby, J., Immunology, 5th Edition, W.H. Freeman and Company, New York, New York, 2003.
16 ELISA Technical Guide-Idexx, available at: https://www.idexx.com/pdf/en_us/livestock-poultry/elisa-technical-guide.pdf

Immunosorbent (coated plates)

There are three shapes of ELISA carrier: microtiter plate, small ball and small tube. Microplate which is 96 wells plate is generally used. The function of the solid phase is to immobilize either antigens or antibodies in the sample, as they bind to the solid phase. The good ELISA plate is strong adsorbing, low-value blank and high-transparency in the bottom of well.

Sample Diluent

Most assays require a specific dilution of the sample. Samples are added to the sample diluent and mixed prior to putting them onto the coated plates.

Controls

The positive control is a solution that contains antibody or antigen. The negative control is a solution without antibody or antigen. The controls help to normalize or standardize each plate. Controls are also used to validate the assay and to calculate sample results. In most tests, the controls are prediluted and ready to use.

Conjugate

Conjugate are enzyme-labelled antibodies or antigens that react specifically to plate-bound sample analytes. They present the key substance in ELISA. Unbound conjugate can be washed away after incubation and before the addition of substrate. The optical density of the colorimetric substrate is directly proportional to the quantity of bound.

Substrate

For peroxidase conjugates, the substrate is a mixture of hydrogen peroxide and a chromogen that reacts with the enzyme portion of the conjugate to produce color.

Wash concentrate

The wash concentrate is a buffered solution containing detergent used to wash away unbound materials from the plates.

Stop solution

The stop solution stops the enzyme-substrate reaction and, thereby, the colour development. Sulfuric acid is widely used as stop solution for peroxidase reaction.

RECENT APPLICATIONS OF ELISA IN FOOD FORENSICS

Various ELISA test kits, in different formats, have been developed for many pesticides. These methods are frequently used in semi-quantitative screening analysis.[17] The determination of several herbicides in food, such as organophosphorous pesticides[18] and polychlorinated biphenyls[19] by ELISA has been reported.

The residues of veterinary drugs or their metabolites in meat and other foods of animal origin may cause adverse toxic effects on consumers' health. Today, there are many different types of ELISA kits commercially available for a large number of drugs like stilbenes, β-agonist, antithyroid agents, steroids, as well as antibiotic residues.[20]

17 Nollet, L.M.L., (Ed), Handbook of food analysis (2nd edition). v3: Methods and instruments in applied food analysis. New York: Marcel Dekker, 2004.
18 Cho, Y.A., Lee, V., Park, E.Y., Lee, Y.T., Bruce, D.H., Chang, A.K., Jae, K.L., Development of an ELISA for the Organophosphorus Insecticide Chlorpyrifos. Bulletin of the Korean Chemical Society, 23:481-487, 2002.
19 Tsutsumi, T., Amakura, Y., Okuyama, A., Tanioka, Y., Sakata, K., Sasaki, K., Maitani, T., Application of an ELISA for PCB 118 to the screening of dioxin-like PCBs in retail fish. Chemosphere, 65(3):467-73, 2006.
20 Shankar, B.P., Manjunatha Prabhu, B.H., Chandan, S., Ranjith, D., Shivakumar, V., Rapid Methods for detection of Veterinary Drug residues in Meat. Veterinary World, 3(5):241-246, 2010.

The ELISA technique is widely used to detect and quantitate various foodborne pathogens by targeting their surface structures, toxins, or whole cells. Many diagnostic companies have marketed ELISA test kits for foodborne pathogens and toxins such as *Salmonella*, *Escherichia coli*, staphylococcal enterotoxins, and so on.[21] Sensitive microtiter plate ELISA formats are commercially available for a variety of mycotoxins including aflatoxins BG, aflatoxin M1, ochratoxin A, the fumonisins, zearalenone, deoxynivalenol, citrinin, and T-2 toxin.[22] Commercially available ELISA is usually designed as sandwich assay. ELISA for pathogens have detection limits ranging from 10^3-10^5 colony-forming units per mL (cfu mL^{-1}) for whole bacterial cells and few ng mL^{-1} for toxins/protein. Therefore, direct detection of pathogens in food is not possible and enrichment is required for at least 16-24 h.[23] Even though they often lack accuracy at very low concentrations and are limited in the range of matrices examined, ELISAs provide fast, inexpensive screening assays. However, matrix interference or the presence of structurally related mycotoxins can interfere with the binding of conjugate and antibody, leading to mistakes in quantitative measurements of mycotoxins. Therefore, ELISA kits should be used routinely only for the analysis of matrices that are extensively tested. Confirmatory analyses by more robust methods, as HPLC or LC-MS, are required for the contamination levels that approach the legal limit.[24]

ELISA is the method choice for the detection of the allergens, due to the high sensitivity, specificity, stability, and possibility for use for the semi-quantitative determination of allergens in food.[25] Commercially available ELISA kits are targeted toward almond, crustaceans, egg, hazelnut, milk, peanut, soy, sesame, mustard, buckwheat, wheat, and lupin, are used by food industries for screening purposes.[26] ELISA methods have been used to certify gluten-free products because of their specificity and sensitivity. Valdez and Mendez[27] developed a highly sensitive and specific sandwich ELISA to quantify low levels of wheat (gliadins), barley (hordeins) and rye (secalins) prolamins, which have been seen as the celiac-active components of gluten, in foods for coeliacs. This method is currently recommended by Codex Alimentarius Commission standard, and is practically the only method used for the quantification of hydrolyzed gluten.

In addition, some manufacturers have developed rapid ELISA screening tests for the detection of genetically modified organisms in raw agricultural or slightly processed food products.[28] These test kits have limitations when applied to highly processed food, because of their heterogeneity and the high degradation levels of many ingredient. In these cases, PCR-based methods are recommended.[29]

A variety of analytical methods, different in their complexity and cost, are potentially available for authentication purposes of many products, such as meat, milk, fish, etc.[30],[31] Legislative authority establishes that these products must be accurately labelled regarding species content. Correct species identification is important for the consumer for several reasons related to possible economic losses from fraudulent substitution or adulteration, intolerance or allergy, and religious, ethical or cultural objections.[32] In this regard, different ELISAs have been used in the past few years for identifying meats of different animal species using antibodies against muscular and serum animal proteins or thermostable proteins.[33],[34] The ELISAs are also applied in the determination of vegetable proteins such as soybean protein concentrates and isolates as cheaper source of high quality proteins or functional ingredients in the meat industry.[35],[36] To avoid the possible fraudulent substitution of the goat and sheep milk with cow's milk, immunochemical diagnostic

21 Fung, D.Y.C., Rapid Methods and Automation in Microbiology. Comprehensive Reviews in Food Science and Food Safety, 1:3-22, 2002.
22 Pittet, A., Modern methods and trends in mycotoxin analysis. Mitteilungen aus Lebensmitteluntersuchung und Hygiene, 96:424-444, 2005.
23 Mandal, P.K., Biswas, A.K., Choi, K., Pal, U.K., Methods for Rapid Detection of Foodborne Pathogens: An Overview. American Journal of Food Technology, 6:87-102, 2011.
24 Pascale, M., Visconti, A. Overview of detection methods for mycotoxins. In: Leslie, J.F., Bandyopadhyay, R., Visconti, A. (Eds.), Mycotoxins-Detection Methods, Management, Public Health and Agricultural. CAB International, UK, pp. 171-183, 2008.
25 van Hengel, A.J., Food allergen detection methods and the challenge to protect food-allergic consumers. Analytical and Bioanalytical Chemistry, 389(1):111-118, 2007.
26 Schubert-Ullrich, P., Rudolf, J., Ansari, P., Galler, B., Führer, M., Molinelli, A., Baumgartner, S., Commercialized rapid immunoanalytical tests for determination of allergenic food proteins: an overview. Analytical and Bioanalytical Chemistry, 395(1):69-81, 2009.
27 Valdes, I., Garcia, E., Llorente, M., Mendez, E., Innovative approach to low-level gluten determination in foods using a novel sandwich enzyme-linked immunosorbent assay protocol. European Journal of Gastroenterology & Hepatology, 15:465-474, 2003.
28 Ahmed, F.E., Detection of genetically modified organisms in foods. Trends in Biotechnology, 20:215-223, 2002.
29 Sun, D.-W., (Ed), Modern Techniques for Food Authentication, Academic Press / Elsevier, San Diego, California, USA, 720 pp., 2009, ISBN: 978-0-12-374085-4.
30 Ibid.
31 De La Fuente, M.A., Juárez, M., Authenticity assessment of dairy products. Critical Reviews in Food Science and Nutrition 45:563-585, 2005.
32 Sun, D.-W., (Ed), Modern Techniques for Food Authentication, Academic Press / Elsevier, San Diego, California, USA, 720 pp., 2009, ISBN: 978-0-12-374085-4.
33 Ayaz, Y., Ayaz, N.D., Erol, I., Detection of species in meat and meat products using enzyme-linked immunosorbent assay. Journal of Muscle Foods, 17:214-220, 2006.
34 Liu, L., Chen, F.-C., Dorsey, J., Hsieh, Y.-H.P., Sensitive monoclonal antibodybased sandwich ELISA for the detection of porcine skeletal muscle in meat and feed products. Journal of Food Science, 71(1):M1-M6, 2006.
35 Macedo-Silva, A., Shimokomaki, M., Vaz, A.J., Yamamoto, Y.Y., Tenuta-Filho, A., Textured soy protein quantification in commercial hamburger. Journal of Food Composition and Analysis, 14:469-478, 2001.
36 Brandon, D.L., Frieman, M., Immunoassays to soy proteins. Journal of Agriculture and Food Chemistry, 50: 6635-6642, 2002.

kits for rapid detection and quantifications of whey proteins, caseins or short-string peptides from milk proteins are commercially available.[37]

Characteristics of some commercially available ELISA tests

Analyte	Kit name & Company	Primary matrices	Incubation time	Limit of detection
2,4-dichlorophe-no-xyacetic acid	2,4-D ELISA Kit, Abraxis LLC Warminster, USA	Water	90 min	-
Organochlorine insecticides	**Organochlorine Screen (ELISA Kit)** EnviroLogix Inc, Portland, USA	Dried vine and tree fruit	130 min	0.05 ppm (DDT)
Ethinylestradiol	RIDASCREEN® Ethinylöstradiol R-Biopharm AG, Darmstadt, Germany	Urine (bovine/porcine), muscle meat (beef/pork) and bovine plasma	150 min	Bovine urine: approx. 370 ppt Porcine urine: approx. 370 ppt Beef: approx. 230 ppt Pork: approx. 200 ppt Bovine plasma: approx. 50 ppt
Tetracyclines	SuperScreen Tetra HS **Tecna s.r.l.**, Trieste, Italy	Honey, Milk, Tissue and Meat drip, Egg, Poultry meat and liver, Seafood.	90 min	Tissues, raw milk, honey, eggs, seafood: 50 ppb
Salmonella	MaxSignal® Salmonella ELISA Test Kit Bioo Scientific Corporation, Austin, USA	Different food products	75 min	$10\times e^5$ cells mL^{-1}
Aflatoxin M1	RIDASCREEN® Aflatoxin M1 R-Biopharm AG, Darmstadt, Germany	Milk, milk powder and cheese.	75 min	Milk: 5 ppt Milk powder (referring to reconstituted milk): 5 ppt Milk powder (referring to g-weight): 50 ppt Cheese: 50 ppt
Prolamins from wheat (gliadin), rye (secalin), and barley (hordein)	RIDASCREEN® Gliadin R-Biopharm AG, Darmstadt, Germany	Raw products like flours (buckwheat, rice, corn, oats, teff) and spices as well as in processed food like noodles, ready-to-serve meals, bakery products, sausages, beverages and ice cream	90 min	1.5 ppm gliadin, corresponding to 3 ppm gluten
Milk proteins	Milk ELISA, Immunolab Kassel, Germany	Different foods product	60 min	0.05 ppm
Soy proteins	I'Screen SOYA **Tecna s.r.l.**, Trieste, Italy	Different foods product	105 min	0.4 ppm
Monsanto's CP4 EPSPS proteins	AgraQuant® RUR Soya Grain Plate Romer Labs, Inc., USA	Soybeans	130 min	Ground bean: 0.14% De-fatted flour: 0.13% Protein isolates: 0.10

As an alternative tests to ELISA, a much faster and simplified qualitative lateral flow dipsticks tests, suitable for a large number of food samples screening, were developed (Figure 2).[38],[39]

37 Zachar, P., Šoltés, M., Kasarda, R., Novotny, J., Novikmecová, M., Marcinčáková, D., Analytical methods for the species identification of milk and milk products. Mljekarstvo, 61(3):199-207, 2011.
38 Bonwick, G.A., Smith, C.J., Immunoassays: their history, development and current place in food science and technology. International Journal of Food Science & Technology, 39:817-827, 2004.
39 Asensio, L., González, I., García, T., Martín, R., Determination of food authenticity by enzyme-linked immunosorbent assay (ELISA). Food Control, 19:1-8, 2008.

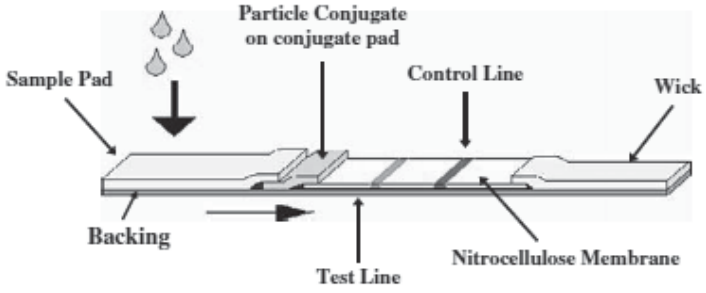


Figure 2 *Typical configuration of a lateral flow immunoassay test strip (adapted from O'Farrell, 2009)*[40]

It employs the same immunoassay principles but coats the antibodies and other reagents on a nitrocellulose membrane rather than the inside of test wells or paddles. It also employs colloidal gold, dye, or latex bead conjugates to generate signal rather than enzymes bead conjugates. Test kits such as Neogen, R-Biopharm and Tepnel kits have been developed for allergen ingredients detection using ELISA test kits or "on-site" rapid tests that employed lateral flow methods.

CONCLUSION

This paper deals with recent developments and applications of the ELISA in determining food chemical contaminants such as residues of pesticides, veterinary medicine residues and other contaminants in food derived from food processing and storage. ELISA techniques could be widely used to detect and quantitate various foodborne pathogens by targeting their surface structures, toxins, such as *Salmonella*, *Escherichia coli*, staphylococcal enterotoxins, or whole cells using readily available test kits. ELISA kits should be used routinely for the mycotoxin analysis of different food matrices that are extensively tested, but the confirmatory analyses by HPLC or LC-MS are desirable. Commercially available ELISA kits for screening purposes are targeted toward food allergens but also to certify gluten-free products. Some rapid ELISA screening tests were developed in order to detect genetically modified organisms in raw agricultural or slightly processed food products having limitations when applied to highly processed food. In addition, ELISA can also be applied for authenticity testing food of animal origin, such as meat and milk-dairy products.

The ELISAs significance for food forensic analysis is evident, but the progress of development of new ELISAs and related immune-technologies is still limited by the availability of antibodies with the desired affinities and specificities for given applications. In this context, the antibody engineering and production of recombinant antibodies with novel binding properties is a very promising field both for research and application.

ACKNOWLEDGMENT

The authors acknowledge funding from the Ministry of Education, Science and Technological Development of the Republic of Serbia, Project no. III 46009, as well as the Ministry of the Interior of the Republic of Serbia, Project no. 242/16-4-2014.

REFERENCES

1. Ahmed, F.E., Detection of genetically modified organisms in foods. Trends in Biotechnology, 20:215-223, 2002.
2. Asensio, L., González, I., García, T., Martín, R., Determination of food authenticity by enzyme-linked immunosorbent assay (ELISA). Food Control 19:1-8, 2008.
3. Ayaz, Y., Ayaz, N.D., Erol, I., Detection of species in meat and meat products using enzyme-linked immunosorbent assay. Journal of Muscle Foods, 17:214-220, 2006.

40 *O'Farrel, B., Evolution in lateral flow–based immunoassay systems. In: Wong, R.C., Tse, H.Y., (Eds.), Lateral flow immunoassay. Humana Press, New York, 2009.*

4. Bonwick, G.A., Smith, C.J., Immunoassays: their history, development and current place in food science and technology. International Journal of Food Science & Technology, 39:817-827, 2004.

5. Brandon, D.L., Frieman, M., Immunoassays to soy proteins. Journal of Agriculture and Food Chemistry, 50: 6635-6642, 2002.

6. Catala, A.M., Puchades, R., Enzymic technique: enzyme-linked immunosorbent assay (ELISA). In: Sun, D.-W., (Ed), Modern techniques for food authentication. 1st ed. Burlington, Mass.: Academic Press. pp. 477-520, 2008.

7. Chen, J., Contemporary monitoring methods. In: Schmidt, R.H., Rodrick, G.E. (Eds.), Food safety handbook (chapter 11). Hoboken, NJ: John Wiley & Sons, Inc. 2003.

8. Cho, Y.A., Lee, V., Park, E.Y., Lee, Y.T., Bruce, D.H., Chang, A.K., Jae, K.L., Development of an ELISA for the Organophosphorus Insecticide Chlorpyrifos. Bulletin of the Korean Chemical Society, 23:481-487, 2002.

9. Crowther, J.R., The ELISA Guidebook. 2nd edition. New York: Humana Press, 2009.

10. De La Fuente, M.A., Juárez, M., Authenticity assessment of dairy products. Critical Reviews in Food Science and Nutrition 45, 563-585, 2005.

11. De La Guardia, M., Gonzalez Illueca, A., Food Protected Designation of Origin: Methodologies and Applications, Comprehensive Analytical Chemistry, 60:2-773, 2013.

12. ELISA Technical Guide-Idexx, available at: https://www.idexx.com/pdf/en_us/livestock-poultry/elisa-technical-guide.pdf

13. Fung, D.Y.C., Rapid Methods and Automation in Microbiology. Comprehensive Reviews in Food Science and Food Safety, 1: 3-22, 2002.

14. Gazzaz, S.S., Rasco, B.A., Dong, F.M., Application of immunochemical assays to food analysis. Critical Reviews in Food Science and Nutrition, 32(3):197-229, 1992.

15. Goldsby, R.A., Kindt, T.K., Osborne, B.A., Kuby, J., Immunology, 5th Edition, W.H. Freeman and Company, New York, New York, 2003.

16. Hsieh, Y-H.P., Immunoassays. Ch. 17. In: Nielsen, S.S. (Ed) Food analysis, 4th edn. Springer, New York, 2010.

17. Liu, L., Chen, F.-C., Dorsey, J., Hsieh, Y.-H.P., Sensitive monoclonal antibodybased sandwich ELISA for the detection of porcine skeletal muscle in meat and feed products. Journal of Food Science, 71(1):M1-M6, 2006.

18. Macedo-Silva, A., Shimokomaki, M., Vaz, A.J., Yamamoto, Y.Y., Tenuta-Filho, A., Textured soy protein quantification in commercial hamburger. Journal of Food Composition and Analysis, 14:469-478, 2001.

19. Mandal, P.K., Biswas, A.K., Choi, K., Pal, U.K., Methods for Rapid Detection of Foodborne Pathogens: An Overview. American Journal of Food Technology, 6:87-102, 2011.

20. Mirić, M., Šobajić, S., Zdravstvena ispravnost namirnica, Zavod za izdavanje udžbenika, Beograd, 2002.

21. Nollet, L.M.L., (Ed), Handbook of food analysis (2nd edition). v3: Methods and instruments in applied food analysis. New York: Marcel Dekker, 2004.

22. O'Farrel, B., Evolution in lateral flow–based immunoassay systems. In: Wong, R.C., Tse, H.Y., (Eds.), Lateral flow immunoassay. Humana Press, New York, 2009.

23. Pascale, M., Visconti, A. Overview of detection methods for mycotoxins. In: Leslie, J.F., Bandyopadhyay, R., Visconti, A. (Eds.), Mycotoxins-Detection Methods, Management, Public Health and Agricultural. CAB International, UK, pp. 171-183, 2008.

24. Pittet, A., Modern methods and trends in mycotoxin analysis. Mitteilungen aus Lebensmitteluntersuchung und Hygiene 96:424-444, 2005.

25. Puchades, R., Maquieira, A., ELISA Tools for Food PDO Authentication, Comprehensive Analytical Chemistry, 60:145-193, 2013.

26. Rakshit, S.K., Diagnostic enzymes. In: Pandey, A., Webb, C., Coccol, C.R., Larroche, C. (Eds), Enzyme Technology; New York: Springer, pp.685-696. 2006.

27. Schmidt, R.H., Rodrick, G.E., Contemporary Monitoring Methods, in Food Safety Handbook, John Wiley & Sons, Inc., Hoboken, NJ, USA, 2003.

28. Schubert-Ullrich, P., Rudolf, J., Ansari, P., Galler, B., Führer, M., Molinelli, A., Baumgartner, S., Commercialized rapid immunoanalytical tests for determination of allergenic food proteins: an overview. Analytical and Bioanalytical Chemistry, 395(1):69-81, 2009.

29. Shankar, B.P., Manjunatha Prabhu, B.H., Chandan, S., Ranjith, D., Shivakumar, V., Rapid Methods for detection of Veterinary Drug residues in Meat. Veterinary World, 3(5):241-246, 2010.

30. Sun, D.-W., (Ed), Modern Techniques for Food Authentication, Academic Press / Elsevier, San Diego, California, USA, 720 pp., 2009, ISBN: 978-0-12-374085-4.

31. Tsutsumi, T., Amakura, Y., Okuyama, A., Tanioka, Y., Sakata, K., Sasaki, K., Maitani, T., Application of an ELISA for PCB 118 to the screening of dioxin-like PCBs in retail fish. Chemosphere, 65(3):467-73, 2006.

32. Valdes, I., Garcia, E., Llorente, M., Mendez, E., Innovative approach to low-level gluten determination in foods using a novel sandwich enzyme-linked immunosorbent assay protocol. European Journal of Gastroenterology & Hepatology, 15, 465-474, 2003.

33. van Hengel, A.J., Food allergen detection methods and the challenge to protect food-allergic consumers. Analytical and Bioanalytical Chemistry, 389(1):111-118, 2007.

34. Zachar, P., Šoltés, M., Kasarda, R., Novotny, J., Novikmecová, M., Marcinčáková, D., Analytical methods for the species identification of milk and milk products. Mljekarstvo, 61(3):199-207, 2011.

UDC: 343.983:623.44

GUNSHOT RESIDUES IN DETERMINING A SHOOTING DISTANCE IN FORENSICS[1]

Ivana Bjelovuk[2]
The Academy of Criminalistic and Police Studies, Belgrade
Aleksandar Ivanovic[3]
Forensic Centre, Police Department of Montenegro
Milan Zarkovic
The Academy of Criminalistic and Police Studies, Belgrade

Abstract: The paper will discuss the traces of gunpowder particles that remain as a result of shooting from a firearm and its passage through the first barrier and the possibility of their use for determining shooting distance. A brief overview of the methods used in practice to determine the shooting distance with a discussion of each of them will be given starting from the chemical methods of Walker, Leszezynski, Shontag and the method of atomic absorption spectrometry, as well as other applicable methods. Experimental firing of a pistol WALTER MTPH, cal. 6.35 PPU98 in the clean, white cotton fabric from different distances is performed with the aim to point out the existence of characteristic traces around the missile trajectory that can be used to estimate the shooting distance also. The above will also be considered in the context of the importance of establishing and evaluating relevant facts of crimes and criminal proceedings.

Keywords: firearm, gunshot residues, halo, shooting distance.

INTRODUCTION

Firearms are misused in the execution of numerous crimes, not only to enhance the seriousness of the threat but also through the shooting that may result in bodily injury, including the killing of a victim. In this regard, in forensic practice, but also in the process of determining and assessment of the facts that are of importance to the legal qualification of a specific event (for example, whether it is about self-injury, injuries by another person, suicide, murder, whether it is a necessary defence or extension of self-defence), the court ballistic expert is asked to give their opinion about the distance from which it was shot, i.e., what was the position of a particular person/persons at the moment when the missile was shot. The use of firearms results with characteristic traces in the form of weapons, ammunition and parts of ammunition, gunpowder particles, traces at the missile trajectory.

The evidence potential of gunpowder traces in forensics is undoubted since with their examination one can establish a fact of shooting from a firearm, time of the shot, as well as from which side and from which distance the shot was fired in regard to a barrier.[4] "The evidence is examined first to see if any bullet holes can be identified. If what appear to be bullet holes is found, an attempt will be made to determine which are *bullet entrance holes* and which are *bullet exit holes.*"[5] The most important is to determine which side of the hole is the entrance hole because the gun shot residues which are used for a distance determination are on the entrance side of clothing. Since the shooting distance is determined on the basis of traces resulting from

1 This article is the result of scientific research project Development of institutional capacity, standards and procedures for countering organized crime and terrorism in terms of international integration, which is funded by the Ministry of Science and Technological Development of the Republic of Serbia (no. 179045) and implemented by the Academy of Police Studies in Belgrade (2011-2015). Also this article is the result of a scientific research project Forensic methods in criminalistics, funded and implemented by the Academy of Criminalistic and Police Studies (2015-2019)

2 Corresponding author, Lecturer at the Academy for Criminalistic and Police Studies, Belgrade, Serbia, e-mail: ivana.bjelovuk@kpa.edu.rs ; Also this article is the result of scientific research project Forensic methods in criminalistics, funded and implemented by the Academy of Criminalistic and Police Studies (2015-2019)

3 Manager of the group for handling evidence material, forensic analytics and quality control in the Forensic Center, Police Directorate of Montenegro

4 Ivanović A., Bjelovuk I. (2010) The reliability of forensic methods to detect gunshot residues on the hands of suspect. Bezbednost, Belgrade, (2010), Vol. 52, No. 3, p. 7-23 (editor in chief: full professor B. Milojković, PhD); Ivanovic A. (2006). Expertise of copper traces, for crimes committed with a firearm, using DTO test - forensic aspect. Podgorica. Ekspertus Forensis No 8. Association of Court Experts of Montenegro. ; Ivanovic A. (2007). Application of infrared spectrophotometry in expertise of bullet traces.. Podgorica. Expertus Forensis No 8. Association of Court Experts of Montenegro.; Ivanovic A. (2007). Sodium rhodizonate test - specific chemical colorimetric test for the detection of trace amounts of lead in GSR. Perjanik No 8. The Police Academy of Montenegro.

5 http://www.firearmsid.com/A_distance.htm retrieved on 20th Jan 2015

the combustion of gunpowder charge in the bullets of a firearm, for the determination of shooting distance it is very important to have the knowledge in the field of ballistics, since that is the science that studies the laws of missile trajectory when fired from a firearm. In a very short period of time reaction products of gunpowder combustion are exposed to a great pressure that causes movement of a missile. Combustion products partially leave the barrel exiting with the missile and spread diffusely in the air. Thus the traces of burned, partially burnt and unburned gunpowder can be found around the missile trajectory and that is only on one of its part, while when the missile is passing through a barrier around the entrance hole through which the missile passed there are traces of gunpowder residue particles in the form of gunpowder halos. This halo is far easier noticeable on lighter fabrics, especially white, compared to the one that occurred on the fabric of dark colour. The presence of gunpowder halo indicates the distance of the weapon's muzzle from which it was fired, and based on its dimensions one can tentatively determine the distance from which the shot was fired. It is important to say that it makes sense to look for the gunpowder particles up to a certain distance, which depends on the type of weapon, the calibre and type of ammunition as they do not follow the missile to the end of its trajectory.

For the determination of shooting distance of firearms with slug (rifled, grooved) barrels with a long tradition we used Walker's method, as well as the methods of Leszezynski, Hoffman and Shontag [6]. Walker method is based on the nitrites contained in the products of gunpowder combustion as characteristic compounds and their chemical reaction with sulfanilic acid, alpha naphthyl amine with acetic acid. Leszezynski's method is based on particles of lead (Pb) in gunpowder halo. Shontag's method is based on elements lead (Pb), antimony (Sb) and barium (Ba) and micro elemental spectrographic analysis. For determination of shooting distance, besides mentioned methods, in the criminal-technical / forensic practice of the Republic of Serbia we are using modified Shontag's method that involves determining the shooting distance using the calibration curve in the coordinate system in which on the ordinate was inflicted with the values of the concentration of antimony (Sb) determined by flameless atomic absorption analysis of indisputable samples (residues of gunpowder particles from the known distance), while the abscissa was inflicted with the values of distance from which the shots were fired. Then after determining the concentration of antimony and the drawing of parallel line to the abscissa we would have the values of the shooting distance. "Nowadays, chemical tests are the preferred method to reveal the GSR pattern on cloths for most forensic laboratories."[7]

In the last few years of forensic practice for the GSR detection experts are using the inductively coupled plasma mass spectrometry (ICP-MS)[8]. "Plasma-Mass Spectrometry (ICP-MS) has also been used for firing distance estimation through the analysis of antimony, barium, and lead on cotton tissue targets at distances ranging between 20 and 200 cm from the target (with 10 cm intervals)"[9] "The analytical technique most used for that purpose is X-ray fluorescence (XRF) which records the generated fluorescence emission after the X-ray source excitation of the sample."[10] Papers were published about the use of Atomic Force Microscopy (AFM) analysis in the examination of the gunpowder particles and the determination of shooting distance.[11]

So far in the criminal-technical / forensic practice in the Republic of Serbia, determination of the shooting distance was done by the registered court expert in the field of ballistics, i.e. by the physics-chemists, chemists, mechanical engineers and other professionals with other educational backgrounds[12]. As it is obvious from the above mentioned that various methods may be used to determine the shooting distance it is necessary to have a multi-disciplinary approach. Traces of gunshot residues (gunpowder particles) are sampled by a forensic technician (CSI officer) if they are found on the clothes of a victim or on some other barrier, and if they are found on the victim's body, then the procedure is done by a pathologist. Those traces must be carefully handled with the obligatory respect for the chain of movement of the evidence. Considering that most of the particles of gunshot residues are soluble in water, it is necessary to strictly take care of packaging and transport of the materials with gunshot residues.

6 Maksimović, R., Bošković, M., Todorić, U. (1998) Methods of physics, chemistry and physical chemistry in criminalistics. Belgrade: Police academy .

7 Lopez-Lopez, M., Garcıa-Ruiz, C. Recent non-chemical approaches to estimate the shooting distance. Forensic Science International 239 (2014)79-85

8 Bjelovuk, I. Ivanović, A., Žarković, M. GSR as Trace Evidence. Thematic Conference Proceedings of International Significance "Archibald Reiss Days", Vol. I (ed. in chief Associate professor D. Kolarić, PhD), Academy of Criminalistic and Police Studies, Belgrade, 2-4 March 2014.

9 Santos, A., Magalhaes, T., Nuno Vieira, D., Almeida, A.A., Sousa, A.V. Firing distance estimation through the analysis of the gunshot residue deposit pattern around the bullet entrance hole by inductively coupled plasma-mass spectrometry Am. J. Forensic Med. Pathol., 28 (2007), pp. 24–30

10 Lopez-Lopez, M., Garcıa-Ruiz, C. Recent non-chemical approaches to estimate the shooting distance. Forensic Science International 239 (2014)79-85

11 Mou, Y., Lakadwar, J., Rabalais, J.W. Evaluation of shooting distance by AFM and FTIR/ATR analysis of GSR. J. Forensic Sci., 53 (2008), pp. 1381–1386

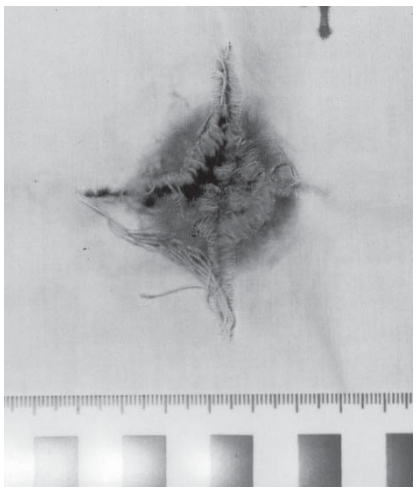
12 Žarković, M., Bjelovuk, I., Borojević, A., Critical review of the work and educational profile of court experts in specific areas of expertise in the Republic of Serbia. Legal Life, the magazine for legal theory and practice. Special issue: Law and the principle of good faith - Vol. 63, Book 571, no. 9, 2014, p. 693-704 (editor in chief: full professor Slobodan Perovic, PhD).

MATERIAL AND METHOD

In this paper we used experimental method. For experimental testing we used clean, white cotton fabric and WALTER MTPH pistol, cal. 6.35mm PPU98 (produced by "Prvi Partizan" - Užice, production year '98). Experimental firing was carried out in the ballistic laboratory in the Forensic Centre in Podgorica. Experimental missile firing was carried out in order to characterize traces of gunpowder on the fabric as the first barrier through which the missile is passing through and to establish correlations between the traces and the shooting distance. The bullets were fired so that the missile penetrates the fabric at an angle of 90 °. In this paper we used the method of visual observation, observation under a microscope, measuring and describing traces of gunshot residues, as well as the method of comparison. Namely, the comparison was done between gunpowder halos on the fabric caused by firing into the fabric from different distances. While experimental firing we took care to shift the shooter in order to avoid contamination of traces when firing from different distances.

SPECIFIC (CHARACTERISTIC) TRACES OF THE USE OF FIREARMS THAT COULD BE USED TO DETERMINE SHOOTING DISTANCE

Given the diversity of traces that occur as a result of shooting from firearms at different distances, the distance from the muzzle of the firearms with short barrel to the first barrier on the missile's trajectory can be divided into several segments: direct contact between a firearm and a barrier (contact - 0 cm), the zone of action of flame and fire (to about 20 cm seen from the muzzle of a firearm towards the target), from about 20 to 40cm from the muzzle of a firearm towards the target, i.e. from 40-50 cm to 90-100 cm and from around 90-100cm. In the cases of contact (direct contact between the barrel of a firearm and a target) expertise of the shooting distance refers to the muzzle of a firearm. Typical traces of such cases occur due to the action of a missile and the action of the pressure of gunpowder gas. When the fabric is the first barrier through which the missile is passing (for example some garment) with contact muzzle of the firearm, due to a high pressure of gases to the muzzle, tearing of the fabric occur in the form of a cross, on which edges there is visible blackness (traces of burning) (picture 1).



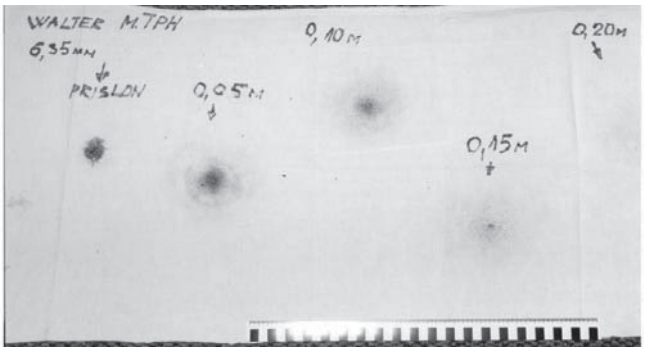
Picture 1[13] *Typical trace on the fabric in case of contact shot*

In case the missile hits a body part that is not covered by clothing or in some other way, as a typical trace there is gunshot wound in the form of large and irregular star shape skin damage, i.e. laceration. The cases of contact shot are also characterized by the occurrence of a print of the muzzle of a firearm on the skin. This is because the contact shots are, in most cases, followed by the pressure on the skin.

When a bullet is fired from a firearm, the flame occurs on the muzzle of a barrel as a result of the burning gunpowder and a fire as a result of the reaction of the products of gunpowder and air combustion (carbon monoxide - CO, hydrogen - H_2 and methane - CH_4). Flame length depends on the type of a firearm, its calibre and ammunition.

13 Ivanovic A., Čukic D. (2006). Expertise of shooting distance with gunshot wounds - a modern approach. Podgorica. Expertus Forensis No 5. Association of Court Experts of Montenegro.

Picture 2 shows the traces of firing a firearm into a white cotton fabric from the following distances: contact - 0cm, 5cm, 10cm and 15cm.



Picture 2[14] *Typical traces on the fabric in the cases of firing a firearm from different distances (in this experiment the pistol WALTER MTPH, cal. 6,35mm was used).*

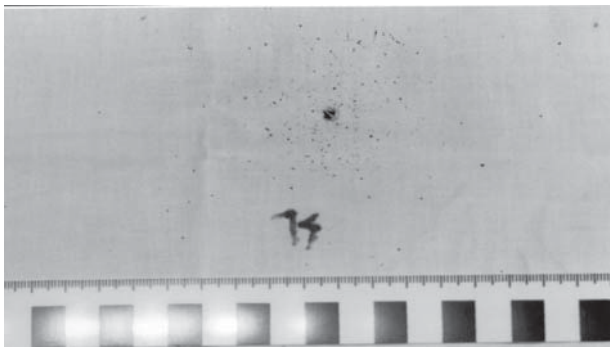
Picture 2 shows that after firing a missile from the pistol WALTER MTPH, cal. 6.35mm at a distance of 15 cm from the muzzle of a firearm to the cotton fabric there are visible traces of burning (blackness), which could be interpreted as the effect of flame when firing a bullet from the pistol, visible up to a distance of about 15 cm from the muzzle to the place where the missile hit. In the case of a gunshot in the uncovered human skin traces of flame effects are manifested in the form of burns and similar skin reactions.

Along with other traces of firing a bullet from a distance at which it is evident that there is a presence of flames and fire, burning traces (blackness) can also be found on the fabric. The appearance of gunshot traces is affected also by the fibre composition of textile which represents a barrier through which the missile has passed. Thus, the fabrics of natural materials (plant fibres), did not show phenomena of burning the fabric in such a way that there is the dissolution of the material and the appearance of the gas phase. This is in contrast to synthetic fibres in which there is an apparent lower resistance to flame and in which (for example in the case of viscose), when exposed to flames and fire from the muzzle of a firearm, burning is happening in the fibres from which the fabric was made, as well as the beginning of the dissolution of material and creation of the gas phase. When a shot is fired from a firearm from a distance of the effect of flame and fire, fibre ends in viscose fabrics at the point where the missile passed through start to form short thickened nodes due to melting, which are clearly visible under the microscope. Besides that, the ends of the fibres may disappear or due to melting they can bend with the creation of beads on the ends. At polyamide fibres (nylon, perlon) such melting causes numerous characteristic of warming on the edges of the entrance hole of the missile. Especially developed occurrence of warming in the form of nodes can be seen in single loose fibres.

The third zone in determining the shooting distance refers to the spread of gunpowder particles to a distance of about 20-40 cm from the muzzle of a firearm to the target and this applies to the firearms with the so-called short barrel.

While recognizing the existence of characteristic traces in the case of contact between a muzzle of a firearm and a human body or a garment, i.e. those that occur due to the effects of flame and fire from the muzzle of a firearm, when determining a shooting distance unburned and half burned gunpowder particles may be of interest. In other words, the shooting distance can also be determined with respect of the distance from the effects of flame and fire from the muzzle of a firearm to the final distance of half burned and unburned gunpowder particles. To the distance (from the muzzle of a firearm to about 40-50 cm to the target, following a missile) gunshot residues have a relatively high kinetic energy causing then to perform penetration into the space between the fibres weave. Within the limits of distance (from 40-50cm, to their final distance, which is about 90cm for short barrel firearms) gunshot residues that after firing a bullet exits the muzzle of a firearm suddenly lose velocity due to air resistance. This causes a reduction of their kinetic energy, and they, with weak adhesion forces, stick to the fabric of the garment, not cutting the fabric of a garment, and partly falling on the surface below the hole. This is also depending on used firearms and ammunition.

14 Ibid.



Picture 3[15] *Traces on the fabric in the form of penetration of gunpowder particles from the 40 cm distance*

Given that, gunpowder particles which exit with the missile at a distance from the muzzle of a firearm to the target of about 40-50cm to 90 - 100 cm, due to the resistance of the environment, rapidly lose their kinetic energy and do not stick with strong adhesion forces to the material of a garment, it is recommended that the garment, which has been hit by a missile from this distance, is handled very carefully. Otherwise, if handled carelessly gunshot residues could fall off or be moved from one place to another (by bending, folding, crumpling, throwing the garment, etc.).

When determining the shooting distance one should not ignore the appearance of the entrance hole of the missile. Namely, the entrance hole with a proper round hole indicates that the missile perpendicularly penetrated the barrier, while elliptical hole indicates a certain angle of penetration.

When interpreting traces at the crime scene, one should always bear in mind that the perpetrator may have used a silencer. The use of a silencer while shooting from a firearm will also affect the quantity and dispersible of gunshot residue and can be an aggravating factor in determining the shooting distance at the moment when a missile was fired. This is due to the fact that a silencer as a mechanical device that is mounted on a firearm with the intention to suppress the sound that is produced when firing a bullet from a firearm (due to the explosion of powder gases and because of the missile velocity which is greater than the speed of sound) takes products of combustion of gunpowder to special chambers or in the openings (depending on the type of silencer).

Experimental firing for comparative analysis, which is a function of defining the shooting distance, is necessary to perform with the use of such type of ammunition whose use is established when processing a crime scene. This is due to the fact that the ammunition of different production types can have different burnishing zones, as well as different types of gunpowder (nitrocellulose, nitroguanidine, etc.). In addition, the ammunition from the same producer may contain different components in a bullet (initial primer within which is the initial mixture, case with gunpowder charge and a missile). Thus, for example, primer can have different combinations of the initial mixture, one or two holes through which the decomposition products of the initial mixture are passing; case (steel or brass) may contain nitroguanidine or some other gunpowder; missile can be out of lead with or without jacket, all depending on which characteristics for a bullet an engineer wanted to achieve when designing the ammunition. Because of all that was said, when performing experimental firing in this case we used the ammunition from one producer, produced the same year and for one firearm.

DISCUSSION

When examining gunshot residues it is necessary to respect standard procedures of examination, meaning those that are used in other countries as well. This is in order to create the preconditions that the provided material evidence obtain undeniable credibility. One of the key assumptions and settings of the procedure requires (orders): "Gunshot residue distance standards are made by firing the firearm, using ammunition like that used in the actual case, into witness panels that consist of white pieces of cotton twill jean cloth."[16]

The determination of shooting distance is done based on the traces around the entrance hole of a missile, based on the gunshot residues. The size of the blackness of the gunpowder halo indicates a shooting

15 Ibid.

16 http://www.firearmsid.com/A_diststandards.htm retrieved at 20th Jan 2015

distance. The experiments in which missiles were fired from the pistol WALTER MTPH, cal. 6.35 in white fabric confirmed the direct dependence of the distance between the muzzle of a firearm and the fabric in which a missile was fired and the size of halo around the entrance hole. Also, it was noticed that the intensity of the coloration and density distribution of the gunshot residues around the entrance hole of a missile is smaller at greater distances.

From chemical analysis methods if gunshot residues in gunpowder halos today in some countries they use methods of Walker and Leszezynski. Flaw of Walker's and Leszezynski's methods is that the number of particles of gunshot residues, which in sampled and secured with these methods, depends, among other things, on the pressure on the layers of fabric, photo paper, etc., the intensity of iron pressure, or possession of presses in the laboratory and they require a lot of time for the performance. In cases where the distance between the barrier through which the missile has passed to the muzzle of a firearm is bigger, the method gives more deviations. It was also observed that the chemicals at high temperature are colouring photo paper with the similar colour as nitrite particles that are produced by the combustion of gunpowder. It is known that nitrites are soluble in water, so in cases of wet clothes unreliable results may be obtained. Since the Leszezynski's method is based on the detection of the presence of lead particles, in this respect it is more precise when it comes to wet fabric samples compared to Walker's method based on nitrites that occur during the combustion of gunpowder. The cost of these methods is relatively low, so it does not require expensive laboratory equipment and supplies when compared to Shontag's method, and training for the use of these methods is simple. Shontag's method is based on particles of lead, antimony and barium, and spectrography. Previously mentioned methods involve determination of the shooting distances for the distances up to about 1m. When comparing the experiences of Shontag and modified Shontag's method (based on the particles of lead, antimony and barium and atomic absorption analysis) it was observed that Shontag's method gives less reliable results than the modified Shontag's method given the greater sensitivity of the atomic absorption analysis, and thus the possibility to identify larger shooting distances. The flaw of modified Shontag's method is that it requires expensive equipment and certified expert in the laboratory.

Collected evidence from a crime scene in the form of fabrics is first visually observed in order to describe the damage and make preliminary conclusion on whether the damage is from a missile of from the use of some other items. Also, it is preferable to observe characteristic traces under a microscope for the detection of gunshot residues due to their specific appearance. After the visual observation of materials with gunshot residues it is desirable to examine the material with the use of a device with IR rays, which are contained within the invisible part of the spectrum of electromagnetic radiation. This way enables one to spot gunshot residues that were not visible when looking just with your eyes. The advantage of using the method with IR rays is that this method is not destructive, i.e. after its use the material can still be examined. With this method it is possible to find traces which are not visible to the naked eye, and which do not origin from the existence of gunshot residue and where there is no physical damage to the fabric (dark patches of different origins for example dirt, traces of paint, ink, soot and grease oils etc.).

These observations are important in order to acquire the image about the distance from which a missile was fired. Typical traces, consequences of firing a bullet, such as split-off part of the garment, slots, melted fabrics, dark spots around the bullet hole, burned, partially burned and unburned gunpowder particles, as well as the presence of metal particles on the fabric are elements that can serve as the basis and parameters for determining a shooting distance.

In the absence of gunshot residue around the entrance hole on the first barrier through which the missile has passed, it is possible that the distance when the missile was fired exceeded the measurable distance for a given weapon and ammunition, but one should certainly be suspicious about inadequate sampling of material for testing, for example in cases of very bloody clothes, wet clothes, reckless handling of evidence when processing a crime scene, the existence of other barriers between the muzzle of a firearm and a victim in the moment when a missile was fired, etc.

It is very important to pay attention on the time that passed from the moment of shooting (time of the performance of a criminal offence) till the time when a ballistic expertise is performed that has the aim to determine a shooting distance. It is therefore necessary as soon as possible to perform a forensic crime scene investigation and sampling of the materials (for example clothes through which a missile has passed) in order for the forensic ballistic laboratory to get, as soon as possible, all the traces secured from a crime scene and complete documentation from the CSI investigation in order to perform necessary analysis, as soon as possible, and to make valid conclusions.

CONCLUSION

First, it should be emphasized the quality securing of material evidence in the form of gunshot residues, their packaging, transport and storage is of paramount importance in determining shooting distance, and therefore for other criminal and criminal proceedings relevant circumstances of a particular event. In addition, determining responses to relevant questions involves securing, analysis and interpretation of other material evidence, the testimony of the participants in a particular event and other persons, as well as numerous other circumstances related to the event (for example use of silencer, handmade, remodelled or modified weapons, small calibre ammunition, ammunition with bad performances - old, etc.). As in the case of other material evidence, relevant material evidence found and secured during CSI investigation should be, as soon as possible, transported to a ballistic laboratory in order to perform adequate timely analysis. Also, it is recommended that in all stages of processing one use methods for the examination of gunshot residues that are accepted in other countries as well. And all that with the objective to provide material evidence with the strongest possible evidence credibility.

The experiments presented in this paper have shown the direct dependence of the distance between the muzzle of a firearm and an object in which a missile is fired (shooting distance) and dispersible characteristics of gunshot residues around the entrance hole expressed with the size of a gunpowder halo. Also, experiments have confirmed the inverse dependence of intensity of colouring and density distribution of gunshot residues around the entrance hole of a missile. Experiments have shown that the missiles which were fired from different distances gave a different picture of the entrance hole in the fabric that was created by a missile with a gunpowder halo.

By examining the evidence material to determine shooting distance also important and unavoidable are non-destructive methods such as visual observation and observation under a microscope, but also the IR device method with which it is possible to estimate the shooting distance based on the size of gunpowder halo around the damage caused by a missile.

When it comes to determining the shooting distance using chemical methods, considering the cost of a method one should give priority to the old tried and validated methods of Walker and Leszezynski, and if there are the conditions for that, the priority should be given to the modified Shontag's method. As the Atomic Absorption Analysis (AAS) and Inductively Coupled Plasma coupled to Atomic Emission Spectrometry (ICP-AES) were also used for the elemental analysis of the gunshot residues, it is important to highlight that they required long pre-treatment of the samples. Also they are destructive for the sample and no other analysis can be used for further examinations.

Besides the mentioned methods that require a multidisciplinary approach (cooperation of mechanical engineers, ballistic experts and chemists) one should not ignore the existence of characteristic traces around the missile trajectory (gunpowder particles, snicks, penetrations, et al.), and which can also be used to estimate the shooting distance especially when we are talking about a preliminary assessment at the crime scene.

REFERENCES

1. Bjelovuk, I. Ivanović, A., Žarković, M. GSR as Trace Evidence. Thematic Conference Proceedings of International Significance "Archibald Reiss Days", Vol. I (chief editor Associate professor D. Kolarić, PhD), Academy of Criminalistic and Police Studies, Belgrade, 2-4 March 2014.
2. Ivanović, A., Bjelovuk, I. The reliability of forensic methods to detect gunshot residues on the hands of suspect. Bezbednost, Belgrade, (2010), Vol. 52, No. 3, p. 7-23 (editor in chief: full professor B. Milojković, PhD)
3. Ivanović, A., Čukic D. (2006). Expertise of shooting distance with gunshot wounds - a modern approach. Podgorica. Ekspertus Forensis No 5. Association of Court Experts of Montenegro.
4. Ivanović, A. (2006). Expertise of copper traces, for crimes committed with a firearm, using DTO test - forensic aspect. Podgorica. Ekspertus Forensis No 8. Association of Court Experts of Montenegro.
5. Ivanović, A. (2007). Application of infrared spectrophotometry in expertise of bullet traces.. Podgorica. Expertus Forensis No 8. Association of Court Experts of Montenegro.
6. Ivanovic A. (2007). Sodium rhodizonate test - specific chemical colorimetric test for the detection of trace amounts of lead in GSR. Perjanik No 8. Police Academy of Montenegro.
7. Lopez-Lopez, M., Garcıa-Ruiz, C. Recent non-chemical approaches to estimate the shooting distance. Forensic Science International, 239 (2014)79-85
8. Maksimović, R., Bošković, M., Todorić, U. (1998) Methods of physics, chemistry and physical chamistry in criminalistics. Belgrade: Police academy.

9. Mou, Y., Lakadwar, J., Rabalais, J.W. Evaluation of shooting distance by AFM and FTIR/ATR analysis of GSR. J. Forensic Sci., 53 (2008), pp. 1381–1386

10. Santos, A., Magalhaes, T., Nuno Vieira, D., Almeida, A.A., Sousa, A.V. Firing distance estimation through the analysis of the gunshot residue deposit pattern around the bullet entrance hole by inductively coupled plasma-mass spectrometry Am. J. Forensic Med. Pathol., 28 (2007), pp. 24–30

11. Žarković, M., Bjelovuk, I., Kesić, T. (2012) Crime Scene Management and Credibility of Scientific Evidence. Academy of Criminalistic and Police Studies, Belgrade.

12. Žarković, M., Bjelovuk, I., Borojević, A., Critical review of the work and educational profile of court experts in specific areas of expertise in the Republic of Serbia. Legal Life, the magazine for legal theory and practice. Special issue: Law and the principle of good faith - Vol. 63, Book 571, no. 9, 2014, p. 693-704 (editor in chief: full professor Slobodan Perovic, PhD).

13. http://www.firearmsid.com/A_distance.htm retrieved on 20th Jan 2015

14. http://www.firearmsid.com/A_diststandards.htm retrieved on 20th Jan 2015

UDC: 005.6:343.983(497.11)

IMPLEMENTATION OF A QUALITY MANAGEMENT SYSTEM IN THE NATIONAL CRIME-TECHNICAL CENTER OF THE MINISTRY OF INTERIOR OF THE REPUBLIC OF SERBIA IN ACCORDANCE WITH INTERNATIONAL STANDARD SRPS ISO/IEC 17025:2006 (ISO/IEC 17025:2005)[1]

Lazar Nesic
National Crime-Technical Center of the Ministri of Interior of the Republic of Serbia
Jasmina Vuckovic

Andjelko Maric
National Crime-Technical Center of the Ministri of Interior of the Republic of Serbia

Abstract: With the use of established and approved procedures of work in forensic laboratories, the requirements of preserving the credibility of the evidence will be met, all in accordance with international standards that regulate this area (ISO/IEC 17025:2005 - General requirements for the competence of testing and calibration laboratories). Meeting the requirements of the international standards, i.e. implementing a Quality Management System enables the accreditation of forensic laboratories which implies recognition of the results of forensic analysis at the global level, as well as the exchange of experience, data and information with other accredited forensic laboratories.

In this paper it will be presented the accreditation procedure of the National Crime-Technical Centre of MOI of the Republic of Serbia, the implementation of a Quality Management System in forensic laboratories in accordance with Council Decision EU 2009/905 JHA and the Prüm Decision, as well as the Swedish initiative, which includes a simplified exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. Requirements in Chapter 24 Process of negotiations on the accession of the Republic of Serbia to the European Union originate from these decisions and those are the requirements that the Republic of Serbia needs to meet concerning successful future interstate police cooperation. Also, in the paper it will be presented the challenges that the Republic of Serbia faces with regarding the implementation of the main achievements of police cooperation that is, aligning its legislation with the relevant legal acquisitions.

Keywords: Quality Management System, accreditation, decisions of the Council of the European Union, forensic laboratory, ENFSI, NCTC, interstate police cooperation.

INTRODUCTION

The use of advanced technology and scientific discoveries has incited the expansion of the scope of forensic work, primarily in the field of molecular biology (DNA), information technology and other highly sophisticated methods and techniques for evidence examination in forensic laboratories. In addition to the fact that forensic science is applied in the criminal justice system, it also finds its role in other spheres of society (ethno genetic studies of the population). Based on wide use of forensic examinations, it can be estimated their significance in the modern world.

Concerning the fast that crime goes beyond the borders of one country, it is necessary to establish interstate police cooperation in order to exchange forensic data such as data of DNA profiles, fingerprints, other biometric data and other. For these reasons, the introduction and use of unique international standards in this area is very important.

In Europe, the process of standardization, and particularly the process of accreditation is new and its introduction has started a few years ago. The first phase includes the standardization and accreditation of

1 This paper is written within the research project of the Criminal Police Academy "Forensic Methods in Criminology". The Project Manager is Professor Radovan Radovanovic, PhD.

DNA laboratories, forensic laboratories and the Institute of Forensic Medicine. The second phase is standardization and accreditation of forensic work at the crime scene during work with traces.[2]

As regards the fact that the Republic of Serbia has a clear tendency of European Union accession, the harmonization of legislation in the field of forensic examination, i.e. giving an expert opinion, is required. The European Union, through its Council, has adopted a number of decisions, which oblige Member States to implement a common quality standard in the field of forensics. Accepting the requirements of the international standard ISO/IEC 17020:2012 and ISO/IEC 17025:2005 and their implementation in forensic institutions of the Republic of Serbia, through the process of accreditation, an international forensic cooperation is being conducted, and forensic evidences obtain an international legitimacy and become transposable. Regarding the fact that these standards have general character, they are useful for all forensic disciplines.

The European Union has intensified its work in order to introduce standards in the field of forensics in countries of the European Union. In order to introduce a Quality Management System in forensic laboratories, a series of obliging documents are issued. In this paper, among other things, it will be presented European quality standards and a significant part of the regulations referring to forensic laboratories and international police cooperation.

THE NATIONAL CRIME-TECHNICAL CENTER – ENFSI MEMBERSHIP

Defining the quality standards of work with evidence in Europe has initially begun with standardization of DNA laboratories and DNA databases, and afterwards with other forensic laboratories. For this purpose, it has been formed an international institution whose task was to draw up standards of accreditation in the field of forensics, obliging for the whole Europe.[3]

The European Network of Forensic Science Institutes (ENFSI) has been established in 1992 as the most important forensic association and the only one of its kind in Europe (currently it consists of 62 laboratories from 35 European countries). The aim of the organization is to increase the number of its members in Europe, to encourage laboratories to work in accordance with the best practice and international standards for quality and competence, and to establish and maintain relationships with other organizations around the world. For these reasons, it is a significant impact of this organization on a Quality Management System implementation in the field of forensics. Forensic laboratories can become a member of ENFSI if they European Union member states or candidate countries, if they do forensic expertise in several areas, if they apply standard ISO/IEC 17025:2005 or they are planning to implement it, if they have competent status in their country and they employ at least 25 experts who testify in court proceedings. The establishment of a Quality Management System in forensic laboratories among members is the first priority for ENFSI.[4]

Within ENFSI Association operates 17 Working Groups. Any liability regarding the definition and implementation of a Quality Management System has been entrusted to The Quality and Competence Committee[5], which provides recommendations for the compilation of manuals relating to the competence and forensic procedures on the crime scene and in the laboratories, the validity and the use of appropriate methods which are used in laboratories, developing awareness of the necessity of quality presence during procedures at the international level respecting international standards in terms of accreditation of forensic laboratories.[5]

As regards the fact that the Republic of Serbia has a clear tendency of European Union accession, harmonization of regulations in the field of forensic investigation, i.e. experts testimony, is necessary to accomplish. This process refers to harmonization of work on a crime scene and work in laboratory during material evidence examination/expertise.

In organizational structure of the Ministry of Interior of the Republic of Serbia within the Police Directorate it has been constituted the National Crime- Technical Centre (hereinafter NCTC), which is a part of the Criminal Investigation Department. Since April 2009 NCTC has been a full member of the European Network of Forensic Science Institutes and as such participates in the creation of European forensic standards. NCTC primarily aims to implement a Quality Management System and obtain accreditation in

2 Simonovic B., Standardization and accreditation as ways of ensuring professionalism of police and crime investigation units, Security, Belgrade, 2009, vol. 51, iss. 1-2, pp. 236-253

3 Simonovic B., General quote, pp. 236-253.

4 Bjelovuk I., Kesic T., Radosavljevic-Stevanovic N., *The accreditation of forensic laboratories - status and perspectives in Serbia.* Thematic collection of essays *Crime scene investigation of criminal offences* (editor prof. dr D. Kolaric), Academy of Criminalistic and Police Studies, Belgrade, 2013, pp. 159-172

5 Zarkovic M., Bjelovuk I., Nesic L., *Scientific evidence and the role of an expert in criminal proceedings: European quality standards*, Fighting against crime and European integration (Collection of essays from the First Scientific Conference with international participation, Tara, June 2010), Academy of Criminalistic and Police Studies and Hanns Seidel Foundation, Belgrade, 2010, pp. 235-244

accordance with the international standard ISO/IEC 17025:2005, i.e. ISO/IEC 17020:2012 that provides international interchangeability and recognition of examination results and given opinions.

IMPLEMENTATION OF A QUALITY MANAGEMENT SYSTEM IN FORENSIC INSTITUTIONS IN THE REPUBLIC OF SERBIA

The accreditation of forensic laboratories implies the establishment and construction of a Quality Management System and a Quality Assurance System. Forensic laboratories, where both systems have been implemented, are subject of accreditation. Key elements of laboratory accreditation are its employees, that is, personal competencies of each employee in forensic laboratories and the concept of unified standards of forensic practitioners work.[6] Accreditation is allocated by national accreditation body, as an independent institution, which has exclusive jurisdiction, through the assessment process of approved documentation, organization and methods of work in laboratories, assesses whether institution and laboratory meets the requirements of the relevant standards for the award of the accreditation certificate. In the Republic of Serbia procedures relating to accreditation in general, and the accreditation of forensic laboratories, are regulated by the Law on Accreditation.[7]

After providing the required material and technical conditions for accreditation of NCTC and its organizational units, in its first phase it has started with the introduction and validation of the working methods in accordance with the international standard ISO/IEC 17025:2005 in five physical chemical and toxicological laboratories (two in Belgrade, Novi Sad, Nis and Uzice), and in the Department for DNA Analysis and Management of Databases of DNA Profiles in Belgrade, as well as with the harmonization of normative acts with the standards of the EU acquits. With all this, NCTC has provided the required conditions for accreditation.

Preparation for the accreditation of the National Crime-Technical Centre of MOI of the Republic of Serbia was accomplished with the help of the international project EMFA-2 - European Mentorship for Forensic Accreditation (EMFA) within ENFSI organization. Program ENFSI and project EMFA-2 implied accreditation of forensic institutions which hadn't been accredited, and all that with the help of accredited mentoring laboratories. EMFA-2 project was funded by the European Union, and the implementation of the project started in March 2011. Eight forensic laboratories, that are ENFSI members, participated in EMFA-2 project in the following way: an accredited laboratory was mentoring laboratory to the other, which was in the process of preparation for accreditation. As a part of this project, laboratory of the Republic of Croatia, Center for Forensic Examination and Expertise "Ivan Vucetic" was a mentoring laboratory to the National Crime-Technical Centre of MOI of the Republic of Serbia.

After the project EMFA-2 was successfully completed in November 2012, and ENFSI gave a positive opinion that NCTC was ready for accreditation in accordance with the requirements of ISO/IEC 17025:2006 for the assessment of competence of laboratories examinations and calibration, it has started with the submission of the application for accreditation at The National Accreditation Body of Serbia (ATS).

After ATS had considered and accepted applications for accreditation of NCTC, five laboratories for physical and chemical analysis and the Department for DNA Analysis and Management of Databases of DNA Profiles, a team for evaluation of work compliance with standards SRPS ISO/IEC 17025:2006, was formed. After evaluation process was finished, it was confirmed that NCTC and evaluated laboratories for applied examination methods meet the requirements for accreditation in accordance with SRPS ISO/IEC 17025:2006.

Accreditation Body of Serbia, based on the report of the evaluation team and the decision of the technical committee, made a decision on accreditation of the National Crime Technical Centre of the MOI of the Republic of Serbia, on 28th of August 2014. Based on the Decision, it was issued a Certificate on Accreditation - accreditation number 01-413. The certificate represents verification of compliance with implemented quality system with requirements of the international standard SRPS ISO/IEC 17025:2006, which is identical to ISO/IEC 17025:2005.[8] Certificate on Accreditation provides international recognition and interchangeability of results of accredited forensic laboratory for court and other procedures. With accreditation of NCTC and its laboratories the Republic of Serbia has retained full membership of its forensic center in ENFSI.

Accredited laboratories have established procedures for monitoring the quality of the results obtained from the internal (repetition of the same or different examination method) and external quality control

6 Ibid

7 Bjelovuk I., Kesic T., Radosavljevic-Stevanovic N., *The accreditation of forensic laboratories - status and perspectives in Serbia.* Thematic collection of essays *Crime scene investigation of criminal offences* (editor prof. dr D. Kolaric), Academy of Criminalistic and Police Studies, Belgrade, 2013, pp. 159-172

8 Milosevic M., Bjelovuk I., Kesic T.: 2009, pp. 1-10.

(participation in competency testing programs and inter-laboratory monitoring), all in accordance with the requirements of SRPS ISO/IEC 17025:2006 (ISO/IEC 17025:2005). Accreditation Body of Serbia will supervise accredited bodies for evaluation of compliance, in order to ensure continuous achievement of the requirements for procedures which have already been accredited for. During 4 years ATS will perform regular and extraordinary supervising evaluation which will monitor the work of accredited forensic laboratory. Regular supervising evaluation will be performed during the interval of 6 to 9 months. During that time of accreditation, regular supervising evaluation will assess if all requirements and rules of accreditation are accomplished. During the procedure of supervising, among other things, the results of management review, the results of undertaken corrective and preventive measures, the results of undertaken internal audits, equipment status, document management, procurement and training program, will also be evaluated.[9]

In addition to the accreditation of forensic laboratories, as a basic element and condition which should be met for further establishing of a Quality Management System, European Union authorities have brought a number of obliging documents, which are related to the field of forensics, and have to be met and implemented in forensic practice and national legislation.

INTERNATIONAL STANDARDS AND DOCUMENTS THAT REGULATE IMPLEMENTATION OF A QUALITY MANAGEMENT SYSTEM IN THE FIELD OF FORENSICS

The accreditation of forensic laboratories provides the implementation of Quality Management System thereby ensures the credibility and validity of the examination results and improves the quality of laboratory services, which provides independent, impartial and objective examination and expertise in criminal and other legal proceedings.

Quality standards ISO/IEC 17020:2012 and ISO/IEC 17025:2005 can cover the entire forensic process from the moment of police arrival on the crime scene: investigating crime scene, finding relevant material evidence, laboratory examination and interpretation of examination results and reporting, to the moment of giving opinion in court. Standard ISO/IEC 17020:2012 determines the procedures on the crime scene and its introduction and implementation will allow the accreditation in this area. Accreditation of crime scene investigation, according to the ENFSI's instructions at this point is not required, but is recognized as a way how to manage activities at the crime scene, as the initial phase of the investigation procedure, in order to provide security of process and procedures in one consistent and impartial way.

The implementation of the international standard SRPS ISO/IEC 17025:2006 (ISO/IEC 17025:2005), titled General requirements for the competence of testing and calibration laboratories, will greatly facilitate the cooperation between forensic laboratories, acceptance of examination results and calibration, i.e. interstate exchange of information and experiences. Standard that regulates the implementation of a Quality Management System in the laboratory, i.e. its use in forensic laboratories ensures its accreditation, which is a prerequisite for the validity of the material evidence wherever it was processed.[10]

Standard SRPS ISO/IEC 17025:2006 (ISO/IEC 17025:2005) includes the general requirements relating to management:

1) Management organization;
2) Management system that includes quality system, administrative and technical systems used to manage the work of the laboratory;
3) Records management;
4) Internal audits;
5) Management review, in order to implement required changes or improvements.[11]

Technical requirements are related to personnel, facility conditions and working environment, methods of testing and calibration, as well as validation methods, equipment, sampling, handling of samples for testing and calibration. A key factor in ensuring the competence of forensic laboratories and obtaining and maintaining accreditation is to provide competence of personnel who work in the laboratory. Competence includes the appropriate level of qualification, appropriate professional knowledge and skills, as well as continuous improving through permanent training and education.[12]

9 http://www.ats.rs/sr/strane/nadzor
10 Milosevic M., Bjelovuk I., Kesic T., 2009, pp. 1-10
11 SRPS 17025:2006 General requirements for the competence of testing and calibration laboratories
12 Bjelovuk I., Kesic T., Radosavljevic-Stevanovic N., Belgrade, 2013, pp. 159-172

'Guidelines for the Implementation of a Quality Management System' in forensic laboratories for analyses is the document that facilitates the implementation of SRPS ISO 17025:2006 (ISO/IEC 17025:2005). The purpose of this document is to provide guidelines for achieving high quality in forensic laboratories using appropriate technology, with a tendency toward its permanent improvement.

The document ILAC G19:08/2014[13] includes entire forensic process and unites standards ISO/IEC 17020:2012 and ISO/IEC 17025:2005. This document defines examination strategy that will be the base of concrete analysis that should be undertaken: requirements of originator, urgency and priority, resources available to the forensic laboratory, tests that have the potential to provide most of the information as a response to originator's requests, limits, and costs, test which has a destructive effect to some subsequent tests and other.

This document emphasizes that personnel in forensic laboratories must have general training on opportunities of available forensic science disciplines for the analysis and examination, which will be the base for the most appropriate method for testing that will be used, as well as the order in the case of multidisciplinary examinations. Laboratories will ensure the existence of documented procedures and training programs in order to cover this aspect of work which will include detailed information about competence, i.e. training of the entire personnel.[14]

Prüm decision[15] on 27th May 2005 in Prüm, seven countries (Germany, Spain, France, Luxembourg, the Netherlands, Austria and Belgium) signed an agreement in the Federal Republic of Germany. In 2008 the Council of the European Union has decided that Prüm agreement becomes legally obliging for all EU Member States.

This Decision obliges EU Member States to strengthen cross-border cooperation, particularly international exchange of information and data. The decision obliges to establish and enable access to the national automatic databases of DNA profiles, databases of fingerprints, wherein the state will ensure the availability of reference data. The availability of personal data and other information relating to the reference data shall be defined by national legislation. The Contracting Parties will enable access to reference data from the automated systems for fingerprints identification wherein the subject cannot be directly identified.[16] Prüm decisions, among other things, provide general regulations on data protection (level of data protection, data processing, accuracy and temporal data storage, technical and organizational measures to protect and to secure data, data subject rights).

Implementation of Prüm decisions will facilitate the exchange of information and experiences between countries of the European Union. Establishment of automated database represents a significantly great challenge within development of information technology. Experts for DNA in ENFSI have prepared a manual for records management of DNA database. It has been established the exchange of DNA profiles, and since 2009 fingerprints records have been linked - AFIS between Germany, Austria, Slovenia and Luxembourg.

Timely access to accurate information and data is a key element that enables successful detection, prevention and management of criminal proceedings. In order to eliminate the lack referring to the absence of a common legal framework for efficient and expeditious exchange of intelligence and information, the Council of the European Union has issued a legally obliging document on simplifying the exchange of information and intelligence data - The Swedish Initiative. The Swedish Initiative 2006/960/JHA regulates requirements regarding:

1) the exchange of information and intelligence;
2) The deadlines for submission of information and intelligence data to the Request for information and intelligence data;
3) the method of communication and language;
4) the protection of confidentiality and withhold of information or intelligence data Articles 8, 9, 10.

The regulations of this Decision (the Swedish Initiative) are transferred to the national legislation of Member States that may conclude bilateral or multilateral agreements and arrangements that will contribute to simplifying or facilitating the process of exchange of information and intelligence data within the scope of enforcement of this Decision. This Decision regulates the forms for exchange and submission of information and intelligence data.

Decision 2008/615/JHA on the enhancement of cross-border cooperation, particularly in combating terrorism and cross-border crime contain regulations that are based on the basic regulations of the Prüm Decision, which are implemented to improve the exchange of information, wherein Member States between each other guarantee the right of access to their automated databases of DNA profiles, dactiloscopic data and data on vehicle registration. This decision is gives possibility to a Member State that in the second

13 ILAC – International Laboratory Accreditation Cooperation
14 ILAC G19:08 /2014 Modules in a Forensic Science Process
15 Decision on interstate exchange of fingerprints and DNA profiles
16 Prüm convention http://register.consilium.europa.eu/doc/

phase of the proceedings requests from another Member State, which manages the database, specific personal data through the procedures for mutual assistance, including those which have been adopted in accordance with the Decision 2006/960/JHA. Submission of personal data to another Member State requires adequate data protection from the Member State that receives them.

With the enforcement of this Decision it will be achieved linking of national databases of Member States, the establishment of a system of data protection, as well as the enhancement of cross-border cooperation, particularly the exchange of information between authorities responsible for preventing and detecting criminal offences of cross-border crime.

Decision 2008/616/JHA on the method of enforcement of the decision 2008/615/JHA determines common normative regulations which are required for administrative and technical implementation of interstate cooperation, particularly with respect to automated exchange of DNA data, dactyloscopic data and data on vehicle registration and other forms of cooperation, which are indicated in Decision 2008/615/JHA. Additional details concerning the technical and administrative enforcement of Decision 2008/615 JHA are indicated in the Annex of this Decision. Member States will take all required measures in order to guarantee the integrity of DNA data, dactyloscopic data, all in accordance with the international standard ISO/IEC 17025:2005.

Decision 2008/615/JHA regarding the enhancement of cross-border cooperation, particularly in combating terrorism and cross-border crime ensured that European Union countries perform more effective exchange of forensic databases. On 30th November 2009, in order to ensure reliability, compatibility and usability of forensic data (for now DNA profiles and fingerprints), from one country to another, the Council of the European Union have made the Decision 2009/905/JHA on accreditation of forensic services in performing laboratory activities. The decision refers to the accreditation of forensic institutions in the countries of the European Union, and regulates that, from 2013, in the Member States of the European Union, in criminal investigations only evidence, obtained in accredited laboratories, can be recognized. If the forensic laboratory is technically and professionally qualified to perform forensic examinations in accordance with international standards, that ensure the quality of work and test results, it would be created the possibility of accreditation of those ones, and for the purpose of laboratory competence, as well as cross-border interstate cooperation in the field of forensics.

"The EU Council Conclusions on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe" (Poland Initiative), which dates from 2011, is an official document of the European Union that, among other things, includes:

– accreditation of forensic laboratories in the European Union;
– consideration of the minimum criteria of personnel competence in forensic laboratories;
– establishment of practical manuals and their use in forensic laboratory practice;
– implementation of international laboratory tests verifiability;
– identification of optimal ways for interstate forensic databases and their use;
– standardization in the field of education and training in the field of forensics;
– se of research and development projects in order to promote further development of forensic infrastructure in the European Union.[17]

ACTIVITIES OF THE REPUBLIC OF SERBIA IN THE PURPOSE OF HARMONIZATION OF REGULATIONS WITH LEGISLATION OF THE EUROPEAN UNION

In order to ensure a high level of security within the states of the European Union, it is necessary to establish cooperation between the Member States, following the principles and rules relating to human rights and the rule of law that are the foundation of the European Union.

In order to harmonize regulations with legislation of the European Union, as well as to achieve an interstate police cooperation, the Republic of Serbia has concluded a number of bilateral agreements with countries in the region related to police cooperation, cooperation in the fight against organized crime, as well as data exchange:

17 Council conclusions on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe, 13 and 14th December 2011

Agreements on the international police cooperation:

– *Police Cooperation Convention for Southeast Europe* which has been signed by the governments of Bosnia and Herzegovina, Moldova, Romania, Albania, Macedonia, Serbia and Montenegro. It involves establishment of cross-border police cooperation and exchange of experts, data exchange and mixed border control. The essence of this convention is close operational police cooperation in the region in order to prevent organized crime.[18]

– *The Agreement on Strategic Cooperation between the Republic of Serbia and the European Police Office* (EUROPOL) was signed in 2008. The purpose of the Agreement is to improve cooperation between European Union Member States, that act through Europol, and the Republic of Serbia in the prevention, detection, suppression and investigation of serious forms of international crime, particularly through the exchange of strategic and technical information;

Police cooperation agreements are concluded with countries in the region:

– *Agreement between the Government of the Republic of Serbia and the Council of Ministers of Bosnia and Herzegovina on Police Cooperation* which determines the exchange of confidential information upon request or without request;

– *Agreement between the Republic of Serbia and the Swiss Confederation on Police Cooperation in the Fight against Crime;*

– *Agreement between the Government of the Republic of Serbia and the Government of the Republic of Croatian on Police Cooperation;*

– *Agreement between the Government of the Republic of Serbia and the Government of the State of Israel on Cooperation in the Fight against Illicit Trafficking*[19].

Agreements on exchange and protection of classified information:

– *Agreement between the European Union and the Republic of Serbia on Security Procedures for Exchanging and Protecting Classified Information* (signed on 26th May 2011 in Belgrade. The Agreement refers to classified information or material in any form and in any field which the European Union and Serbia submit and exchange);

– *Agreement between the Government of the Republic of Serbia and the North-Atlantic Treaty Organization on Security of Information and Code of Conduct*;

The Republic of Serbia has concluded several agreements with this content with the Czech Republic, Slovakia, Bulgaria, Slovenia, Bosnia and Herzegovina and Macedonia. In the preparation are the agreements with Poland, Germany, Italy and Spain. The significance of these agreements reflects in active interstate cooperation in the field of defense, police cooperation, which directly affects international security.

Based on Council Decision 2009/905 EU JHA and the Prüm Decision, as well as the Swedish Initiative, which includes a simplified exchange of information and intelligence data between law enforcement authorities of the Member States of the European Union, there have been defined the requirements in Chapter 24 process of negotiations on the accession of the Republic of Serbia to the European Union, which the Republic of Serbia should accomplish in order to create future successful interstate police cooperation. Screening was completed for Chapters 23 and 24, relating to the judicial system and fundamental rights, freedom, justice and security. Serbia is in the process of preparing action plans that have been set as a standard for their opening.[20] In the process of development is the Action Plan for the Chapter 24 "Justice, Freedom and Security" in the process of joining the European Union.

It is necessary to accomplish obligations relating to the adoption of the Action Plan that will be focused on strengthening human resources and operational capacity for implementation of the various instruments in the field of police cooperation, particularly in combating terrorism and cross-border crime (Prüm Decision) and the Framework Decision 2006/960/JNA on simplifying the exchange of information and intelligence data between law enforcement authorities of the Member States of the European Union (Swedish Initiative) and to evaluate the need for further reform. Development Strategy of the Ministry of Interior of the Republic of Serbia for the period 2011-2016 includes the harmonization of national legislation with the European legislation, the further development of the capacity of the National Crime-Technical Centre, the acceptance of EU standards.

It will be continued with intensive international activities that will be focused on the further implementation of priority reform programs, projects and processes that are already in process in this Ministry, including harmonization of statutes and other regulations in this area with the European legislation.

18 Stajic Ljubomir, Lukic Tatjana, *International and regional cooperation between the competent authorities in detecting and preventing cross-border organized crime* Fighting against crime and European integration (Collection of essays from the First Scientific Conference with international participation, Tara, June 2010), Academy of Criminalistic and Police Studies and Hanns Seidel Foundation, Belgrade, pp. 441-454

19 http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/sporazumi-ugovori.h

20 http://www.euractiv.rs/pregovori-sa-eu/8064-neizvesnost-oko-otvaranja-prvih-poglavlja-published: 19/11/2014.

In the field of forensic science it will be undertaken activities for a timely and rational provision of material and technical resources required for crime scene investigation (finding, securing, fixing, recovering, transporting and storing traces) and performing expertise within all lines of work (forensic medicine, ballistics, traceology, cause of fires, explosions and accidents, manuscripts and documents, identification numbers on motor vehicles, explosives, narcotics and other prohibited substances, toxicology, DNA analysis and forensic acoustics).

Obligations of the Ministry of Interior in the coming period, that have to be accomplished, refers to:

– The implementation of the law on confidentiality of data at the level of the Ministry;

– Development of the Action Plan for the Chapter 24 "Justice, freedom and security" in the process of joining the European Union, that will include the obligations which arise from the European exchange of data and information.

CONCLUSION

In order to implement a Quality Management System in forensic laboratories, some standards and a number of obliging documents of the European Union were adopted. Implementation of international quality standards in forensic laboratories has a great importance for the credibility and validity of material evidences in criminal proceedings, the establishment and exchange of forensic databases, as well as for cross-border cooperation in the fight against international crime and terrorism. Accreditation is a fundamental element and a condition that can be a base for accessing further establishment of a Quality Management System. NCTC of the MOI of the Republic of Serbia was accredited based on standard ISO/IEC 17025. This provides international recognition and exchangeability of the work results with other accredited forensic laboratories and in order to further implement a Quality Management System it was created the condition for the implementation of the series of decisions of the European Union. Accepting the standards and obliging decisions of the European Union, the Republic of Serbia will ensure a successful interstate police cooperation and it will establish quality in every aspect of the forensic process. Based on membership of the Republic of Serbia in international organizations and signed international agreements, and in accordance with national legislation and international commitments, it will be continued with the implementation of a Quality Management System in the field of forensic activities within different lines of work, as well as with interstate exchange of forensic data and information in accordance with authorization and competences in the national legal system and EU standards.

REFERENCES

1. Bjelovuk I., Kesic T., Radosavljevic-Stevanovic N., *The accreditation of forensic laboratories - status and perspectives in Serbia.* Thematic collection of essays *Crime scene investigation of criminal offences* (editor proof. dr. D. Kolaric), Academy of Criminalistic and Police Studies, Belgrade, 2013, pp. 159-172;
2. Council framework decision 2006/906/JHA on simplifying the exchange of information and intelligence data between law enforcement authorities of the Member States of the European Union;
3. Council decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime;
4. Council decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime;
5. Council conclusions on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe 3135th JUSTICE and HOME AFFAIRS Council meeting Brussels, 13 and 14th December 2011;
6. Development Strategy of the Ministry of Interior of the Republic of Serbia 2011-2016, December 2010;
7. *EU Council Framework Decision 2009/905/JHA* of 30th November 2009: Accreditation of forensic service providers carrying out laboratory activities;
8. Guidance for the Implementation of a Quality Management System in Drug Testing Laboratories, United Nations Office on drugs and crime;
9. Gajin S., Matic G., Implementation of Data Protection Act, 10 major obstacles (Collection of essays), 2014; http://cups.rs/wp-content/uploads/2014/08/Primena-zakona-o-tajnosti-podataka.pdf
10. ILAC G19:08/2014 Modules in a Forensic Science Process;
11. Ivanovic Aleksandar, Kazic Jasna, Grbovic Natasa, Forensic institutions accreditation as an imperative of EU Thematic Proceedings of International Significance, International Scientific Conference "Archi-

bald Reiss Days", Vol. I (editor in chief prof. dr G. Milosevic), Academy of Criminalistic and Police Studies, Belgrade, 2013, pp. 1-2, 27-30

12. Ivanovic B. A., *Forensics in the European Union,* Fighting against crime and European integration (Collection of essays from the First Scientific Conference with international participation, Tara, June 2010), Academy of Criminalistic and Police Studies and Hanns Seidel Foundation, Belgrade, pp. 279-288;
13. Ivanovic B. A., Ivanovic P. A., The coordination of forensic work in Serbia and Montenegro with the legislation of the European Union, *Journal of the Department of Legal Sciences of the International University of Novi Pazar, Legal topics,* I year, 2013, no. 1, Vol.1, pp. 21-29;
14. Ivanovic B. A., Ivanovic P. A., Directions of forensic development in the countries of Europe, *Journal of the Department of Legal Sciences of the International University of Novi Pazar, Legal topics,* I year, 2013, no. 2, pp. 170-184;
15. Milosevic M., Bjelovuk I., Kesic T., Quality Management System in Forensic Laboratories, *Science-Security-Police, NBP Journal of Criminalistics and Law*, Belgrade, 2009, Vol.14, no. 2, pp. 1-10;
16. Prüm Convection;
17. *Recommendations* from the report on screening for Chapters 23 (fight against corruption), 24 and an overview of the current situation for Chapter 18;
18. Simovic B., Standardization and accreditation as ways of ensuring professionalism of police and crime investigation units, Security, Belgrade, 2009, vol. 51, iss. 1-2, pp. 236-253;
19. SRPS ISO IEC 17025:2006 General Requirements for the Competence of Testing and Calibration Laboratories;
20. Stajic Ljubomir, Lukic Tatjana, *International and regional cooperation between the competent authorities in detecting and preventing cross-border organized crime* Fighting against crime and European integration (Collection of essays from the First Scientific Conference with international participation, Tara, June 2010), Academy of Criminalistic and Police Studies and Hanns Seidel Foundation, Belgrade, pp. 441-454
21. The program of work of the MOI in 2014;
22. Zarkovic M., Bjelovuk I., Kesic T., Crime scene investigation and credibility of scientific evidence, Academy of Criminalistic and Police Studies, Belgrade, 2012;
23. Zarkovic M., Bjelovuk I., Nesic L., *Scientific evidence and the role of an expert in criminal proceedings: European quality standards*, Fighting against crime and European integration (Collection of essays from the First Scientific Conference with international participation, Tara, June 2010), Academy of Criminalistic and Police Studies and Hanns Seidel Foundation, Belgrade, 2010, pp. 235-244;
24. http://www.enfsi.eu/about-enfsi/structure/working-groups
25. http://www.ats.rs/sr/strane/nadzor
26. http://www.mup.gov.rs/cms_cir/sadrzaj.nsf/sporazumi-ugovori.h
27. http://www.euractiv.rs/pregovori-sa-eu/8064-neizvesnost-oko-otvaranja-prvih-poglavlja-

UDC: 343.982.4(497.6)
340.64:159.925.6(497.6)

CONTEMPORARY TRENDS IN THE AREA OF HANDWRITING ANALYSIS AND POSSIBILITY OF THEIR IMPLEMENTATION IN BOSNIA AND HERZEGOVINA

Muamer Kavazovic[1]
Nebojsa Bojanic[2]
University of Sarajevo, Faculty for Criminalistics, Criminology and Security Studies

Abstract: A modern society reached its peak in the area of information technology, but handwriting is still the most dominant tool of written expression. That kind of expression allows us to determine individual characteristics that are necessary for identification of its author. For a long time, all these facts have been used as a foundation for an idea of creating a handwriting database to resemble fingerprint databases. Therefore, the authors of this article decided to analyze this issue and to determine the possibility of its implementation in local criminalistics - forensic practice. The subject of this work is realization and presentation of capabilities and current achievements within the field of handwriting forensic examination. By utilizing the aforementioned methods, this work aims to outline and present, in the opinion of the authors, all the contemporary achievements that constitute specific contribution to the improvement of this area of expertise in Bosnia and Herzegovina. The reasons for selection of this topic can be identified as an effort towards achieving mandatory modern standards of application of scientific methods and expert procedures for this area of expertise in the procedures of proving and detecting crime and its perpetrators. The goals of our society and our state, in all walks of life, as well as in this particular one, are to reach the standards required for accessing the European Union. With that in mind, it would be necessary to make some improvements, and this work is presenting concrete solutions to this matter through presentation of certain types and models of computer systems and software for handwriting identification. Methods used in this work are: analysis of content, methods of description, classification and specialization.

Keywords: forensic handwriting analysis, handwriting databases, systems for computer identification of handwriting.

INTRODUCTION

Today, handwriting examination presents very important segment of forensics and crime-technical investigations and examinations. Different types of investigations and examinations have been performed in this field of work. In literature and practice a variety of terms are in use for the above mentioned investigations and examinations (different terminology is in use within the countries that were formed after dissolution of Former Yugoslavia and around the world). The most common terms used in Bosnia and Herzegovina are: graphology, graphoscopy[3] and handwriting examination (both criminalistic and forensic examination[4]). Similar situation can be found in other regions of the former country. In our

1 mkavazovic@fkn.unsa.ba
2 nbojanic@fkn.unsa.ba

3 The term graphoscopy is used by Maksimovic and Todoric (1998, p. 489). Beside them, this term is used by the Association of Court Examiners "Forenzika" from Novi Sad http://www.forenzika-novisad.org/oblasti.html (12.11.2014) and the Association of Vojvodina Court Examiners, but they are also using the term graphology http://www.forensicexp-vojvodina.org.rs/clanovi-novac (12.11.2014). It is necessary to emphasize that this variety of terms is caused by inadequate knowledge of the legal bodies that are implementing afore mentioned terms in a wrong manner into the laws regulating this area of expertise or forensics of handwriting and documents. It is well known fact that graphology is the border science, dealing with psychology and determining personal characteristics based upon handwriting (Krstic, 1999, p.11, Gardner, 1995. p. 7., Wadel, 2000, and Graphology – graphoanalysis, http://skepdic.com/graphol.html (22. 02. 2007.). Also, it is very interesting to emphasize the opinion that graphology is paralinguistic (Esnoseso, 1989, p.21). According to these facts, we can state that graphology is suitable tool, used when there is a need to perform a profiling of the perpetrator.

4 This prefix does not have sources in our literature. It is used in our practice that adopted the term forensics (for the purpose of the usage by the court, from the Latin word *forensis*) for all the tasks that are related to the criminalistic examinations, and that were in past part of crime-technical field. From the international arena, we will mention an example of American Society for Testing and Materials (ASTM) that provided the standard job description for forensic document examination (including handwriting) in their document E.444-79. Furthermore, that document is listing all the requirements for the individual performing that work, and making a clear distinction between forensic handwriting examination, calligraphy, transcription and graphology (Huber R.A.-Headrick A.M., "Handwriting Identification-Facts and Fundaments", Boca Raton, New York, 2000., p. 8. and 9.). Also, Safferstein (2007, p.498) is using

opinion, the most adequate term should be handwriting and documents forensics or examination of handwriting and documents, considering the fact that these terms are specifically meant to be used by judicial sector, in order to clarify extralegal issues. Taking all the things into consideration, it is necessary to emphasize that terms graphology or graphoscopy are not the most adequate ones from the criminalistics perspective, since these two terms do not include documents examinations that are not part of handwritings. Sabol[5] is sharing the similar opinion.

Beside the aforementioned issues, and especially if we take into consideration the lack of expert literature in local languages (small number of published books that are related to these topics), as well as non-standardized methods of training and experts certification in this area of work,[6] it is noticeable that in practice,[7] while performing this type of examination, experts are not using always and in all cases identical, scientifically determined methodological findings on rules and scopes of this type of examination (rules of profession). This particular issue is causing differences in final conclusions (opinions) of the examiners and communication confusion among prosecuting bodies and experts.

The main reason for selection of this topic is our goal to achieve European and world standards[8] regarding the application of scientific methods and expert hypothesis for this area of expertise, during the process of discovering and proving the criminal activities and perpetrators. The goals of our society and the state, in all areas of life, as well as in this one, are the achievement of actual level that is necessary for accession to the European Union. Taking this into consideration, it would be necessary to make the appropriate steps forward in this area of work.

First of all, that would be acceptance of the necessary standards that are related to methodological hypothesis and frameworks, that are prerequisites for membership, of our expert institutions and experts from this field of work in appropriate expert associations and institutes (within the EU as well as associations within the USA). It is especially important to emphasize and to integrate world achievements that were accepted long time ago, related to terminology, unified standards of training for experts and quality control of their work.[9] All the aforementioned is supervening from unique theoretical and methodological framework that this field of expertise should have. All of this is generally accepted and codified in all developed countries in the world, but in our country (in many cases) it is not.

All these theses that we mentioned require broader and more in depth approach and the goal of this work is to present and to promote scientific and technical achievements in this field of work, in the last 30 years and for which the implementation in BH we still do not have necessary prerequisites. The authors would like to emphasize and explain the necessity of raising this field of work to the international scientific standards, as well as their acceptance and implementation in a daily work by the experts from this field of work. Implementation of the above mentioned standards would assist in achieving the highest level of objectivity with this type of examinations, and it would reduce the possibility of different mistakes, so called factor of subjectivity (non-scientific elements of examination). This is very important since the number of these types of examination is constantly increasing.

When we are talking about new achievements that are related to this field of forensic handwriting examinations, two things are of the most importance.

First one is related to forming of specific handwriting collections according to predetermined methodology, and their usage for handwriting examinations and determination of the scirptor identity, when there

terms examination of handwriting and documents, with a basic goal of determining authenticity of handwriting and documents. The same opinion is shared by Fisher (1993, p.123), who is comparing handwriting with fingerprints or dactiloscopy. He believes that these two areas of expertise have the same value in determining the identity of a certain person.

5 Sabol, Z. (1986), p.12

6 In practice within Bosnia and Herzegovina, there is no unified training, nor expert certification for handwriting examination. Every institution that is performing this type of examination has its own training programs and methods of verification of acquired knowledge. Before 1992, that was performed by one institution, so the training and certification process was unified for the whole territory of Bosnia and Herzegovina. Recently, during the process of court examiners selection for this area, it was introduced a special professional exam, in accordance with the Law on Court Experts, at the level of entity Ministries of Justice (Articles 7-9, Law on Court Experts of Federation of Bosnia and Herzegovina, Official Gazette of Federation of Bosnia and Herzegovina, No. 49/05 and 38/08; Articles 7-9, Law on Court Examiners of Republika Srpska, Official Gazette of Republika Srpska, No. 16/05 and 16/08).

7 In court practice, there were cases of selected experts that were not following the basics norms regulated for this area of expertise (for example, some experts were providing final opinions based on the examination of photocopied materials). This is the result of the fact that, in practice, the title of expert was given to the individuals that did not have even the basic training for this area of expertise or they had inadequate training (in any form). Also, in the District of Brcko of Bosnia and Herzegovina, there is a professional exam regulated by the Law, and selection of the court experts is performed based on the analysis of submitted documents for every applicant.

8 For example, DeForest, Gaeenslen and Lee (1983:369) are stating that in standard examination of handwriting, two more general standards are important (1) collection of handwriting, and (2) searching for handwriting. This means the collection of standard samples written before the criminal act took place, and standard samples after the criminal act has been committed, written by dictation, using the same type of paper, same size of paper, same writing tool, same type of ink or similar, if it is possible.

9 Norms based on historical, scientific and experientially development of this area of expertise, given in the appropriate literature, and in the recent historical period, regulated by appropriate instructions and recommendations of scientific institutions dealing with this type of work, as well as from appropriate expert working groups within professional associations. For example: ENFSI (European Network of Forensic Science Institutes), AAFS (American Academy of Forensic Science), ASQDE (American Society of Questioned Documents Examiners) or afore mentioned (footnote 1) ASTM (American Society for Testing and Materials).

is no suspect. The essence of these collections is in the possibility of finding the scriptor from the handwriting specimens that were collected earlier. An appropriate methodology is required for maintenance of these collections.[10] These collections are maintained for the individual types of criminal activities (handwriting collections of individuals that committed criminal activities or in a different ways can be related to these activities, such as: terrorism, homicides, sexual delicts, etc.). For the purpose of better understanding, these collections can be compared (according to the method of collection and maintenance) with so called monodactiloscopic and decadactiloscopic collections in fingerprint examination and identification arena.[11]

The second achievement is related to the constant striving to make the criminalistic handwriting examination more objective, or maybe it is better to say to have possibility to present the results of this examination in more exact manner. It is well known factor that this type of examination is dominated by the so called factor of subjectivity,[12] or personal observation of the individual that is performing it, the expert. Because of that factor, there was a need to develop an appropriate cybernetic (computer) methods and means that would be used with this type of examination. This achievement is the key element of this work, considering the modern strivings to embed two functions: electronic storing of handwriting collections, or samples, and usage of an appropriate computer programs for comparative examination of the handwriting and certain handwriting characteristics, supported by the computer system, for so called automatic identification of the scriptor. For the better understanding, this can be compared with the functioning of the AFIS system for fingerprint identification. It is very important to emphasize, that for now, these systems cannot provide an automatic identification, but instead the main burden of identification is still on an expert – the operator of that system.

These tendencies are not some novelty in the modern world, but in our country that is still unknown fact, and the usage of the aforementioned systems, in this environment, is practically impossible.

Our goal is not to present all modern technical achievements that are characteristic for this kind of examination, and that are the result of historical development of this area of work, as well as other scientific and technical achievements. We will present just certain achievements that are, according to the opinion of the authors, true advancements and in the certain way milestones for this kind of examinations. The development of these methodological and technical achievements is still not finished, and it is quite correct to state that they will be further advanced in the future.

As an example of the aforementioned possibilities, we will present brief description of the handwriting collections maintained according to the MALLY system; system of the computer examination of the handwriting called FISH; and system of the computer examination of handwriting called WANDA. All these systems will be subject of such an analysis that is possible to be presented in this work. These systems were developed in the Forensic Institute BKA (Bundeskriminalamt) in Wiesbaden. We will also present the software package for handwriting analysis that is available at the market and it is produced by the CEDAR TECH Company.

CLASIFICATION SYSTEM MALLY

The first steps of this classification were made back in 1942. The system, in the current form, was defined and implemented by the Forensic Institute BKA in 1950. Since then, it is named after the BKA officer Rudolf Mally, who developed this scheme and gave it a practical form.[13]

The principle of work of this system is based on the collection method of the questioned material from the province criminalistic offices (Landeskriminalamt – LKA) and its submission to Forensic Institute BKA in Wiesbaden, where this material is being classified by the MALLY system, and in that way it created some sort of the central collection.

10 The Law on Police Officials of Federation of Bosnia and Herzegovina regulates the maintenance of registers and collections in Article 34, Paragraphs 1 and 2, so we can state that there is a legal base for maintaining these collections. Law on Police Officials of Federation of Bosnia and Herzegovina, No. 27/05.

11 AFIS system is based upon certain basic settings of these collections. Furthermore, collection based on MALLY system is the foundation for later developed electronic system FISH.

12 In reference to this, we can agree with Simonovic (2004) who is sharing Hecker's opinion (1993) that the problem is that handwriting is relatively stable and with its variables, criteria for examination and applied methods cannot be completely objective and extracted from subjective elements. But, it is possible, during the process of comparison of standard and questioned handwriting, to have positive or negative final opinion on the identity of the hand, actually the individual that was writing that text. Furthermore, the authors are stating the problems of self-education of the experts that are relying on their own knowledge, experience, technical equipment and improvisation, without having standard training with elements of certification.

13 BKA, »Methodenbeschreibung Handschriften-Klassifizierung, Klassifizierungsystem nach Mally-Handbuch«, Wiesbaden 2001.

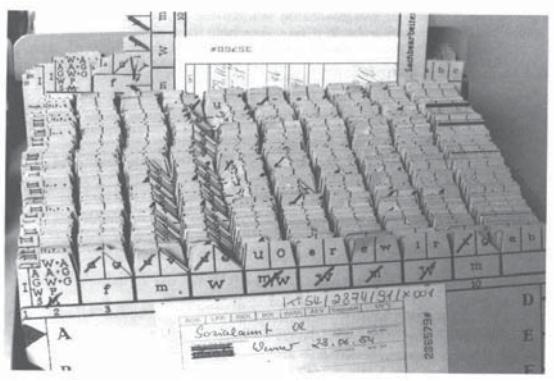


Figure 1 *Collection of handwriting based upon MALLY classification system*[14]

MALLY system is based on the classification of certain handwriting characteristics, and derivation of the handwriting formulas from that. Acquired results – handwriting formulas, together with handwriting, are then being put on appropriate cards, forms (specimen cards), and stored and kept in that manner. These cards are practically the backbone of this system.

This classification system provides us with the possibility to divide the acquired information based on the gender of the scriptor, and colour coded cards are being used for this purpose.

For the classification purpose, certain handwriting characteristics can be used:[15]

- handwriting method;
- method of letter connection;
- sub-method of connection;
- the degree of the letter connection;
- alignment and formatting;
- curves within the handwriting;
- position of the writing;
- letter size;
- distinctive punctuation.

Handwriting style is one more criterion for classification. The difference is determined between cursive writing, all capital letters, block letters and combination (the manner of graphic expression.)

The handwriting that is classified in the aforementioned manner is being described with appropriate formulas and recorded on the specimen cards. This method is providing an easier way of finding the handwriting that can match the questioned sample.

All the originals are kept in collection of the Forensic Institute, handwriting examination department of BKA, and are available only during the court process.

Handwriting specimens are kept in the central collection, in accordance with the rules regulating the method of storing the personal documents by the police. The maximum length of this storing can be 10 years.[16] After the period of 10 years, documents are being removed from the collection, unless the certain specimen can be related with the criminal activity committed within this time range.

SYSTEM FOR COMPUTER IDENTIFICATION OF HANDWRITING FISH

The abbreviation FISH is created from the first letters of the words in German language: *Forensiscches* - forensic, *Informations* - information, *System* - system and *Handschriften* - handwriting.

According to Hecker, the development of the FISH project was started in 1971 by Manfred Hecker. His interest for this kind of the system was stimulated by the publication by Stein-Lewinson (1942 and 1973),

14 BKA, »Methodenbeschreibung Handschriften-Klassifizierung, Klassifizierungsystem nach Mally-Handbuch«, Wiesbaden 2001.
15 BKA, »Methodenbeschreibung Handschriften-Klassifizierung, Klassifizierungsystem nach Mally-Handbuch«, Wiesbaden 2001.
16 BKA, »Methodenbeschreibung Handschriften-Klassifizierung, Klassifizierungsystem nach Mally-Handbuch«, Wiesbaden 2001.

Eden (1962), Kosintz and others (1966) and Lanzmann (1965, 1966, 1967 and 1968). The significance of Stein-Lewinson formulation is in the quantity and the quality aspects of handwriting. Quantity aspect – the handwriting is being observed as geometric shape with measurable characteristics; quality aspect is taking into consideration individual handwriting characteristics related to the shape and the movement.[17] The problem that the author faced was the exclusion of the subjective element during the process of determination of individual handwriting characteristics. Meaning, if it would be possible to exclude this element, and if only pure computer based method of objective analysis of geometric shapes was used, then it would be possible to use, not just the quantity individualization of handwriting for forensic purposes, but also the general statistical analysis with the large scriptor population. The result would be the significant amount of individual characteristics that would assist us in understanding the complexity of these characteristics.

Form the original list of characteristics by MALLY, that were used for classification, parameters such as width, height and upper length (length separation) position of the letters and the loop type were taken.[18]

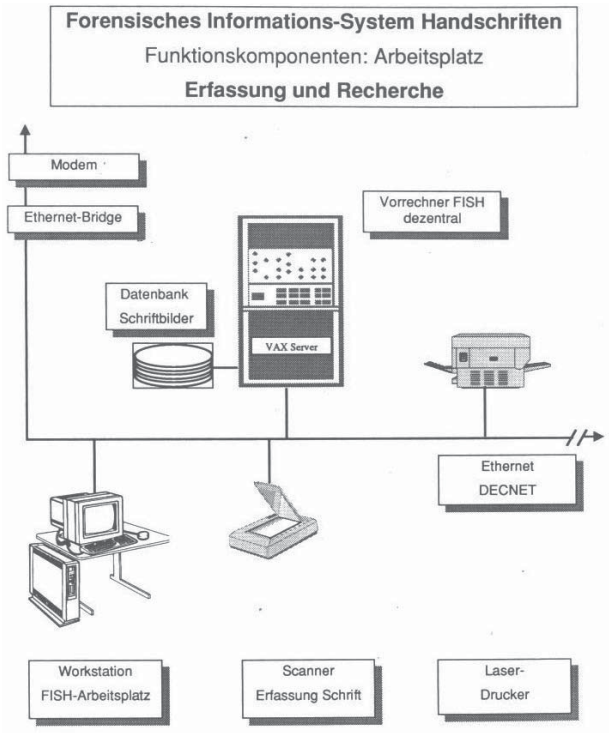


Figure 2 *Scheme of the work station of FISH system*[19]

Figures 3, 4 and 5 show the handwriting characteristics that are the foundation for handwriting identification of the FISH system.

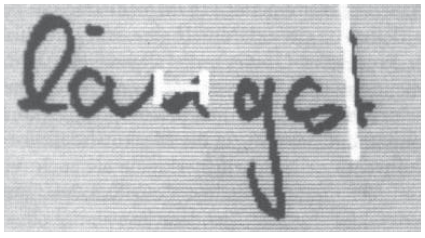


Figure 3[20]

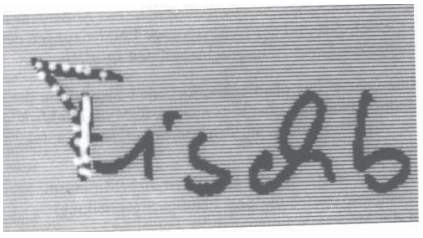


Figure 4[21]

17 Hecker M., „Forensiche Handschriften-untersuchung", Heidelberg 1993.
18 Hecker M., „Forensiche Handschriften-untersuchung", Heidelberg 1993.
19 Hecker M., „Forensiche Handschriften-untersuchung", Heidelberg 1993., p. 327.
20 Hecker M., „Forensiche Handschriften-untersuchung", Heidelberg 1993., p. 316.
21 Hecker M., „Forensiche Handschriften-untersuchung", Heidelberg 1993., p. 317.

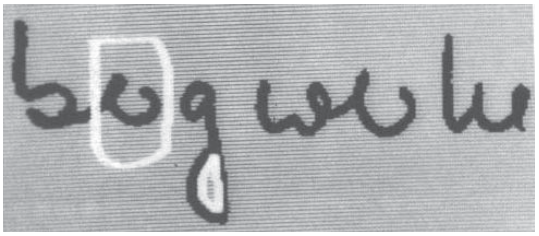


Figure 5[22]

SYSTEM FOR COMPUTER IDENTIFICATION OF HANDWRITING WANDA

This system is observed as the successor of the system for computer identification of handwriting FISH. Computer aided identification of the scriptor, based on digital handwriting sample, is very challenging task for recognition of the sample. Numerous systems are being used in Europe, the USA and Australia. In order to create an environment for international exchange, it was suggested to develop standardized approach for storing and exchanging of application for analysis and evaluation of procedures for forensic identification of handwriting. WANDA system is the result of that desire.[23]

The main goal is creation of useful and efficient platform for forensic identification of the scriptor, and that means:

1) Standardization of data format;

2) Harmonization of the components and possibility of upgrading the system concept, and

3) Objectiveness of the measurements and reliability of the results of analysis.

When we talk about standardization of data format, it is very important to emphasize, that it is related to the possibility of using the data from different sources (data exchange). It is very important for these data to be compatible, therefore it is necessary to use identical or comprehensible format.

Objectivity of the measurement implies that program, which is the foundation of the system, and the system components provide the objective measurement of certain handwriting characteristics. At the same time, reliability of result analysis should imply the correctness of the performed analysis. In this case, we can discuss just about the reliability of the manner for data processing, but not about correctness of the final results.

Configuration of the components that are part of this system must be adequate for the possibility of upgrading (if there is a need for that), and reducing the original capacity of the system itself.

During the classic process of forensic examination, an expert – human being is performing handwriting comparison, based upon well defined set of characteristics. As in other areas of forensic science, handwriting examination, as well, is primarily based upon the knowledge and experience of the forensic expert. Due to the problems of non objective measurement and non reproductive decisions, it was attempted to support traditional methods (such as visual observation and expert evaluation) with semi-automatic and interactive systems. The subject of computer based forensic examination of handwriting is the sample of human handwriting that is transferred into digital form using electronic pad and electronic pen.

WANDA provides us with possibility to use different formats - software packages of images for data entries. Besides that, this system is capable of processing general data, data filtering, classification and extraction of data based on given characteristics. Furthermore, it is not requested to predefine application domain, the flow of processing and data structure.

22 Hecker M., Forensiche "Handschriften-untersuchung", Heidelberg 1993, p. 319.

23 Franke K., Schomaker L., Veenhuis C., Taubenheim C., Guyon I., Vuurpijl L., Van Erp M, Zwarts G., » WANDA: A Generic Framework applied in Forensic Handwriting Analysis and Writer Identification«, source: http://www.kyfranke.org/uploads/Publications/franke03d.pdf, taken 22.10.2014.

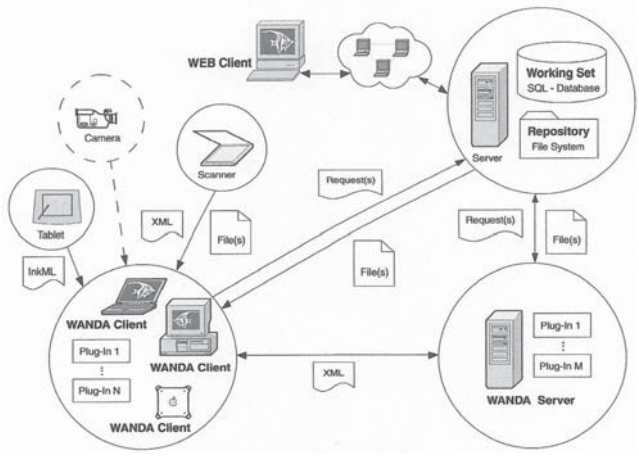


Figure 6 *System architecture and individual parts of the WANDA system*[24]

System server is implemented in JAVA program language and it is compatible with the following operating systems: Linux RedHat, Windows 2000 and MacOS X.

Recommended data-image format is Target Image File Format (TIFF).

SYSTEM FOR COMPUTER IDENTIFICATION OF HANDWRITING CEDAR FOX

CEDAR FOX system is computer supported program created to assist with handwriting identification. This system was developed in 1978, by American company CEDARTECH. Numerous experts from this field of work were involved in the development of this system, as well as computer experts for New York University and National Institute of Justice.[25] In certain phases, support was given by the DBI experts, as well. Original version of this system was upgraded numerous times.[26]

This system is used during the comparison process of standard and questioned samples of handwriting. During this process, the system uses certain graphometric settings related to general handwriting characteristics (angles, connections, etc.) and certain specific handwriting characteristics (shape of the letters and method of writing certain elements). It is possible to use this for the specific parts of the document being examined, where we have questioned handwriting, or it can be used for the whole document. The system is using two processes: (1) comparison of the questioned document-handwriting with concrete standard document-handwriting, and (2) comparison of the questioned document-handwriting with larger number of standard documents-handwritings that are stored in the data base of this system. These processes can be used also for signature examination. System is based on the software for processing of the digital images through computer scanning of the handwriting elements. In most of the cases, for the comparison within the standard and questioned samples, identical or similar parts of the handwriting-words are being selected. System is based on partial processing of data-images by the user (this process includes labelling of the parts of handwriting that are interesting for comparison, improving the image quality, removal of the lines in the background, etc., while the processing of the similarity and differences of given images is performed by the system-computer itself with the assistance of computer program. Also, the results of the search-comparison include an appropriate computer based statistical ratio that can imply the results of comparison, recognized by the system.

One big advantage of this system is that this program can be installed on every computer that is supported by standard Windows operating system, without some extreme performances of the computer itself.

The following images show the screen-shots of certain parts of the work process of this system.

24 Franke K., Schomaker L., Veenhuis C., Taubenheim C., Guyon I., Vuurpijl L., Van Erp M, Zwarts G., » WANDA: A Generic Framework applied in Forensic Handwriting Analysis and Writer Identification«, source: http://www.kyfranke.org/uploads/Publications/franke03d.pdf, taken 22.10.2014.

25 James, S.H., Nordby, J.J. (2005), Forensic Science, An Introduction to Scientific and Investigative Techniques, Boca Raton, Singapure, Taylor & Francis, p. 429.

26 "Cedar-Fox A Computational Tool for Questioned Handwriting Examination", source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.

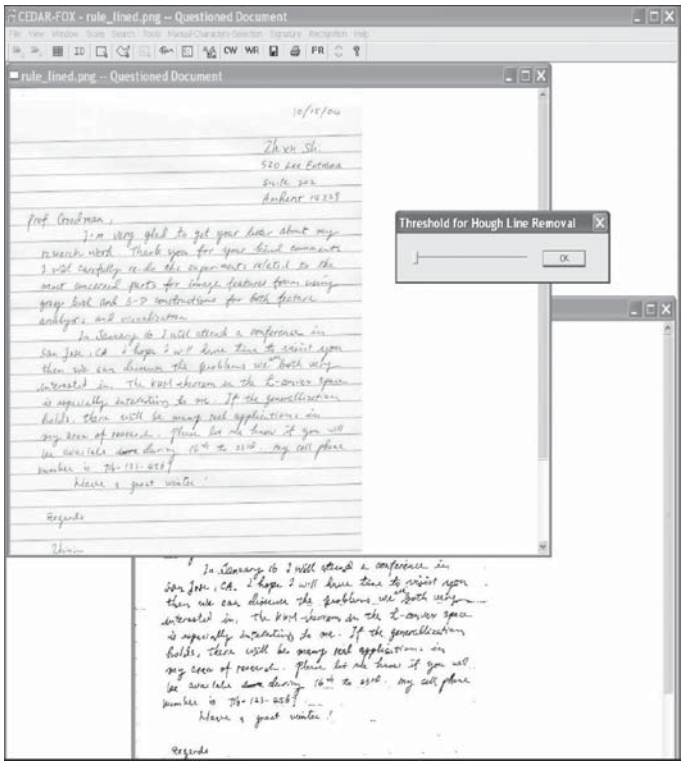


Figure 7[27]

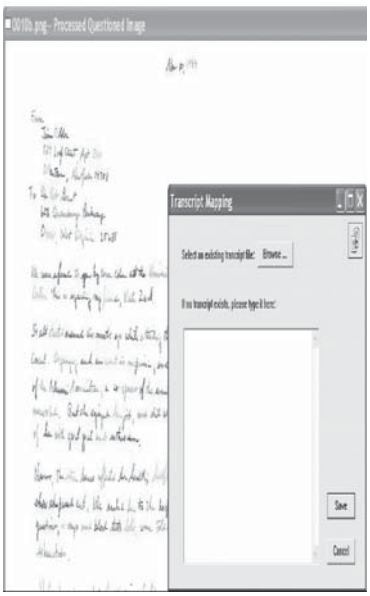


Figure 8[28]

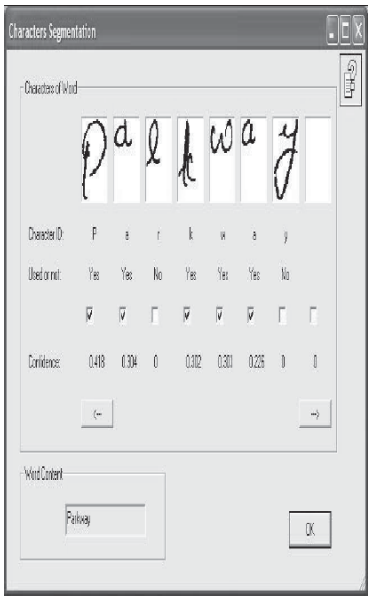


Figure 9[29]

27 "Cedar-Fox A Computational Tool for Questioned Handwriting Examination", source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.
28 "Cedar-Fox A Computational Tool for Questioned Handwriting Examination", source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.
29 "Cedar-Fox A Computational Tool for Questioned Handwriting Examination", source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.

Figure 10[30]

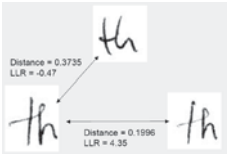


Figure 11[31]

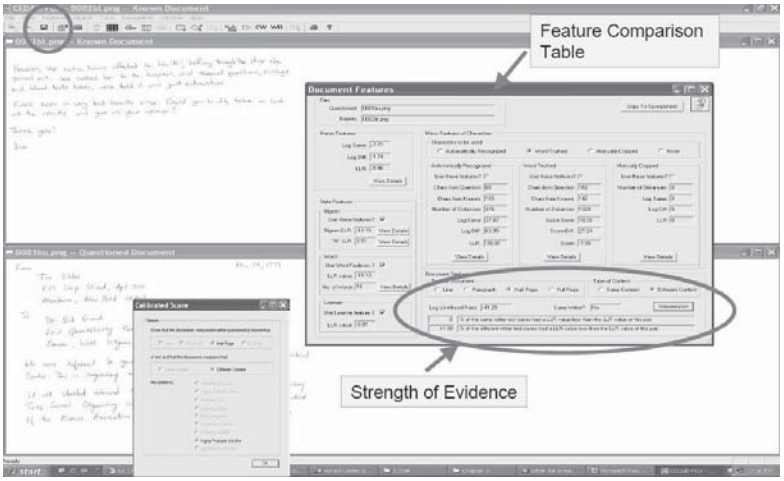


Figure 12[32]

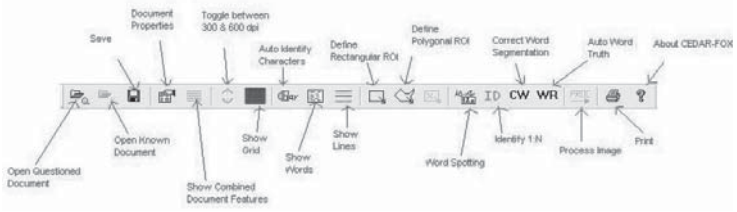


Figure 13 *Toolbar of the computer program of CEDAR FOX system*[33]

30 "Cedar-Fox A Computational Tool for Questioned Handwriting Examination", source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.
31 "Cedar-Fox A Computational Tool for Questioned Handwriting Examination", source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.
32 "Cedar-Fox A Computational Tool for Questioned Handwriting Examination", source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.
33 "Cedar-Fox A Computational Tool for Questioned Handwriting Examination", source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.

Analyzing the available material, objectively speaking, this system is an assisting tool that can be used for examination of handwriting and signatures. This system is valuable only in the case it used by trained experts and if they are using and performing the evaluation of results (this is general evaluation of this kind of systems). It is very important to emphasize that this system cannot replace the trained expert. Additional advantage of this system is that the positive results of the comparison (tables, statistical ratios, images, etc.) that are confirmed by the expert, can be used as objective evidence in court (this is very important advantage due to the fact that these examinations are considered the most subjective type of examinations, and the aforementioned facts-indicators contribute to the objectiveness of these).

Currently, there is no formal training for usage of this system. During the development phase, this system was tested by several police and other state agencies, such as the FBI Forensic Laboratory, the Canada Border Agency and the United States Secret Service – USSS. The results of this testing were presented at the ASQDE conferences (The American Society of Questioned Document Examiners). The fact being emphasized is that the development of this system is a constant process and the upgrades are being implemented quite often.[34]

At the end, it is very important to emphasize that this system is functioning on similar settings as FISH and WANDA systems, and the systems created for the analysis of other biometric data such as fingerprint system AFIS.

POSSIBILITY OF IMPLEMENTATION OF COMPUTER SYSTEMS FOR HANDWRITING INDENTIFICATION IN BOSNIA AND HERZEGOVINA

In order to present the possibility of using these systems in Bosnia and Herzegovina, it is necessary to perform the analysis of legal prerequisites for usage of such systems in the states where these systems were tested and used. There is a large number of practical prerequisite for usage of these systems. Considering the fact that our country has tendency to join the European Union, it is necessary to harmonize the experience related to the legal frame for using these systems, with the experience of the European Union. All of the aforementioned is related to the procedures of collecting and entering data, time frame for storing these data and the manner of that storage, actually the practical protection of personal data that will be the subject of processing. In our case, the only difference with legal procedures of the EU state members is the time frame for storing the biometric data (in our legal system there is no concrete time frame). In the European Union, there are strict legal procedures for storing these data, or deleting the biometric data, depending upon the length of the sentence for concrete criminal activity performed by the individual whose biometric data are the subject of the process.

At the same time, we would like to initiate the discussion related to certain problems we can face during the process of handwriting examination and collection of the standard handwriting samples, because our legal practice and legal experts do not provide concrete solutions and instructions, but try to deal with this through broader process solutions.

The issues related to the handwriting samples (questioned and standard) are not explained in Criminal Procedure Code in Bosnia and Herzegovina (CPC of BH[35], CPC of F BH[36], CPC of RS[37] and CPC of

34 "Cedar-Fox A Computational Tool for Questioned Handwriting Examination", source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.

35 Criminal Procedure Code of Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina No: 3/03 from 10.02.2003., effective from 01.03.2003. Correction of the Law, Official Gazette of Bosnia and Herzegovina No: 32/03, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 36/03, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 26/04, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 63/04, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 13/05, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 48/05, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 46/06, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 37/03, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 76/06, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 29/07, Law on adopting the changes of Criminal Procedure Code, Official Gazette of Bosnia and Herzegovina No: 32/07, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 53/07, Law on adopting the changes of Criminal Procedure Code, Official Gazette of Bosnia and Herzegovina No: 76/07, Law on adopting the changes of Criminal Procedure Code, Official Gazette of Bosnia and Herzegovina No: 15/08, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 58/08, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 12/09, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 16/09, Changes and amendments, Official Gazette of Bosnia and Herzegovina No: 93/09 and Law on adopting the changes of Criminal Procedure Code, Official Gazette of Bosnia and Herzegovina No: 72/13

36 Criminal Procedure Code of Federation of Bosnia and Herzegovina No: 35/03 from 28.07.2003., changes and amendments Official Gazette of Federation of Bosnia and Herzegovina: 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09 and 12/10

37 Criminal Procedure Code of Republika Srpska, Official Gazette of Republika Srpska No. 53/12.

BDBH[38]), but it can be interpreted through certain general decision. Generally speaking, in our country, force cannot be used during the collection of standard handwriting samples. This means, if a person does not want to write the dictation, there is no way to force it. In that case, the only possible solution is to use handwriting samples of that person written in the past (if we can be provided with such samples and if these samples are of satisfying quality and quantity standards).

With all these facts in mind, it is possible to understand certain legal problems that we can experience, if we try to implement MALLY, FISH, WANDA or similar systems in Bosnia and Herzegovina.

First of all, the basic prerequisite for the implementation of these systems would be the existence of central forensic institution at the state level that would process all submitted handwriting samples. Current organizational chart of police and security agencies includes the Agency for Forensic Expertise of Bosnia and Herzegovina,[39] as an independent unit within the Ministry of Security of Bosnia and Herzegovina that would be able to perform the function of the center in case of implementation of these systems. In this case, the problem is that this Agency is not fully functional, and some legal issues can appear if this Agency becomes the center of activities related to forensic examination within Bosnia and Herzegovina (such as, jurisdiction, vertical coordination, standardization, training, quality control, storing, using and exchange of data related to forensic examination, etc.) At the same time, it would be necessary to change and improve legal acts and bylaws defining the category of individuals whose standard handwriting samples would be collected and stored in appropriate data base (either changing the Criminal Procedure Code or passing a new law that would regulate this area). Also, it is very important to act in accordance with the Law on Personal data Protection.[40]

Furthermore, it would be necessary to adequately define by Criminal Procedure Code of Bosnia and Herzegovina and its Entities, certain procedural issues related to the handwriting examination and the manner of collecting the handwriting samples. The question that can be posed is: is the suspect obliged to provide us with handwriting sample; or, can we understand the refusal of that individual to write by dictation as his/her right to remain silent or his/her right not to answer the questions except on his identity; or during the procedure of collecting the standard handwriting samples from suspect we should apply the Criminal Procedure Code decisions related to, for example, collection of fingerprints for examination, DNA samples or photographs. Legal bodies did not provide us with the official decision on this matter.

Also, it would be necessary to find a legal solution and interpretation of the legal base for maintaining the collection of standard handwriting samples.

Besides all this, if we decide to implement such systems, it would be necessary to have physical prerequisites, such as providing adequate computer equipment, training of the personnel and providing a budget for software licenses or acquiring the permit to use these systems.

After all, it is also very important to have adequate personnel for the implementation of these systems. This means the sufficient number of people for such examinations within the systematization of appropriate agencies, their adequate training to work on these systems, as well as concentrating the highest quality people in forensic department. Also, it would be important to pass written procedures for work and mutual relations of departments in the chain that is necessary for functioning of these systems.

CONCLUSION

Implementation and usage of computer systems for handwriting identification in Bosnia and Herzegovina at the moment is not a realistic option. Considering the volume of work (number of cases with unknown perpetrator), the cost of investment, as well as necessary number of experts and other personnel that would work on these tasks, the implementation of electronic systems for handwriting identification in Bosnia and Herzegovina is not the project that would be paid off, nor the task that can be accomplished. Upon the analysis of necessary parameters, we may consider the possibility of implementation of these systems on regional level.

In case that in the near future we start with the implementation of these systems, it would be necessary to perform adequate changes of laws and bylaws (instructions, procedures, Memorandums of understanding, adequate book of rules, etc.)

38 Criminal Procedure Code of District of Brcko of Bosnia and Herzegovina, Official Gazette of District of Brcko No: 10/03 from 01.08.2003, changes and amendments, Official Gazette of District of Brcko: 48/04, 06/05, 12/07, 14/07, 19/07, 21/07, 02/08, 17/09, 44/10 and 27/14

39 Established and functioning in accordance with the Law on Directorate for Coordination of Police Bodies and of Agencies for support of police structure in Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina: 36/08

40 Law on Personal Data Protection of Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina: 49/06 from 27.06.2006., changes and amendments, Official Gazette of Bosnia and Herzegovina:76/11 and 89/11

At the same time, usage of specialized programs for handwriting analysis in Bosnia and Herzegovina is quite realistic and possible. The cost is not too high, and these programs contribute to more objective results of certain segment of examination, and experts using these programs will be provided with the possibility of easier explanation of certain segments of their work and results, as well as better understanding by other official involved in this process.

It is very important to emphasize that this is based upon graphometric principle, that does not take into consideration all elements for handwriting identification (possible handwriting variation of the same scriptor), and usage of these programs is just an additional tool for experienced and trained experts who are link and needed for complete and quality procedure of identification.

REFERENCES

1. BKA, (2001), "Methodenbeschreibung Handschriften-Klassifizierung, Klassifizierungsystem nach Mally-Handbuch", Wiesbaden
2. De Forest, P.R., Gaensslen, R.E., Lee, C.H., (1983), Forensic Science An Introduction to Criminalistics, McGraw-Hill, Series and Criminology and Criminal Justice, New York, Toronto.
3. Ellen D., (1997), "The Scientific Examination of Documents, Methods and Techniques", London.
4. Fisher, A.J.B., (1993), Techniques of Crime Scene Investigation, 5ft Edition, Boca Raton, London, CRC Press.
5. Hecker M., (1993) "Forensiche Handschriften-untersuchung", Heidelberg.
6. Huber R.A.-Headrick A.M., (2000), "Handwriting Identification-Facts and Fundaments", Boca Raton, New York.
7. Esnoseso, F. (1989) „Grafologija", Nova Vest, Novi Sad.
8. Gardner, R. "Fast Handwriting Analysis" („Analiza rukopisa na brzinu"), Andrijići d. o. o., Korčula.
9. James, S.H., Nordby, J.J. (2005), Forensic Science, An Introduction to Scientific and Investigative Techniques, Boca Raton, Singapure, Taylor & Francis.
10. Krstić, J., (1999), "Grafologija", Izdavač Autor, Beograd.
11. Maksimović, R., Todorić, U., (1995) „Kriminalistika Tehnika", Policijska akademija, Beograd.
12. Sijerčić-Čolić H., (2008), "Krivično procesno pravo", Knjiga I, Pravni Fakultet, Sarajevo.
13. Sabol, Ž. (1986), "Identitet rukopisa", Informator, Zagreb.
14. Simonović, B. (2004) „Kriminalistika", Pravni fakultet, Kragujevac.
15. Wadel, B. (2000), Write Living", New York.
16. Law on Directorate for Coordination of Police Bodies and agencies for support of police structure in Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina No: 36/08
17. Criminal Procedure Code of Bosnia and Herzegovina, Official Gazzette of Bosnia and Herzegovina No: 3/03 from 10.02.2003., effective from 01.03.2003. Correction of the Law, Official Gazzette of Bosnia and Herzegovina No: 32/03, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 36/03, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 26/04, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 63/04, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 13/05, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 48/05, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 46/06, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 37/03, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 76/06, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 29/07, Law on adopting the changes of Criminal Procedure Code, Official Gazzette of Bosnia and Herzegovina No: 32/07, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 53/07, Law on adopting the changes of Criminal Procedure Code, Official Gazzette of Bosnia and Herzegovina No: 76/07, Law on adopting the changes of Criminal Procedure Code, Official Gazzette of Bosnia and Herzegovina No: 15/08, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 58/08, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 12/09, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 16/09, Changes and amendments, Official Gazzette of Bosnia and Herzegovina No: 93/09 and Law on adopting the changes of Criminal Procedure Code, Official Gazzette of Bosnia and Herzegovina No: 72/13
18. Criminal Procedure Code of Distric of Brcko of Bosnia and Herzegovina, Official Gazzette of District of Brcko No: 10/03 from 01.08.2003, changes and amendments, Official Gazzette of District of Brcko: 48/04, 06/05, 12/07, 14/07, 19/07, 21/07, 02/08, 17/09, 44/10 and 27/14

19. Criminal Procedure Code of Federation of Bosnia and Herzegovina No: 35/03 od 28.07.2003., changes and amendments Official Gazzette of Federation of Bosnia and Herzegovina: 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09 i 12/10
20. Cirminal Procedure Code of Republika Srpska, Official Gazzette of Republika Srpska No. 53/12 from 11.06.2012.
21. Law on Police Officials of Federation of Bosnia and Herzegovina, Official Gazette of Federation of Bosnia and Herzegovina, No. 27/05.
22. Law on Experts of Federation of Bosnia and Herzegovina, Official Gazette of Federation of Bosnia and Herzegovina, No: 49/05 from 08.08.2005. and Official Gazette of Federation of Bosnia and Herzegovina, No: 38/08 from 25.06.2008.
23. Law on Experts of Republika Srpska, Official Gazette of Republika Srpska No: 16/05, 16/08
24. Law on Personal Data Protection of Bosnia and Herzegovina, Official Gazzette of Bosnia and Herzegovina: 49/06 from 27.06.2006., changes and amendments, Official Gazzette of Bosnia and Herzegovina:76/11 and 89/11
25. Franke K., Schomaker L., Veenhuis C., Taubenheim C., Guyon I., Vuurpijl L., Van Erp M, Zwarts G., »WANDA: A Generic Framework applied in Forensic Handwriting Analysis and Writer Identification«, taken 22.10.2014. from http://www.kyfranke.org/uploads/Publications/franke03d.pdf,
26. Association of Vojvodina Court Experts, taken 12. 11. 2014. from http://www.forensicexp-vojvodina.org.rs/clanovi-novac
27. Association of Court Experts „Forenzika“, from Novi Sad, taken 12. 11. 2014. from http://www.forenzika-novisad.org/oblasti.html
28. “Cedar-Fox A Computational Tool for Questioned Handwriting Examination“, source: http://www.cedartech.com/documents/CedarTech_presentation.pdf, taken 22.10.2014.
29. Graphology (Graphoanalysis), taken 22.02.2007. from http://skepdic.com/graphol.html

UDC: 377:343.982

EDUCATING FUTURE CRIMINALISTS IN THE FIELD OF CONTEMPORARY CRIMINALISTIC IDENTIFICATIONS

Biljana Koturevic[1]
Smilja Teodorovic
Ljiljana Maskovic
The Academy of Criminalistic and Police Studies, Belgrade

Abstract: An integral theme in the field of criminalistics is the concept of identification, including human identification, as well as identification of objects (such as weapons, clothing, documents, etc.) and trace evidence (biological traces, fibers, etc.). This is precisely why we developed, at the Academy for Criminalistic and Police Studies, Republic of Serbia, a modern curriculum for future criminalists which incorporates courses in Forensic Science ("Kriminalisticka tehnika", "Osnovi forenzike") and Biometric Identification ("Biometrijske identifikacije", "Biometrijsko-forenzicke identifikacije"). These vital topics are offered at both the Bachelor's and Master's programs. The courses have been designed to cover scientific principles underlying identification methods, traditional and contemporary identification techniques, including emerging approaches, as well as their significance and impact in current criminalistics practice. Importantly, notable efforts have been made to develop practical exercises, in order for students-criminalists to gain hands-on experience in a wide array of identification methods. This paper will discuss an extensive range of approaches used in contemporary criminalistics for identification of humans (such as fingerprints and facial features), objects, materials (various solid and liquid substances) and trace evidence (drugs, and biological fluids such as blood, urine, saliva, etc.). The authors will particularly point out the uniqueness of the Academy's curriculum and significance of the theoretical and practical knowledge gained for the future work in criminalistic identifications.

Keywords: identifications, criminalistics.

INTRODUCTION

As earlier defined, criminalistics is profession and scientific discipline directed to the recognition, identification, individualization and evaluation of physical evidence by application of the natural science in law-sciences matters[2]. Nowadays, the generally accepted definition of criminalistics is given by American Academy of Forensic sciences: "Criminalistics is analysis, comparison, identification and interpretation of physical evidence". So the main role of criminalist is to objectively apply the techniques of the physical and natural sciences to examine the physical evidence, thereby to prove the existence of crime or make connections[3]. In most countries, examination of physical evidence that arises as a result of criminal event is entrusted to forensic scientist or criminalist. However, it must be noted that there is a clear boundary between criminalists who are educated as scientist, and "crime scene investigators" who are primarily police personnel[4]. Educated and trained scientist work in laboratories, and in most countries they are known as forensic scientists compared to crime scene investigators who are not typically educated and trained as scientist. In this paper, for easier understanding, the noun criminalist is used for undergraduate and graduate - master students of criminalistics at the Academy of Criminalistic and Police Studies, Belgrade, Serbia. Students of criminalistics at our institution are being trained for the application of various operational / tactical and technical actions, operational / technical methods and certain investigative activities in order to detect the criminal offense identify the offender and secure the evidence.

Since criminalistics is the recording, identification, and interpretation of physical evidence, a number of standard techniques and procedures have been developed to do this. Both forensic scientists and criminalists need to be intimately familiar with the basic concepts behind these techniques. However, some

1 Corresponding author, Teaching assistant at the Academy of Criminalistic and Police Studies, Belgrade, Serbia, email: biljana.koturevic@kpa.edu.rs
2 California Association of Criminalists. (1963). Definition adopted at the 21st semiannual seminar at Ventura, California.
3 Inman, K., & Rudin, N. (2002). *Principles and practice of criminalistics: the profession of forensic science*. CRC Press.
4 Gaensslen, R.E. (2002). Forensic Science education and Educational Requirements for Forensic Scientist, *The NEACT journal,* 21(1), 19-23.

authors[5] have pointed out that there is a widespread lack of awareness within the police personnel about forensic itself, and solution that forensic methods can offer. For many years, there was also different understanding of how forensic science contributes to criminal justice. Today, with technical progress in number of forensic disciplines, there is a general agreement of exceptional contribution of forensics in criminal investigations and prosecutions[6]. Also, over time, a set of fundamental concepts of criminalistics that form the infrastructure for the practice of forensic science have been developed. These concepts are: identification, classification or individualization, association, and reconstruction, and they are used in attempt to answer the various investigative questions: "who, what, where, why, when and how"[7].

All these facts lead to a general assumption that it is very important to incorporate courses that provide basic knowledge about Forensic Science and Biometric Identification in education of future criminalists. This is why we have developed, at the Academy of Criminalistics and Police Studies, Republic of Serbia, a modern curriculum for the Bachelor's and Master's programs of Criminalistics. In both programs, basic principles of identifications of human, object and trace evidence are studied through theoretical and practical parts of courses. This paper discusses main scientific topics of identification that are studied in our institution and particularly points significance of the acquisition of theoretical and practical knowledge for future work in the field of contemporary criminalistic identifications.

CONCEPT AND DESIGN OF CRIMINALISTIC IDENTIFICATION PROGRAM

One of the most important concepts in criminalistics is identification. It is known that criminalistic identification of humans, objects and trace materials have produced outstanding results in providing evidence for courts. In the curriculum of criminalistics degree program in our institution, the concept of identification is incorporated in both the Bachelor's and Master's Studies. On course "Biometrijske identifikacije" students of undergraduate studies, have the opportunity to become familiar with wide range of approaches that are applied in modern criminalistics for the identification of humans, while the courses "Kriminalistička tehnika" and "Osnovi forenzike" are designed to instruct students on concepts and techniques involved in crime scene investigation, collection, evaluation and characterization of material evidence. Also, students are introduced to the traditional and modern methods for the identification of objects and materials, as well as trace evidence. All of these courses include theoretical lessons, followed by practical exercises and individual or team seminar papers. Because practical exercises are invaluable in process of understanding any study material, special efforts was done regarding their design and implementation in criminalistics study program.

IMPLEMENTATION OF HUMAN IDENTIFICATION IN EDUCATION OF FUTURE CRIMINALISTS

The notion of utilizing human physiological and behavioral characteristic for identification purposes has been used through history back to ancient civilizations[8]. However, despite early discovery, two commonly used biometric - based personal identification methods[9], Anthropometry and Dactyloscopy, were not used in the system of criminalistic identification until the 19th and the beginning of the 20th century. The idea of implementing specific measures of human bodies for their identification (anthropometry) was developed by Alphonse Bertillon[10]. This very significant step forward in identifying criminal offenders was followed by discovery of the uniqueness of the human fingerprints in the late 19th century. Soon after this discovery, many police departments accepted fingerprinting (dactyloscopy) and created a base in a form of identification cards, which are then used for comparison with evidence found at the place of a criminal event. These methods are known as the traditional methods of biometric identification. Development of modern biometric methods appeared at the end of the 20th century. These modern approaches of identification and verification identity of individuals, commonly known as biometrics, are defined as a set of technologies or automated information systems that are used for recognition of individuals based on their characteristics. To elaborate on this definition, identification of humans is based on their physiological and

5 Tilley, N. & Ford, A. (1996). *Forensic Science and Crime Investigation*. Crime Detection and Prevention Series, Paper 73. London: Home office.
6 Fraser, J., & Williams, R. (Eds.). (2009). *Handbook of forensic science*. Routledge.
7 Inman, K. & Rudin, N. (2002). The origin of evidence. *Forensic Science International,* 126, 11–16.
8 Ashbourn, J. (2000). *Biometrics: Advanced identity verification*. Springer-Verlag.
9 Swanson, C.R., Chamelin, N.C., Territo, L., Taylor, R.W. (2012). *Criminal Investigation - 11th Edition*. McGraw- Hill.
10 Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4-20.

behavioral characteristic[11]. The physiological or anatomical characteristic of the human body used for the determination of a person's identity are characteristics that are genetically implied (e. g. face, iris, retina, hand characteristics, and DNA). On the other hand, examples of behavioral traits used for identification are gathered or learned during time[12] (handwriting, voice, gait, gestures, keystroke dynamics, etc.).

In contemporary society, there is a constant need to identify people, therefore, biometric identification has found wide application in criminalistics, public sphere of interest, as well as in commercial society. In criminalistics, the aim of identification humans using their biometric features is finding the link between the individual and the place of the criminal event, and thus finding the offender or releasing innocent suspected citizens[13].

Given the importance of the use of biometric technologies in criminalistics, biometric based human identification is usually incorporated in the curriculums of criminalistics, forensic science and criminal justice degree programs. Therefore, at the Academy of Criminalistics and Police Studies, biometrics is part of courses "Biometrijske identifikacije" and "Biometrijsko – forenzičke identifikacije" on undergraduate - Bachelor's and graduate – Master's studies. In the first part of these courses, some of the traditional identification methods are given as a unique introduction to modern biometric identification. In addition, students are learning how to find connection between sciences, primarily biology, technology and engineering concepts with new technologies[14]. At last, the main objective of the above mentioned courses is to familiarize students with the development of new technologies as well as with possibilities of their application in field of criminalistics.

EXAMPLES OF BIOMETRIC IDENTIFICATION LESSON DESIGN

On the courses "Biometrijske identifikacije" and "Biometrijsko – forenzičke identifikacije", students are learning about the traditional and modern methods of human identification through theoretical and practical part of the lessons. Special emphasis is given to practical exercises, so based on their own experience and in interaction with the traditional and modern technologies, students could, for example:

- draw some conclusions about the advantages and disadvantages of both the traditional and modern identification approaches;
- find possibilities of applying these methods in various segments of criminalistic identification;
- remove ambiguities and possible misconceptions based on previous experience or gained from the media;
- understand how biometric systems work, etc.

Overview of some biometric based identification methods that students of criminalistics are learning in this course is presented below.

Identification of humans based on their fingerprints – Fingerprint is pattern of the epidermis on a finger and consists of papillary ridges and valleys. Papillary ridges are formed through a combination of genetic and environmental factors[15] and the formation of these patterns is complete by the seventh month of natal development[16]. This is why there is a very low probability ($1/1.9x10^{15}$) that two people have the same fingerprint[17]. The first scientific fingerprint technique was initiated in the 16th century[18], but as identification method it was formally accepted in the early 20th century. Through history, various fingerprint acquisition, classification and matching techniques were developed. Traditionally, in criminalistics dactyloscopy was performed using dactyloscopic ink, and fingerprints were transmitted on the identification cards. The identification was carried out by comparison of the latent fingerprint left by the offender on the crime scene with fingerprints from the identification cards. For a positive identification it was necessary to find the number of the same immutable anatomic features of the papillary ridges (minutiae) on the compared fingerprints.

11 International Organization for Standardization (2007): ISO/IEC JTC1/SC37 Standing Document 2- Harmonized Biometric Vocabulary. Geneva SC37N1779.

12 Bača, M., Schatten, M., Ševa, J., Behawioralnych, M., & Fizykalnych, I. (2009). Behavioral and Physical Biometric Characteristics Modeling used for ITS Security Improvement. *Transport problems*, 4(4), 5-13.

13 Teodorović, S., Branković, A. (2010). Biometrijski sitemi: Ultimativni vid identifikacije ljudi u kriminalistici i civilnom društvu. Proceedings of conference Law and Forensics in criminalistics, 2, 281-290.

14 Kukula, E. P., & Harbor, J. M. (2009). Biometric Technology Program to Promote Stem Education for the K-12 Environment. *In international conference on engineering and computer education*, 200-204.

15 Cappelli, R., Ferrara, M., & Maltoni, D. (2006). The quality of fingerprint scanners and its impact on the accuracy of fingerprint recognition algorithms. *Proceedings of Multimedia Content Representation, Classification and Security*, 10-16.

16 Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4-20.

17 Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. *Image Processing, IEEE Transactions*, 9(5), 846-859.

18 Jain, A. K., & Maltoni, D. (2003). *Handbook of Fingerprint Recognition*. Springer, New York.

Figure 1 *Traditional dactyloscopy*[19],[20]

The modern method of human identification by their fingerprints in criminalistics is performed using Automatic Fingerprint Identification System (AFIS). This system is the most widely used biometric technology for human identification, and it is of great importance in criminalistics because fingerprints, unlike some other biometric characteristics (e.g. iris) are very often found at the crime scene locations. Submitting the fingerprint image is performed electronically, using a live scan device or sensor module that images the ridge and valley structure of the user's finger. After the set of discriminatory features is extracted in the extraction module, the comparison of fingerprints based on position, orientation and frequency of minutiae in papillary lines is performed in the matching module. The identification of individuals through AFIS requires comparison of query fingerprint with the prints that exist in the database[21]. A result of this comparison is match score that represent the number of matching minutiae between two fingerprints. In criminalistics this method is very useful for matching latent fingerprints left by offender at the crime scene, with the fingerprints from the database.

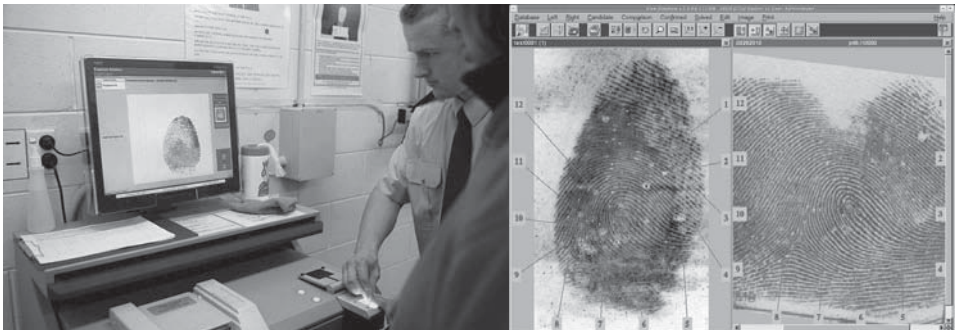


Figure 2 *Acquisition and comparison of latent fingerprint with one from database in AFIS*[22],[23]

For gaining hands-on experience in the process of identification of humans based on their fingerprints, students of criminalistics are practicing both the traditional and modern methods. On the first part of practical exercises of this lesson, students are fingerprinting each other, following the principles of the traditional method. After they recognize the global fingerprint pattern configuration and local pattern features using fingerprint magnifying glass on query fingerprint, they compare it with the few identification cards in order to find the match. In the second part of this lesson, students are familiarized with the work of the automatic fingerprint identification system. Using the scanner they submit the fingerprints and if they are satisfied with the quality of the image displayed on the screen, they are saving the entered fingerprints into a fingerprint record. After scanning the latent fingerprint and extraction of features, students are observing the automatic comparison of created query with all the templates which are stored in the fingerprint record. In addition, they are asked to explain the results of the automatic identification gained in a form of matching score, and to compare it with the results obtained using the traditional method of identification.

The i**dentification of humans based on their facial features –** Facial images are probably the most common biometric characteristic used by humans for making the personal recognition. This is why the photograph was very early acknowledged as the most accurate way to depict people, document and objects,

19 CasTech Fingerprinting Services. Fingerprinting Services. Retrieved from http://www.alaskafingerprinting.com/Fingerprinting.html
20 Just another wordpress.com site, Retrieved from https://mlbl13.wordpress.com/page/2/
21 Teodorović, S., Mašković, Lj. (2011). Intertwined relationship between biometrics and forensic science: Use of biometrics in forensic personal identifications. Proceedings of international scientific conference "Archibald Reiss Days".
22 Fingerprint Technician Training, Retrieved from http://www.fingerprinttechnician.org/category/uncategorized/
23 PrintQuest AFIS - APIS System, Retrieved from http://www.spexforensics.com/applications/printquest

and in the late 19th century was introduced in the process of criminalistics identification. Furthermore, the fact that every face has unique characteristics that distinguish humans from each other, was also used in the first criminalistics identification method, anthropometry. According to this, as later defined as an unreliable method of human identification, the sum of a specific body measurement yields a characteristic formula for each individual[24]. The creator of this method, Alphonse Bertillon was the first who had realized that photographs have to be standardized by using the same lighting, scale and angles[25]. Also, one of the traditional methods of human identification based on their facial characteristic is photorobot. Photorobots have been used to obtain images of wanted criminals, which aid in investigative searches. Based on eye witness memory, these images represent a composite of individual facial features. In contrast to this, the new generation of photorobot software generates images of wanted criminals based on holistic facial descriptions[26].

Figure 3 *Identification card with photograph and personal measurement in early 20 th century (left) and taking anthropometric measurement (right)*[27]

Modern method of human identification is performed using automatic facial recognition system. This application ranges from static or controlled used for the verification to uncontrolled face identification in a crowd (e.g. airport, stadiums, etc.). 2D face recognition systems are geometric or photometric. Geometric systems are based on the location and shape of facial features (eyes, nose, lips, cheeks, chin, and eyebrow) and their spatial differences, and photometric systems consider human face as a whole[28]. The acquisition of biometric characteristic in two-dimensional system for identifying persons is performed using the camera or camcorder and after that, the system automatically performs detection and localization of human face in picture, extracts the facial features and compares it with others from the database in order to identify the person.

Figure 4 *Automatic Face Recognition System*[29]

24 Swanson, C.R., Chamelin, N.C., Territo, L., Taylor, R.W. (2012). *Criminal Investigation - 11th Edition*. McGraw- Hill.
25 Platt, R. *Forensics*. (2005). Kingfisher Publications, Boston.
26 Teodorović, S., Mašković, Lj. (2011). Intertwined relationship between biometrics and forensic science: Use of biometrics in forensic personal identifications. Proceedings of international scientific conference "Archibald Reiss Days".
27 Swanson, C.R., Chamelin, N.C., Territo, L., Taylor, R.W. (2012). *Criminal Investigation - 11th Edition*. McGraw- Hill.
28 Jain, A. K., & Maltoni, D. (2003). *Handbook of Fingerprint Recognition*. Springer, New York.
29 Brothersoft. Face Recognition System 2.1, Retrieved from http://www.brothersoft.com/face-recognition-system-107219.html

On this practical lesson, students are practicing some of the traditional methods of human identification, anthropometry and photorobot. After that, they are gaining practical experience in handling with automatic face recognition system. Using digital photography for capturing images under different illumination conditions, from different angles, with cluttered background, and with various facial obstructions, students are learning what the biggest challenges for this system are. Based on the experience from the traditional and modern approaches in human identification, students are asked to discuss about advantages and disadvantages of both methods, and after all whether the face itself is a sufficient basis for identifying a person.

THE IMPLEMENTATION OF OBJECTS AND TRACE EVIDENCE IDENTIFICATION IN THE EDUCATION OF FUTURE CRIMINALISTS

The objects and the smallest objects, referred as trace evidence, are often found on the place of the criminal event. These, as they are called physical evidence, are part of four types of evidence of criminal event, next to testimony, documentary and demonstrative evidence[30]. Physical evidence (also known as real or direct evidence) is the one which is tangible and can be observed - seen or touched[31]. Objects that could be found on the crime scene are: firearms, and its parts, bullets, casing, shell, clothing, documents, various solid and liquid substances, etc. Trace evidence usually include blood, body fluids, hair, fibers, gunshot residue, glass fragments, soil, etc. Evidence found on the place of the criminal event is the crucial part of investigation, and could provide a link to a person (offender, victim or witness), approve or disapprove witness or suspect testimony, provide important leads for further investigation, and most important to identify a specific suspect. Beside the place of the criminal event, some evidence like fibers, hairs, blood, etc., could also remain on perpetrators or victims and thereby could link a person with a crime scene. After their collection from the place of the criminal event, objects and trace evidence are analyzed in the forensic laboratory. This analysis includes comparison, for example questioned with reference material, and identification. Criminalistic identification is the process of clarifying the physical and chemical identity of substance with near certainty as applied scientific technique allows[32].

Due to the specific job description and a big responsibility that criminalists have during the process of clarification and resolution of criminal offense, at the Academy of Criminalistics and Police Studies a programs (courses) that include education of students in the field of forensics sciences have been designed. These courses "Kriminalistička tehnika" and "Osnovi forenzike" on undergraduate studies of criminalistics include a wide variety of approaches for identification of objects and trace materials, and are designed to assist students in recognition, classification, identification and collection of objects and trace evidence from the crime scene. Although the process of identification (determination of physical and chemical properties) is entrusted to educated and trained scientists, it is equally important for criminalists and future criminalists to understand operation mode of specific forensic method and to recognize the results of those analyses. Also, the goal of the course is to train students to use preliminary tests for the analysis of unknown samples in the field (e.g., tests for blood, urine, semen, drugs, etc.) which can give focus and shorten the forensic analysis itself. Furthermore, modern identification of objects and trace evidences requires constant education and training of police personnel in terms of detection, packaging and storage of trace evidences[33]. These trainings that include rules for handling with evidence, safety concerns of handling evidence and detection techniques, recovery of some evidence, preservation methods, prevention of contamination, and significance of trace evidence analysis results, are provided through education at the Academy of Criminalistic and Police Studies.

EXAMPLES OF OBJECTS AND TRACE EVIDENCE IDENTIFICATION LESSON DESIGN

On the courses "Kriminalistička tehnika" and "Osnovi forenzike", students are practicing some methods for the identification of objects and trace evidence that could be found on the place of the criminal event. In criminalistics, there are two types of identifications, morphological and physico-chemical. Morphological identification of objects is based on comparison of trace evidence with indisputable object and is usually

30 Girard, James E. (2011). Criminalistics: Forensic Science, Crime, and Terrorism. Sudbury, MA; Jones & Bartlett Learning.
31 Shinder, D. L. & Cross, M. (2008). Scene of the Cybercrime. Syngress.
32 Girard, James E. (2011). Criminalistics: Forensic Science, Crime, and Terrorism. Sudbury, MA; Jones & Bartlett Learning.
33 Pyrek, K. M. (2006). Forensic nursing. CRC Press.

performed using optical and measuring methods. On the contrary, physico-chemical identification is used for identification substances by their chemical end elementary composition and they require the use of qualitative and quantitative analysis[34]. Some basic methods for determining the physico-chemical constants of solid and liquid substances are practiced by students on the course "Kriminalistička tehnika". This practical exercises includes for example, determination of density, refractive index, viscosity, etc. Several other methods of objects and trace evidence identification that students of criminalistics are learning in these courses are presented below.

The identification of firearms based on the marks on the casings - The firearm has features that were designed by the factory. These characteristics can be imparted as tool marks on the fired bullet and case during firing, and can be classified by their class characteristics. If the class characteristics agree in every respect with the evidence item (i.e., the cartridge case or the recovered bullet) and with the test-fires from a suspect firearm, the examiner then uses the comparison microscope to compare the individual characteristics of both evidence and test tool marks. Individual characteristics usually arise from the tool working surface, but can also be the result of use, wear, and care of the tool. The characteristics that make the tool surface unique are called individual characteristics. When these characteristics are compared in tool marks, and sufficient agreement is found, identification can be established. Fired cartridge cases are often left at shooting scenes, and they usually contain impressed and striated marks from the magazine and firearm mechanism that fired it. When the firing pin or striker impacts the fire cartridge, it leaves an impressed tool mark on the cartridge case, and any microscopic imperfections on the surface of the firing pin can be transferred onto the case. Chamber sides of the firearm also leave impressions on cartridge case, called chamber marks. All these tool marks are usually individual in nature and can be reproduced during firings[35].

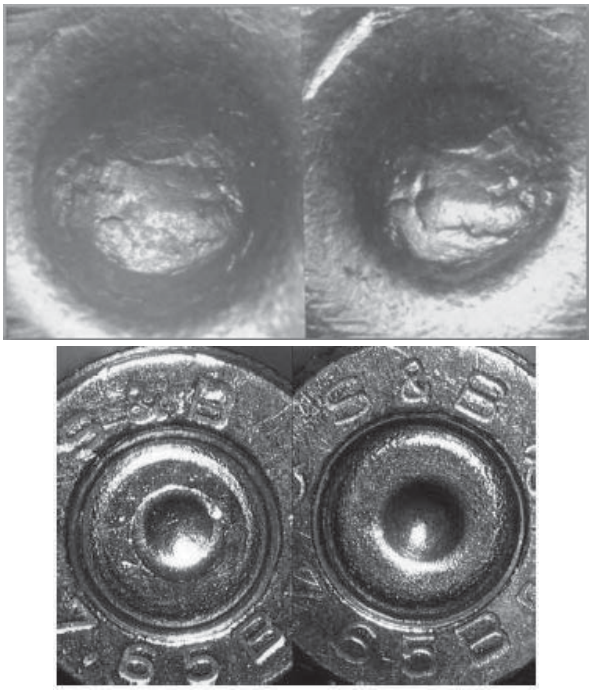


Figure 5 *Microscopic comparison between two cartridge cases*[36]

In this lesson students use a comparison microscope to compare tool marks originating from the firing pin on evidence and test cartridge case. Based on this specific individual tool marks on the chamber case, students are discussing whether the evidence and test chamber could be fired from the same firing mechanism.

The identification of inks –Subtle alterations or additions to documents such as tax returns, wills, and insurance claims, can be detected using chemical and physical examinations. The comparison of two inks involves using optical microscopy, infrared reflectance and luminescence, ultraviolet, fluorescence, solubility tests, and thin-layer chromatography (TLC). The introduction of chromatographic methods for

34 [33] Maksimović R., Bošković, M., Todorić, U. (1998). *Metode fizike, hemije i fizičke hemije u kriminalistici*. Policijska Akademija. Beograd.
35 Thompson, R. M. (2010). *Firearm Identification: In the Forensic Science Laboratory*. National District Attorneys Association.
36 The Smallest Minority, Retrieved from http://smallestminority.blogspot.com/2005/01/why-ballistic-fingerprinting-doesnt.html

comparison of writing inks had a major impact in the detection of fraudulent documents. TLC is the most successful method presently used for the separation and comparison of ink components, being rapid and relatively simple to use[37]. Comparison and identification of separated compounds of inks from the analysed documents is done by measuring the retardation factor (Rf). This factor is influenced with various chromatographic conditions, but the retardation factor is always the same for the compound separated under identical conditions.

For the purpose of identification of inks, students are using TLC method. Extracted ink from analysed document (sample) is compared with the selected writing inks. After developing and drying the TLC plate, the separated color spots of the sample on the TLC plate are measured and their Rf values are recorded. The conclusion is based on the comparative examination of the analysed inks, more precisely their Rf values.

The identification of drugs –Thee identification of unknown sample, suspected to be a drug, is performed by using preliminary tests or laboratory analysis. Preliminary tests represent non-specific method for fast drug sample analysis. This method usually contains couple of independent tests, which can give an indication for presence of controlled substance in the analysed sample. If the preliminary tests come back positive for a certain drug, it is necessary to confirm the presence of the drug with precise laboratory methods. Most common preliminary tests used today are: chemical (spot) tests, microcrystalline tests, thin-layer chromatography, etc.

On the forensic based courses, students are familiarized with preliminary tests and their application in the identification of drugs. Practicing with various preliminary tests gives students an insight in advantages and disadvantages (false positive result) of the tests.

The **identification of biological traces** – Biological traces found on the place of criminal event is of great importance for criminalistics from the revelation of first forensic tests. The first presumptive test for blood was presented in the 19th century and was based on the ability of hem from hemoglobin to oxidize hydrogen peroxide making foam. This and many other tests, including microscopic crystal test for hemoglobin and luminol test, are still in use. The major discovery of blood groups in 1900 enabled even better differentiation between humans. Along whit these revelations, procedure for microscopic detection of sperm was published in the 19th century, followed by presumptive acid phosphatase test for detection of seminal fluid, and salivary amylase test as indicator for the presence of saliva in 20th century[38].

Figure 6 *Positive reaction on Phadebs test*[39]

On the practical exercises, students are applying Phadebas test on an unknown sample (an item or surface) for the detection of saliva stain. This test is based on the reaction of α-amylase enzyme with starch solution on filter paper. Based on the reaction of starch that is immobilized on paper, with unknown sample, students can detect presence of saliva and locate the saliva deposits on sample.

Human urine contains large amount of metabolite products that can serve as a presumptive test for urine in the analysed samples. Students are identifying traces of urine using tests for urea, creatinine and uric acid[40]. In the first test, the detection of urine traces is based on the reaction between sodium hypobromite and urea. In the second test detection of urine traces is based on reaction of creatinine with water solution of picric acid (Jaffe test). The presence of uric acid is also used for identification purposes, and also can be used for distinguishing human from animal urine[41]. The most commonly used test for detection of the presence of uric acid is Schiff test.

37 Chen, H. S., Meng, H. H., & Cheng, K. C. (2002). A survey of methods used for the identification and characterization of inks. *Forensic Science Journal*, 1, 1-14.
38 Inman, K., & Rudin, N. (2002). *Principles and practice of criminalistics: the profession of forensic science*. CRC Press.
39 James, S. H., Nordby, J. J., & Bell, S. (2014). *Forensic science: an introduction to scientific and investigative techniques*. CRC press.
40 Chawla, R. (2014). *Practical Clinical Biochemistry*. JP Medical Ltd.
41 Cooper, G., & Negrusz, A. (2013). *Clarke's analytical forensic toxicology*. Pharmaceutical Press.

Blood is also very common trace event on the crime scene. In forensic science based courses, students are practicing gathering potential blood traces from various surfaces, and their identification. After the collection of liquid or solid traces, they are usually handled with presumptive tests, luminol, phenolphthalein, hydrogen peroxide, etc. These are chemical tests that could only indicate the presence of blood in sample.

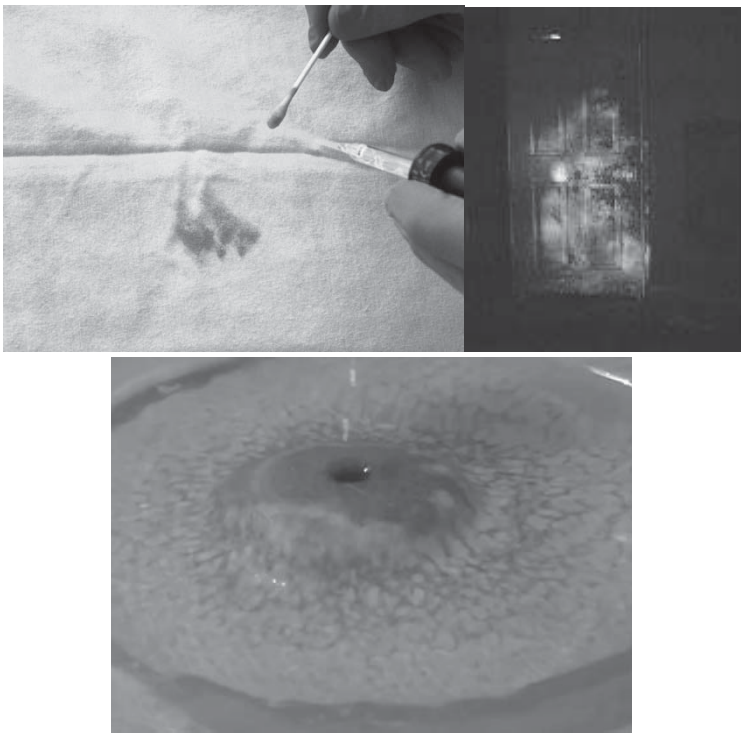


Figure 7 *Some positive tests on presence of blood. Phenolphthalein test (left)*[42]*, luminol test (middle)*[43] *and hydrogen peroxide (right)*[44]

CONCLUSION

In the literature, the significance of criminalistics in clarification and resolution of the crime event was already emphasized. Also, over time the set of basic principles of criminalistics, where the identification has important part in answering the various investigative questions, have been developed. This is why the importance of incorporation of basic concepts about Forensic Science and Biometric Identification in education of future criminalists is very clear. On undergraduate and graduate studies of criminalistics at the Academy for Criminalistic and Police Studies, Republic of Serbia, special attention is directed to concepts of identification, so students are familiarized with the traditional and modern methods of identification of humans, objects and trace evidences through theoretical and practical part of courses. Practical exercises were developed in agreement with constructivism theory[45], according to which the knowledge cannot be transmitted, but can be constructed through hands - on experience. Following this guideline, students of criminalistics on our institution are practicing an extensive range of approaches that are used in criminalistics for identification.

Although, various criminalistic identification programs are developed, our goal is to improve existing elements and adopt the successful elements of other programs in order to enhance education and inspire student's interest in science.

42 Science Lab Supplies. Presumptive Blood Test Kit. Retrieved from http://www.sciencelabsupplies.com/Presumptive-Blood-Test-Kit.html

43 Formerly The Forensic science Laboratory. Forensic Areas, Biology. Retrieved from http://www.forensicscience.ie/Services/Forensic-Areas/Biology/Blood/

44 World News. Retrieved from http://article.wn.com/view/2014/07/09/Global_Hydrogen_Peroxide_Market/

45 Seel, N. M. (2012). *Encyclopedia of the Sciences of Learning*. Springer Science & Business Media.

REFERENCES

1. Ashbourn, J. (2000). *Biometrics: Advanced identity verification*. Springer-Verlag.
2. Bača, M., Schatten, M., Ševa, J., Behawioralnych, M., & Fizykalnych, I. (2009). Behavioral and Physical Biometric Characteristics Modeling used for ITS Security Improvement. Transport problems, 4(4), 5-13.
3. Brothersoft. Face Recognition System 2.1, Retrieved December, 25, 2014, from http://www.brothersoft.com/face-recognition-system-107219.html
4. California Association of Criminalists. (1963). Definition adopted at the 21st semiannual seminar at Ventura, California.
5. CasTech Fingerprinting Services. Fingerprinting Services. Retrived, December 19, 2014, from http://www.alaskafingerprinting.com/Fingerprinting.html
6. Cappelli, R., Ferrara, M., & Maltoni, D. (2006). The quality of fingerprint scanners and its impact on the accuracy of fingerprint recognition algorithms. *Proceedings of Multimedia Content Representation, Classification and Security*, 10-16.
7. Chawla, R. (2014). *Practical Clinical Biochemistry*. JP Medical Ltd.
8. Chen, H. S., Meng, H. H., & Cheng, K. C. (2002). A survey of methods used for the identification and characterization of inks. *Forensic Science Journal*, 1, 1-14.
9. Cooper, G., & Negrusz, A. (2013). *Clarke's analytical forensic toxicology*. Pharmaceutical Press.
10. Fingerprint Technician Training. Electronic Fingerprints. Retrieved December 19, 2014, from http://www.fingerprinttechnician.org/category/uncategorized/
11. Formerly The Forensic science Laboratory. Forensic Areas, Biology. Retrieved December 25, 2015, from http://www.forensicscience.ie/Services/Forensic-Areas/Biology/Blood/
12. Fraser, J., & Williams, R. (Eds.). (2009). Handbook of forensic science. Routledge.
13. Girard, James E. (2011). Criminalistics: Forensic Science, Crime, and Terrorism. Sudbury, MA; Jones & Bartlett Learning.
14. Gaensslen, R.E. (2002). Forensic Science education and Educational Requirements for Forensic Scientist, The NEACT journal, 21(1), 19-23.
15. Inman, K., & Rudin, N. (2002). Principles and practice of criminalistics: the profession of forensic science. CRC Press.
16. Inman, K. & Rudin, N. (2002). The origin of evidence. Forensic Science International, 126, 11–16.
17. International Organization for Standardization (2007): ISO/IEC JTC1/SC37 Standing Document 2-Harmonized Biometric Vocabulary. Geneva SC37N1779.
18. Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. Image Processing, IEEE Transactions, 9(5), 846-859.
19. Jain, A. K., & Maltoni, D. (2003). Handbook of Fingerprint Recognition. Springer, New York.
20. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.
21. James, S. H., Nordby, J. J., & Bell, S. (2014). Forensic science: an introduction to scientific and investigative techniques. CRC press.
22. Just another wordpress.com site. Retrieved December 19, 2014, from https://mlbl13.wordpress.com/page/2/
23. Kukula, E. P., & Harbor, J. M. (2009). Biometric Technology Program to Promote Stem Education for the K-12 Environment. In international conference on engineering and computer education, 200-204.
24. Maksimović R., Bošković, M., Todorić, U. (1998). Metode fizike, hemije i fizičke hemije u kriminalistici. Policijska Akademija. Beograd.
25. Platt, R. Forensics. (2005). Kingfisher Publications, Boston.
26. PrintQuest AFIS - APIS System, Retrieved December 19, 2014, from http://www.spexforensics.com/applications/printquest
27. Pyrek, K. M. (2006). Forensic nursing. CRC Press.
28. Seel, N. M. (2012). Encyclopedia of the Sciences of Learning. Springer Science & Business Media.
29. Science Lab Supplies. Presumptive Blood Test Kit. Retrieved January 20, 2015, from http://www.sciencelabsupplies.com/Presumptive-Blood-Test-Kit.html
30. Shinder, D. L. & Cross, M. (2008). Scene of the Cybercrime. Syngress.

31. Swanson, C.R., Chamelin, N.C., Territo, L., Taylor, R.W. (2012). Criminal Investigation - 11th Edition. McGraw- Hill.

32. Thompson, R. M. (2010). Firearm Identification: In the Forensic Science Laboratory. National District Attorneys Association.

33. The Smallest Minority. Retrieved January, 10, 2015, from http://smallestminority.blogspot.com/2005/01/why-ballistic-fingerprinting-doesnt.html

34. Teodorović, S., Branković, A. (2010). Biometrijski sitemi: Ultimativni vid identifikacije ljudi u kriminalistici i civilnom društvu. *Proceedings of conference Law and Forensics in criminalistics*, 2, 281-290.

35. Teodorović, S., Mašković, Lj. (2011). Intertwined relationship between biometrics and forensic science: Use of biometrics in forensic personal identifications. *Proceedings of international scientific conference "Archibald Reiss Days"*.

36. Tilley, N. & Ford, A. (1996). Forensic Science and Crime Investigation. Crime Detection and Prevention Series, Paper 73. London: Home office.

37. World News. Global Hydrogen Peroxide Market. Retrieved January, 25, 2015, from http://article.wn.com/view/2014/07/09/Global_Hydrogen_Peroxide_Market/

UDC: 343.983.2:616-001.45

FORENSIC ASPECTS OF FIRERAMS INJURIES IN FORENSIC IN MEDICO FORENSIC EXPERTISE

Danijela Ristic[1]

Goran Ilic[2]

University of Niš, Medical Faculty, Institute of Forensic Medicine

Abstract: Injury by firearms takes a very important place among the cases of forensic medicine. They represent a kind of mechanical injuries caused by projectiles or firearms or explosive bursting means. Continuous improvement of weapons and ammunition are changing some basic features of gunshot injuries to the clothes and body victims, especially if the effects of fire and gunpowder soot. Therefore in forensic medical expertise org gunshot injuries should be constantly improved by research methods, using the achievements of physics, chemistry, medicine, criminology and other sciences. The quality and identification of tangible traces depends largely on the effectiveness and appropriateness of judicial proceedings in connection with the offense where these are treated as relevant material evidence.

When forensic experts analyses gunshot injury, the interpretation of experts goes in many directions: from determining whether it is a gunshot early and differentiate the input from the exit wound, determining the approximate distance from which, the breach has occurred, determining the direction of the bullet channel, in case of injuries in the event of death, which has its origin (suicidal, murderous or accidental), in cooperation with ballistic weapons expert identification.

Traces of the projectile on the clothes with which the first autopsy, are an important identifying symbol, not only to indicate a gunshot wound and its direction, and distance firing, but they contain different kinds of clues that come from firing gunpowder, gunpowder soot, particles of gunpowder and metals.

Keywords: firearm injuries, gunshot wounds, ballistics wounds, ballistic expert, the mechanism on the early traces of the projectile and autopsy.

INTRODUCTION

With the development of science and application of their achievements in combating crime have contributed to a greater solidarity and chemical forensic and forensic medicine in the process of solving homicides committed with a firearm, and the points of a ballistic expertise which make the application of chemical methods and forensic medical expertise.

Of feedback forensic ballistic expert evidence obtained using chemical methods, with forensic expertise, the questions that are related to firearm injuries can be answered.

Forensic medicine deals with medically discovering the truth, which is necessary for solving the puzzles posed by law. It deals with the analysis of offenses, victims analysis, cases where a crime is committed, etc. It deals with the relationship of cause and effect. (Milovanovic, M. 1982).[3]

Forensic experts analyzed death, its causes and mechanisms of death, bodily injury, the mechanisms of their forensic significance in criminal proceedings, forensic aspects of murders and other crimes against bodily integrity.

What is now important for forensic medicine is the existence of new methods through analytical techniques, which reveal the presence of newly designed drugs, new scientific drugs and toxic substances at very low concentrations.

Forensic experts with firearms injuries are determined:

- Whether it is an injury infected by gunfire,
- Whether the entry or exit wound,
- At what distance was the blast committed,
- Characteristics and direction of the wound channel,

1 danijela.ristic14@gmail.com
2 gilke@medfac.ni.ac.rs
3 Milovanovic, M: Forensic medicine Medical books Beograd – Zagreb, p.35 - 39

• What the consequences are in relation to the threat to health,
• The origin of the injury whether it's a murder, suicide or Ades
• The identification of weapons and ammunition,

Comparing forensic ballistics, medico forensic experts can determine the distance to the firing.

Firearm injuries in origin may be suicidal, homicidal and accidental. The conclusions as to what kind of injury is done are made only after careful consideration of all available factors is taken.

• Localization and number of wounds,
• Characteristics of the injury magnitude and direction of the wound channel,
• Position of the body and arms,
• Localization of traces of blood on the victim clothes and surrounding objects,
• The presence or absence of damage to clothes and the surrounding objects,
• The existence or absence of signs of a struggle at the scene

On the murder scene, the experts can indicate numerous gunshot wounds in different parts of the body that bear a compartment in the back of the head, back, abdomen or extremities which, extend in different directions with the existence of more lethal injuries.

Picture 1 *Entry wound to the right temporal*

Picture 2 *Exit wound to the right temporal*

In cases of serious injury and suicidal, the victim's clothes should be carefully inspected before they are removed from the body and determine the relationship between the damage done to clothes and the victim's body. The experience has shown that in suicides injuries infected on the body part that was previously released clothes, although this is not the rule.

INTERDISCIPLINARY COOPERATION BETWEEN A FORENSIC EXPERT AND A BALLISTICS EXPERT

During resolving criminal cases, questions often arise to which the answer can be given based on a deeper knowledge of ballistics?

The identification of export evidence obtained answers to questions such as:

• Which is the system of fabrication and a firearm model fired where the missile or shell were found,
• Whether the projectile was fired from processed or handmade firearms,
• Whether a given projectile was fired from a given of firearms submitted expert,
• To determine whether a given projectile fired from weapons testing is performed i.e. fires,
• The bullet in order determine micro grave that is left.

Thank photographs of the crime scene ballistics determined.

• From any kind of firearms is committed blast,
• Direction blacking
• Distance i.e. the place from which the shots were fired
• Position of the offender at the time of firing missiles
• Timing of firing
• When is the last time you fired such weapons

If you are at the scene and found the timber calls the court physician to determine the time of death the manner in which it occurred. The doctor carefully analyzes the surface of the body and takes every element useful for further investigation. He describes the position of wood in the surrounding objects, clothes on it any stains of biological fluids, ambient temperature.

The aim of this first inspection is to determine the possible injuries and gunshot wounds and characteristic traces which could identify an unknown person. Checking if the kild has something in pockets or hands, whether on clothes or below it, and if there are any traces..

During examinations, the court doctor analyses photographing and recording. To determinate approximate time of death takes a sample of transparent gelatinous mass from its socket whereby the concentration potassium ions increases in proportion to the time of death estimated muscle hardness and the occurrence of dead person's stain and measurement of rectal temperature.

The next step is the autopsy the body from the crime scene which is sent to the hall where the autopsy was performed precise description of the injuries observed even in the first analysis, because some signs become noticeable several hours after death. The autopsy mucus is used to determine the consequences of firearms to detect possible internal injuries, to find traces of possible diseases. Monitor and examine the contents of the stomach in order to determine the time of death, the mere quantity of the food indicates that the victim spent the last moments of life. The crime scene is recorded and puts everything that would be helpful in the investigation stage.

The forensic aspect of traces of gunpowder on the victims clothes are essential. The quantity of powder particles that contaminate some clothes depends on the type of fabric and clothing. Then on the very objects such as T –shirts, coats, sweaters all the quantities of powder particles and soot are preserved. From the forensics' point of view, traces of gunpowder on the clothes are important because according to them one can determine the distance cracking which often affects the judicial qualification work. Just by specifying distance shooting in answer to the questing of whether a work is executed in self – defense or not.(Franjic 2004)[4]

Picture 3 *Traces of gunpowder on the victims clothes and defect items*

Traces of the projectile is not the victims clothes are first fortune b a pathologist, are important identification sign and indicate not only the gunshot wound and its direction of movement, but also in the firing distance. Traces in the form of a defect or cleft on clothes caused by a projectile can be a rectangular or circular shape and proper. Neither fabric at the edges of the defect are usually directed towards the movement of projectiles at the entrance to the body, and at the exit from the body.

Clothing or ordering traces in order to determine the distance of shooting as well as determining the input and output openings are treated in such a manner that the area around the inlet opening protects from folding gluing pieces of falling particles of pure paper, while the wet and bloody items dry in shade and at room temperature. For the purpose of determining the precise distance shooting clothes should forwards the forensic technical – on the expertise of the laboratory (Franjic and associates).

The forensic medicine expert wound is a type of mechanical injury, which affects both more tissue. At each wound is to distinguish between inlet and outlet and the wound area. In addition to opening it is necessary to describe its localization appearance, environment, edged, sides, angles, chamels and the content area possibly the bottom of the wound.

4 Franjic, B., Milosavljevic, M., The possibility of identifying the powder particles on clothes Journal of the judicial experts Montenegro 2004. maj

Gunshot wounds fall into the kind of injury in which to solve them requires the cooperation of forensic experts and ballistics expert.

Login gunshot wounds are characterized by tissue defect squashed ring projectile tattoo, distance and toasted goats, print muzzle. The inlet post gunshot wounds from a distance is round and oval shapes depending on the angle at which it come penetrating projectiles.

Picture 4 *agaunpowder tattoo*

Picture 5 *Entrance wound absolute proximity*

Picture 6 *Entrance wound absolute proximity*

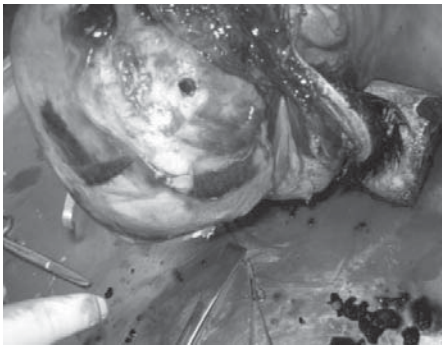
Gunshot wounds of the absolute proximity occurs when the muzzle abuts directly on the skin or the skin at a few millimeters. The entry wound larger irregular edges and stretched.

Forensic experts and interpretation of the code of gunshot injuries of experts moving in several directions.:

- You need to determine whether it is about of gunshot wounds and make a difference input of the output gunshot wound
- Determine the direction of the bullet canal
- If the injury was caused by two or more weapons to be determined which a projectile is created that damage,
- To determine the origin of the injury, suicidal, homicidal accidental,
- In cooperation with the ballistic expert witness strive identification weapons,

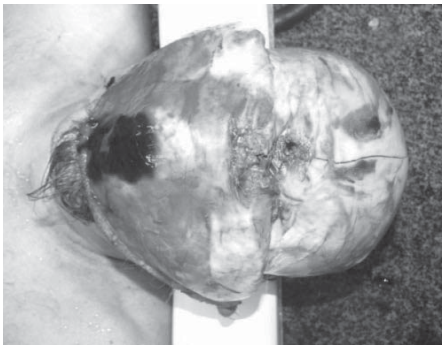
Gunshot wounds to the head are classified in relation to the depth of penetration and the type of projectile. The first group consists of wounds that look reminiscent of the chase and they characterize the outside grazes list cranial bones of the sides of the projectile penetration into the epidural space. When hit by a projectile skull small energy occurs inward fracture circular shape, with a grain of infringing bone. The skull was hit at an angle to the longitudinal axis of the tear so there is an early from of keyhole (Tasic and associates 2006)[5]

5 Tasic M., and associates, Forensic Medicina, Newi Sad, 2006. p: 47 -66



Picture 7 *a) Imput defect in the bone right*

b) Imput defect in the right temporal inside



Picture 8 *a) Defect in the bones on the skull - imput*

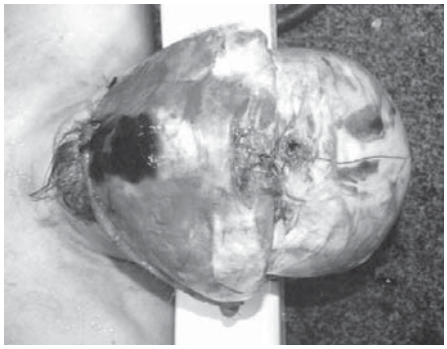
b) Defect in the skull bones along the wound channel back

FROM AUTOPSY EXAMINATIONS TO

According to the Code of criminal Procedure, scene investigation is managed by the investigation judge. At the scene investigations expose the public prosecutor and inspector Criminal Police. Recognizes by order of a judge attend forensic doctors. All actions at the scene investigations are can red out without violating looks scene investigations. The doctor records all of the information and facts the appearance of the scene investigations, temperature, the condition of the clothing on wood, its position relative to the blood stains.

When shoot autopsy was cautiously approaches. Well done an investigation provide transport timber, taking traces of chemical toxicological analysis is completed by a mosaic of events autopsy addition to determining the direct cause and time of death determines the number of gunshot wounds differentiating shoot and spread out determine the direction and the direction of the wound channel their detailed look angle and distance shooting.

Picture 9 *a) The entry wound in the forehead*



b) Imput defect in the bones on the skull

c) The bones on the skull base along the wound chanel

d)Apperance of the projectile in the neck below the skin

CONCLUSION

Firearm injuries occupy an important place among the subjects of forensic medical expertise. They represent a form of mechanical injury caused either by missiles fired from a firearm or by explosive bursting means.

There are many traces that can be present in weapons or in connections with weapons that have a significant judicial medical and forensic significance. State forensic firearms. It can be determined whether the firearms are ridges whether the shot was fired missile and projectile whether this corresponds to projectile, during the last firing of a particular weapon the distance from which the blast enforced the direction from which the shots were fired, the projectile traces on the body and clothes.

In solving and proving criminal offenses involving firearms results ballistics forensic expert evidence medical experts many have operational and evidentiary significance, so it is important that the site be found and fixed traces originating from firearms.

REFERENCES

1. Walker J. T. Chemistry and Legal Medicine, New. Eng J. Med 216: 1024 -1027, 1037.
2. Green A. I., Sauve J. P., The analysi of Gunshot Resida bye Atomic Apsorption Spectrophotometry, Atomic Apsorption Newsleter, Vol. 11, No 5. Sep –Oct, 1972.
3. Eckert, W G.,Introduction to Forensic Sciences (2nded). CRC Press Inc 1997.p: 10 – 15.
4. Zecevic D., and associate (1989.), Forensic Medicine, Yugoslav medical copies, Zagreb, p. 43 – 81.
5. Milovanovic M: Forensic medicina, Medical books, Belgrade – Zagreb, 1982. p.35 – 89.
6. Tasic M ., and associate: Forensic medicina, New Sad, 2006. p 47 – 66.
7. Franjic B., Milosavljevic, M., The possibility of identifying the powder particles on clothes 2004. May
8. Christane, D., R: (2004), . Forensic Investigation of Clandestine Laboratories CRC: Press, LLC.
9. Htp/www. Forensic. Com, February 2010.
10. www. Afte. Org March 201.1
11. www. Firearmsid. Com October 2010.

UDC: 343.983.2:502.51(285)(497.7)

FORENSIC ASPECTS OF POLLUTED WATERS FROM LAKE MAVROVO

Latif Latifi[1]
State Environment and Nature Protection Inspector
Slobodan Oklevski[2]
The Ministry of Interior of the Republick of Macedonia

Abstract: Pollution of waters in current conditions presents serious environmental problem, not only in the Republic of Macedonia, but also within global frames, especially in conditions of limited approach to natural recourses. Water has significant part in creating healthy human environment. Because of the numbers of penalties, crimes and misdemeanours of water pollution the legislator has to incriminate the behaviours that pollute the drinking water, water for livestock and irrigation, etc.

Environmental forensics is significant element for detecting causers of polluted water, and the same presents the subject of interest for this scientific work. However, the authors performed forensic water expertise from Lake Mavrovo and thereby gave reference to the actual state of polluted water. These examinations were realized in order to prevent and suppress this phenomenon leading to the pollution of water in this region, positive practice which could be applied to the waters in other regions, as well.

Examinations were realized in order to define the environmental status of the lake, through monitoring biological and physicochemical parameters of water and, also expertise in the area of water pollution were performed.

Keywords: water, pollution, expertise.

INTRODUCTION

70% of the Earth's surface is covered by water expanses. Water has universal significance for the whole living world. It is in the base of the physiological processes in living organisms, almost all biogeochemical processes are affected by the presence and its course, water is a primordial and current living medium. Despite its importance, today water or water surfaces are facing increased anthropogenic pressure that effects, with their increased spending on the one hand, and pollution on the other hand, a process that not only limits their use value but has negative repercussion on biological components that inhabit them.

Pollution of water surfaces is a global problem that equally affects surface drinking water, surface waters - lakes, rivers and oceans, but also the groundwater. In order to stop further degrading anthropogenic effect on water surfaces, and even more, to take action to improve the conditions to the extent that would be close to the situation with very small or no anthropogenic pressure, in 2000, the European Union promoted and put into effect the European Water Directive.[3] It should serve as a framework for water management and protection, uniformed throughout the European Union, and generally on the territory of whole Europe. Deadline which is defined for achieving the main goal of this Directive which is "good ecological status" is 2015.

The European Water Directive allows harmonization of legislation for the water protection and management and it should be implemented in all EU member states. Candidate countries also need to harmonize the national legislation according to the principles of the European Water Directive. From this perspective, the Republic of Macedonia as a candidate country for the EU membership is also obliged to coordinate its own legislation with the European Directive regulation and to implement the requirements contained therein.

In order to protect the waters in the Republic of Macedonia in 2008, the Law on Water[4] was adopted. This law implemented international legal acts, i.e. directives for water protection. This paper analyzes the situation regarding water pollution of Mavrovo Lake,[5] through the application of forensic methods of research in order to define the ecological status of the lake, by monitoring the biological and physicochemical parameters of water, and also expert report was given in the field of water pollution.

1 l.latifi@yahoo.com
2 o_slobodan@yahoo.com
3 Directive 2000/60/EC of the European Parliament and of the Council, taken from http://www.nve.no/PageFiles/1835/EU_vanndirektiv_eng.pdf?epslanguage=no
4 Official Gazette No. 87/2008
5 Mavrovo Lake is an artificial reservoir created by the accumulation of waters on Marvovska, Nikivorovska and Leunovska Rivers as part of the upper reaches - flow of the Radichka and Belichka Rivers. It is situated 1,230 meters above the sea level, and is bordered by the Bistra and Shar Mountain. The reservoir is situated in the former Mavrovo Pole area of 1,320 ha1,202 meters above sea level and a maximum elevation of 1,233 m above the sea level with the possibility of accumulation of 274.8million m3 of used water volume.

CRIMINAL LAW ASPECTS OF WATER POLLUTION IN THE REPUBLIC OF MACEDONIA

The environmental crime (Article 218)[6] provides that the one, if does not comply with the regulations for the protection and improvement of the environment that pollutes the air, soil, water, surface water or water flow to a greater extent or in a wider area, thus causing danger for the life or health or destruction of animal and plant life on a larger scale, shall be punished with imprisonment from four to ten years.

This is primarily environmental crime, estimated as an attack on the totality of the goods that are basic elements of the biosphere that enable the survival of living beings.[7] In order to eliminate the danger that threatens human health from pollution of the environment, this provision imposes a sanction for non-compliance of the regulations to protect the environment and take measures for prevention and annulment of pollution of the environment.

Article 218, paragraph 2 provides a special form of the crime of committing an act which consists in non-adherence to the regulations for protection and improvement of the environment. This prescribes setting devices or allowing construction, or usage of a plant that pollutes the environment or otherwise if this is missed, to take measures to prevent or disable the pollution of air, soil, water, any surface water or water flow which exceeds the limit or prevent noise that significantly exceeds the allowed limit.[8]

The crime contamination of drinking water (Article 219) provides that a person, who with some harmful substance makes the water unusable for drinking in fountains, wells, cisterns or tanks or some other source of drinking water, shall be punished by a fine or with imprisonment up to three years. If as a result of this the crime from paragraph 1 causes an epidemic of an infectious disease, the perpetrator shall be punished with imprisonment of one to five years. If the crime from paragraph 1 was committed out of negligence, the one shall be punished by a fine or imprisonment up to six months. If the crime from paragraph 1 is committed by a legal person, the one shall be punished by a fine.

But this tort is a special kind of pollution of the environment since it refers to drinking water, but does not refer to the water for livestock, water for industrial purposes-irrigation, washing, etc., that in fact, is an object of this crime while a subject can be any person who causes the above harmful consequences.

This crime exists only if it is established that drinking water is contaminated that endangers the life and health of the people. It means if it contains toxins, sewage, dead animals, decaying animals, products, swill or garbage. It is not considered as a crime if the taste and the appearance are changed (bad taste, smell, unpleasant appearance, tasteless, causing nausea or disgust, etc.).With pollution of drinking water it is not required to specifically threaten the life and health from the use of contaminated water, but also if there is an abstract danger. In order to make a case it is only enough if there is "the possibility of causing mild health disbalance".[9] The crime from Article 219 is very important, because we must use forensic water expertise to prove it.

The crime pollution of fodder or water (Article 223) consists in the act that a person with some harmful substance contaminates fodder or water in rivers, streams, springs, wells, cisterns or other water used for livestock, poultry or game, and thus endangers the life or health of the animal, shall be punished by a fine or imprisonment of up to three years. The sentence from Article 223 paragraph 1 shall be applied to any person who with some harmful substance pollutes waters in: fish ponds, lakes, rivers and streams, and thus endangers the survival of all living organisms. In case of death of animals of greater value, the perpetrator shall be punished with imprisonment of three months to three years. If the crime from paragraph 1 is a legal person, the one shall be punished by a fine.

In this way, with the prediction of these and other crimes in other legislations that treat water protection, the legislator tries to settle this matter. Namely, punishable conducts are predicted that threaten the water as an ecosystems and natural resources, and thus create conditions for its protection. These offenses are the base for the competent national authorities to act in order to detect crimes and perpetrators.[10] In this direction the Ministry of Interior, Inspection Services, Ministry of Environment and Physical Planning, Ministry of Agriculture, Forestry and Water Management and others are acting.

6 Criminal Code, Official Gazette No. 114/2009
7 Malis Sazdovska M. "Manual on environmental crimes investigations" Skopje2014, page 10
8 More about environmental crimes see Malis Sazdovska M. Environmental Criminology, 2009, p. 22
9 G. Vasilevski Criminal-criminological aspects of hydro pollution in Macedonia and the impact of law enforcement methods for timely detection and determining its scope and intensity, Skopje, 2001, p.41
10 For more see Sazdovska M, "Manual for environmental crimes investigations" Skopje 2014

FORENSIC ASPECTS OF THE STUDY OF THE WATER IN LAKE MAVROVO

Van-Veen-excavator with a capacity of 400cm^2 is used while exploring the waters in Mavrovo Lake[11] and collecting the material for quantitative research (Figure 1).

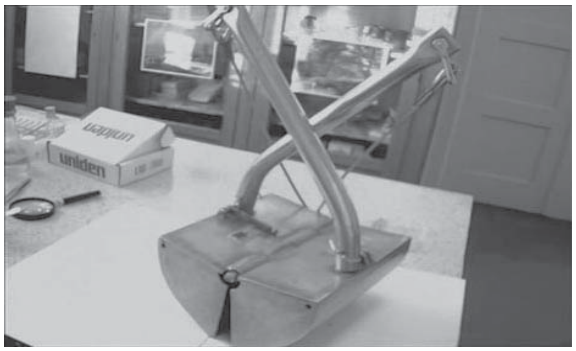


Figure 1 *Van-Veen-excavator*

Also other tools were used for sifting the material, collected in glass jars previously labelled with the date and place. Namely, the collected material was fixed with a usage of 96% ethyl alcohol and transported to the laboratory where the determination of macrozoobenthos was performed (Figure 2).

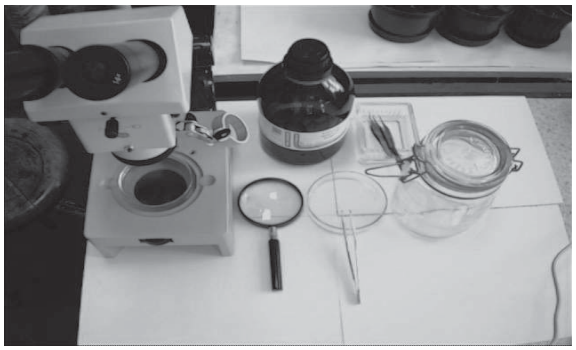


Figure 2 *Part of the equipment used during the laboratory work*

Researches concern the establishment of physico-chemical parameters where the suspended substances are heated and organic substances burnt. Also the pH, the alkalinity of the water and carbon is analyzed by the method of titration. Samples for analysis were taken by Ruttner bottle (Figure 3).

Figure 3 *Ruttner bottle (Foto-www.aq12.com)*

It should be noted that during the research reference profiles were selected according to the criteria of the Water Directive.[12]

11 For more see Latifi L."Assessment of the ecological status of Mavrovo Lake by European directives," Master's thesis, Tetovo, 2011
12 Directive 2000/60/EC of the European Parliament and of the Council, taken from http://www.nve.no/PageFiles/1835/EU_vann-direktiv_eng.pdf?epslanguage=no

RESEARCH AND DISCUSSION

On some localities from the depths of over 10 meters, the slimy material is mixed with **allochthon**, organic material and waste of anthropogenic origin - mostly plastic and nylon. A general characteristic of all types of facie is weak representation of organic detritus connected with other types of sediments. In all localities of 5 meters depth, dominates stony-sandy surface which does not hold detritus, or is mixed with allochthon material mostly from anthropogenic origin and plant residue that is not connected with the rest sediment medium. Of course, this feature is based on the distribution of benthic fauna, and is a major limiting factor that determines the absence of macrophyte vegetation. The water temperature in researched localities shows proportional dependence on the air temperature, rather than on the climatic characteristics.

In fact, during spring there begins the period of warming of the water volume, which is due to the increase in external temperatures and increased hours of the sunlight. The maximum values for all researched localities recorded during the summer are in a range from 23.8°C in the water near the village Leunovo to 24.2°C in the water near the dam. The fall in the temperature is recorded during autumn, and minimum values recorded during winter are in the range from 5.1°C at the locality Vrutok to 5.5°C in the water near the village Mavrovo. Interims of the sereneness of the water, obtained results[13] are shown in the following chart.

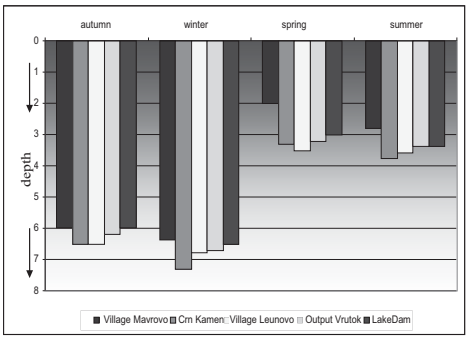


Chart 1 *Seasonal distribution of values for sereneness in the researched localities*

Thus, on the basis of the obtained values, generally it can be observed that greater sereneness is recorded during autumn and winter. The minimum values recorded during spring, that probably besides the suspended particles, an additional factor in this situation is the period of production. Also, the pH of the water is examined and the results show almost equalized values of reaction of the environment, in the range of 8.1 near the village Leunovo to 8.24 in the localities: the village Mavrovo and near the dam.

Alkalinity is a parameter that is closely related to the pH of the environment (Chart 2). According to this, during the vegetation period, with the intensification of the process of photosynthesis, as a result of the use of free carbon dioxide from the water ecosystems, there is an increase in the values of this parameter.

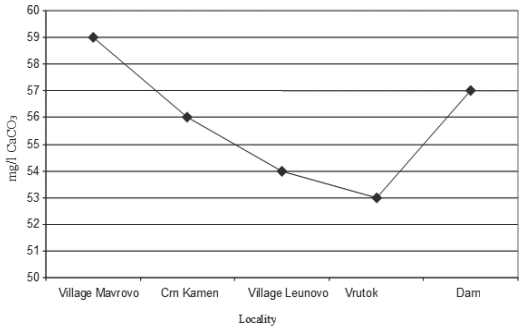


Chart 2 *Total alkalinity in the water of the examined localities*

Within the survey, the results are also obtained of dissolved biodegradable organic substance in the water (Chart 3). Based on the results, it can be concluded that the most organically loaded localities are the village Mavrovo and the locality near the dam, while the least organic loads are noted on the site called Crn Kamen. It is worthwhile noting that in the locality of the village Mavrovo during winter and summer period

13 The adopted samples were analyzed four times during the research period.

there is an increased frequency of tourists. Because of the fact that there isn't a collector and the communal wastewater directly flows into Mavrovo Lake, as an important factor for increased organic load of water in this locality can be considered as a consequence of these waste waters. According to the Regulation on classification of waters in RM (Official Gazette18/99), based on the content of biodegradable organic substances, water in researched sites is mostly of II and III class.

The collection of samples for the analysis was performed with quarterly dynamics, once in the middle of each of four seasons. Reference profiles were chosen according to the EU criteria of water directive and they should depict natural state of the lake, in other words those are profiles located in the coastal part of the lake where there are no anthropogenic pressures.

The values for biodegradable organic substances, presented as consumption of $KMnO_4$ are shown in the chart below. Based on the performed analysis, the samples of water from the respective sites (reference profiles) in the lake Mavrovo were collected, and the obtained values of biodegradable organic substances show seasonal dynamics. In other words, their presence marked an increase during spring and maximum during summer. However, during autumn and winter the visible drop or decline in the values was obtained.

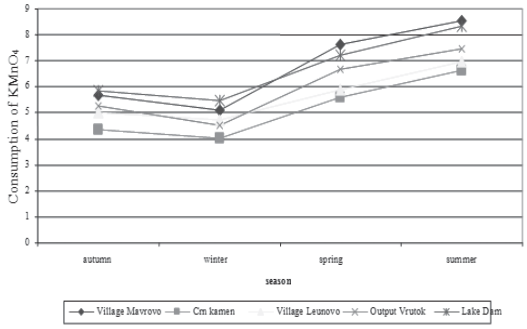


Chart 3 *Biodegradable organic substances (consumption of $KMnO_4$) in water of researched localities*

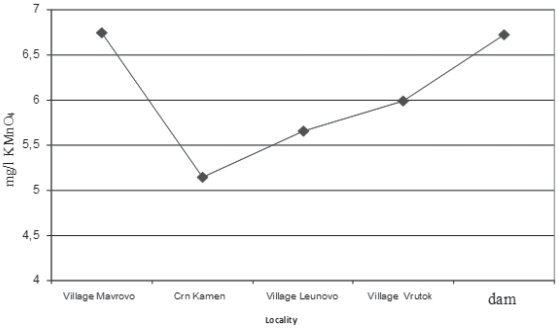


Chart 4 *Average values fo rbiodegradable organic substances (consumption of $KMnO_4$) in water of researched localities*

Further estimation is the presence of oxygen in the water, filled with nutrit,[14] total phosphorus[15]content the concentration of which contributes to put the water in III class, macrophyte vegetation benthic fauna, ecological status, and other parameters.[16]

Biotic index in the Reference profile Crn Kamen has values that indicate good ecological status. The values of the biotic index in the non-referent profile the River Bistra (Figure 4) are within moderate ecological status, while the values of the Biotic index in other three profiles indicate bad ecological status and the presence of organic pollutants.

14 According to the Regulation on Classification of Waters PM (Official Gazette18/99), based on the concentrations of total nitrogen, water in the explored areas is mostly of II or III class.

15 Primary anthropogenic sources of phosphorus in aquatorium first included rainage from urban areas, specifically domestic wastewater (from detergents, personal hygiene products, etc.), industrial waste water and drained waters from agricultural areas.

16 More about this research see Latifi L. "Assessment of the ecological status of Mavrovo Lake according the European Directives" Master's thesis, Tetovo, 2011

Figure 4 *Researched profile - Flow of the river Bistra into Mavrovo Lake (Village Mavrovo)*

CONCLUSION

Environmental forensics is part of the criminalistic techniques, specifically its discipline that develops and applies knowledge, methods and means of detection, investigation and clarification of the disturbance of the environment. In order to determine the current status of all ecosystems, including water and water resources, it is necessary to perform situational expert in the field[17] in order to prove the pollution of water and detect causes of pollution. Situational expert's report on water should be part of the review, because it shows the content of pollutants, such are: heavy metals, mineral oils, pesticides and phenols. It is necessary to investigate the transmission and interaction of potential contaminants and the environment and to determine how water, coming through the sections of the riverbed changes its composition.

Besides the differential method of sampling the water, there is also an integral method. Integrated sampling of water means that from a specific profile, samples are taken and mixed together and an integrated sample of water from a single profile is gained. Such integral sample is representative, but not recommended because the samples lose their individuality.[18]

The authors applied methods from the field of environmental forensics and performed situational expertise in the field and in the laboratory, proving that the water in Mavrovo Lake is polluted and that the level of pollution in certain areas is of III class. These and similar expert's reports are a good indicator of how and in what way, using a certain methodology of work and adequate means and technical equipment for analysis of water environmental crimes can be proved.

But, the next stage, which is no longer a part of the field of criminalistic techniques, but an integral part of the criminal methods or criminal-operative activity, should determine the offender or the offense. Namely, in the future it is necessary to apply operational tactical measures and investigations from the police broad range of instruments, in order to determine the cause of the pollution of the lake. In addition the principle of speed, or operativeness should be applied, with timely treatment and detection of perpetrators of environmental crimes or offenses.

REFERENCES

1. Black, A. R., Barlow, G. W. and Scholz, A. T. 2003: Carbon and nitrogen stable isotope assessment of the Lake Roosevelt aquatic food web. Northwest Science 77: 1-11

2. Callisto, M., Goulart, M., Barbosa, F.A.R., Rocha, O. (2005): Biodiversity assessment of benthic macroinvertebrates along a reservoir cascade in the Lower Sao Francisco River (Northeastern Brazil). Braz. J. Biol., 65(2): 1-6.Rieradeval&Real, 1994

3. Criminal Code of the Republic of Macedonia, Official Gazette No.114/2009

4. Directive 2000/60/EC of the European Parliament and of the Council of 23 October 2000 establishing a framework for community action in the field of water policy. Official Journal of the European Communities, 72 p.

5. ECOSTAT Working Group 2A, 2003. Overall approach to the classification of ecological status and ecological potential. Guidance document N.13. Common Implementation Strategy for the Water Framework Directive (2000/60/EC), 53pp.

17 More on situational expert's repots see Malis Sazdovska M. Manual on ecological crime investigations, p.102

18 Ljustina A. Ecological tort and the police, Zaduzbina Andrejevic, Belgade, 2010, p.61

6. Ervin, P. and J. Haberman, 2001: Lake Peipsi. Flora and fauna. Sulemees Plublishers, Tartu, P. 151.

7. G.Vasilevski Criminal-criminological aspects of hydro pollution in Macedonia and the impact of law enforcement methods for timely detection and determining its scope and intensity, Skopje, 2001

8. Irvine, K.2004: Classifying ecological status under the European Water Framework Directive: the need for monitoring to account for natural variability. Aquatic Conservation: Marine and Freshwater Ecosystems Volume 14, Issue 2, pages 107–112, March/April 2004

9. L.Latifi "Assessment of the ecological status of Mavrovo Lake by European directives" Master's thesis, Tetovo, 2011

10. Ljustina A. Ecological tort and the police, Zaduzbina Andrejevic, Belgrade,2010

11. Malis Sazdovska M. "Environmental Criminology", Skopje, 2009

12. Malis Sazdovska M. "Manual on environmental crimes investigations" Skopje2014

13. Mandaville, S. M., 2002: Benthic Macroinvertebrates in Fresh waters – Taxa Tolerance Values, Metric, and Protocols. (Project H-1) Soil & Water Conservation Society of Metro Halifax. 48, Appendices

14. Miljanović, B., Kostov, V., Zivić, N., Djukić, N., Teodorović, I and Stešević, D. 2004: Characteristics of the bottom macroinvertebrate fauna from Strezevo reservoir and its alimentary water bodies. Proceedings of the 2nd Congress of ecologists of the republic of Macedonia with international participation., 6:257-261

15. Official Gazette No. 87/2008

16. Regulation of classification of waters in the Republic of Macedonia, Official Gazette18/99

UDC: 343.98:621.397.4

INTELLIGENT VIDEO SUPERVISING TECHNOLOGIES AND THEIR APPLICATIONS IN PUBLIC SECURITY

Zhang Hong Jun[1]
National Police University of China, Shenyang

Abstract: Intelligent video surveillance, also called video analytics, is a technology that uses software to automatically identify specific objects, behaviors or attitudes in video footage. It transforms the video into data to be transmitted or archived so that the video surveillance system can deal with them accordingly. It may involve activating a mobile camera in order to obtain more specific data about the scene or simply to send a warning to surveillance personnel so that a decision may be made on the proper intervention required. It represents the trend of future video surveillance. The role of intelligent supervising technology in city public security management becomes more and more important. In this article, we first introduce some background and related technologies of intelligent video surveillance and the key problems involved in intelligent video surveillance development. Then, we present the challenges and key scientific problems involved in intelligent video surveillance development. Finally, this paper takes Pudong airport as an example, introduced construction and characteristics of the video surveillance

Keywords: Intelligent video surveillance, video analytics, public securit**y.**

INTRODUCTION

In recent years, due to the need for public safety, many domestic and foreign universities and research institutions are dedicated to studying on the intelligent video surveillance technology. The United Kingdom can be said to widely use of surveillance cameras at the forefront of the world. The terror attacks cause the situation. 1993 and 1994, the Irish Republican Army in densely populated detonated two bombs in London's financial district. The two terrorist incidents prompted the government installed eight cameras in entrances of the city. But that still does not quell the anxiety people on terrorist activities, so the British government began to install the cameras in more places.

In 1990s, the United Kingdom government began to implement "closed-circuit television (CCTV) program". Since then, CCTV system in all over the country began to install and use on a large scale. The video surveillance system has become an important tool for the British government to crack down on crime and terrorism. London subway carries more than 5000,000 passengers every day. After the London subway bombings, the British government spending more than 20 million pounds on the subway to upgrade camera of the existing video surveillance. Now, more than 6000 cameras have been installed in the London subway. And the function of intelligent video processing and alarm is added to the monitoring system. Such as the system can identify the object which is left in place over a period of time through the dynamic detection function, and alert the security personnel to inspect the object. The existence of CCTV makes public feel more secure. CCTV has made an important contribution in protecting the public safety and providing the police with the criminal investigation. For example, in 2009 95 percent of Scotland Yard murder cases used CCTV footage as evidence.

Many people know that United Kingdom has the most intensive CCTV system in the world. In the security world, at this point, it's fairly common knowledge. In fact, it is estimated that there is one camera for every 14 people in this country. In United Kingdom, whether you at the airport, subway, bus, train, or walking in the street, there are many cameras to monitor you quietly. Someone made the average statistics show every Londoner will be captured by the cameras about 300 times a day or so. If you need, through the camera can easily find anyone to go out every day activities.

From the time when Beijing's Tiananmen Square began to install the first monitoring system to the present, more than 30 years have passed. After 30 years of development, China's monitoring technology has experienced the introduction, imitation, digestion and absorption, innovation and development process. Recalling the development of China's video surveillance industry, the development of the video surveillance technology can be divided into the following three stages. Before 2005, most of the Chinese surveillance cameras are still the analog devices. The surveillance video is storage in the analog video recorders. The

1 269621976@qq.com

number of surveillance cameras is very little, and mainly of them are installed by government. From 2005 to 2009, the majority of analog surveillance equipment has been replaced by the digital monitoring equipment. The rapid development of domestic digital video surveillance technologies has benefit from the Safety City Project. Under the stimulus of Chinese Ministry of Public Security, the major cities of the country begin constructing the public security project to meet the need for security management, urban management, traffic management, emergency command and so on. The core of the project is the video surveillance command center. Through the integration of video surveillance system & other security systems, we can deal with the emergencies in real time. Since 2009, the video surveillance technology has entered the era of network. The intelligent will be an important development direction for the video surveillance technology in China. Development of China's video surveillance industry has entered a new historical period, and the intelligent monitoring system has been used in all areas of domestic industries.

THE KEY TECHNOLOGY OF INTELLIGENT VIDEO SURVEILANCE

Digital signal processor (DSP)

Only by using the high-speed digital signal processor (DSP), the video surveillance use can be transformed from traditional passive surveillance to currently active surveillance with the intelligence analysis capabilities. The DSP has powerful data processing capability and high operating speed. These two features of DSP greatly increased video surveillance in real-time. The development and progress of the DSP can make intelligent video analysis algorithm from running in the background becomes foreground. In modern cameras, DSP technology has been widely used. The photovoltaic signal generated by the solid image sensor is too weak. In addition, the generated image has other defects such as color is not natural, brightness is not even. Therefore, the signal must be processed by video signal amplifier. We need to embed a DSP chip inside the cameras to process digital signal. This is the common type of DSP cameras. In order to improve the performance of the camera, sometime we need to use the DSP chip for further processing such as increase the dynamic range of the camera, reduce noise, and so on. The camera embed the DSP is called smart DSP camera. In the intelligent monitoring system, DSP chip not only coding compression, but also running some intelligence software at the same time. Network video server (DVS) is also called a digital video encoder; it is special equipment to finish audio and video data coding and network transmission. Intelligent Network DVS is the DVS which is embedded the DSP with intelligence software. In summary, DSP is an important part of the intelligent monitoring system.

Intelligent video analysis algorithm

Moving object detection is to extract the target from the monitoring scene through the image change of the video screen. Moving object detection of video surveillance system is the basis of subsequent processing. We need to use moving object detection to achieve motion compensation, video compression, video understanding. Moving object detection not only are the cornerstone of the advanced processing and application, such as target classification, behavior analysis, event detection, behavior recognition, the video image compression and semantic index and so on, but also are the key of intelligent and real-time application of a video monitoring system. The effect of motion detection will directly affect the accuracy of subsequent target tracking and behavior analysis. However, in the real scene, due to weather changes, the shadow of the object, camera shake and other factors, the accuracy of the moving target detection will be decreased. Therefore, it is important to choose the suitable moving target detection algorithm to apply in practice. The following are two common methods of moving object detection.

The first method is inter-frame difference[2]. Using the method, we can detect the moving object by the difference between two images at different time which have the same background. Through the method, we can detect the moving object by the difference between two images at different time which have the same background. The basic principle of the method is subtract two pixels which in the same coordinate but belong to sequence frame in the image, and we can get the location of the moving object from the results. The object is considered static in case of the difference between the two gray levels of the pixels is too small. If the gray levels of the pixels in the image changes greatly, we can think it is caused by the movement

2 Cheng gui xiang, the construction and management of the British video monitoring system [J]. China Security & Protection, 2010, (4):100-107.

of object in the image. The advantages of the inter-frame difference method are not only fast, but also adaptive in the dynamic background. The second method is background difference[3].

The background difference method is another common method to detect the moving object in stationary or slowly changing background. The basic idea of the method is subtract the current frame image from background, and then judge whether there is something abnormal happened based on the changing of the gray level and the histograms statistics information in the result. We can directly extract an image in the video sequence or calculate the average of a series of images to establish the background modeling. The background subtraction method can completely extract the moving object. Because this method is sensitive to the changes of the background, it doesn't suit to be used in the video which background is rapidly changing.

The technology of moving object tracking based on visual image is a hot research topic in the field of computer vision. It is difficult to track object accurately and spontaneously on the influence of fast moving. Hence, the research has the important theory and application value in intelligent video surveillance. In target tracking, there are many different types of tracking algorithm. The earliest algorithm is using the contrast between target and background to identify and extract the target signals, to realize automatic target tracking. But the image matching tracking algorithm is the most widely used method. The basic idea of the algorithm is to compare the characteristics of the image based on a priori (or the estimated characteristics of the target object in the image) with the characteristics of candidate target to get the true position of the target. The image matching tracking algorithm can track the target well when the target has obvious characteristics, but it is too dependent on characteristics. The template matching algorithm can track the target under the complex environment without the characteristics of the target. The algorithm construct model to represent the target, and then get the position of target by tracking the defined model in the image sequence.

THE DEVELOPMENT TREND OF INTELLIGENT VIDEO SURVEILLANCE

With the popularization of the digital monitoring equipment in the city and the improvement of the second generation wireless communication technology, the third generation wireless communication technology has become more and more mature. A variety of new technologies, including SCDMA and WIMAX can give us a very large bandwidth. This makes the remote transmission of video data through wireless technology become possible. Wireless technology not only solved the problem in the area where the cable cannot reach, but also promoted miniaturization of the monitoring terminal. Wireless communication technology made it possible to deploy the monitoring terminal whenever and wherever.

Intelligent video analysis technology combined with cloud computing technology is also an inevitable trend in the development of the future[4]. Let's take the face recognition system as an example. There are two important requirements in the face recognition: First, we need a sample library large enough. Second, the system must be able to match the image in a short period of time. It isn't an easy thing to satisfy the two requirements at the same time. In the cloud computing mode, the terminal equipment (including DVR, DVS, etc.) are only responsible for the collection, compression and transmission of video signal. The establishment of the sample library and search matching are completed in the cloud. All the operation is complete through the large scale distributed computing technology.

If you have hundreds of high-definition cameras, it will produce very large video files. The video files need larger capacity and more stable storage memory. Meanwhile, the transmission of the video files put forward a higher requirement for bandwidth. Although the H.264 video compression technology has the highest data compression ratio, it still can't solve the fundamental problem. Cloud storage is a new concept developed on the basis of the concept of cloud computing. Cloud storage contains a large variety of network storage devices of different types. These network storage devices work together according to the method of distributed computing. Cloud storage provides external access to data storage and business functions. Cloud storage has broken through traditional storage pattern and made it possible to storage huge data[5].

3 Lipton A, Fujiyoshi H, Patil R. Moving Target Classification and Tracking from Real-time Video [C]. Proceedings of IEEE Workshop on Application of Computer Vision, 1998: 8-14.

4 Chang xiaofeng, Fen xiaoyi. A New Method of Detection Based on Background Subtraction and Spatial Temporal Entropy [J]. Computer Simulation, 2008, 25(4): 235-238.

5 Ray-I Chang, Te-Chih Wang, Chia-Hui Wang, Jen-Chang Liu, Jan-Ming Ho. Effective distributed service architecture for ubiquitous video surveillance [J]. Information systems frontiers, 2012, 14(3): 499-515.

INTELLIGENT VIDEO SUPERVISING TECHNOLOGIES IN AIRPORT

Security is the key of the airport management. Security is important for all the departments such as the command center, the runway, terminal, air traffic control, freight, fire protection, garage, frontier defense, public security, customs and other units in the airport. The management of different departments is not only independent, but also overlap. As a result, the structure of video supervising system in the airport is very complex and the system has a complex user requirements. Intelligent video supervising technologies will gradually change the alarm way from passive to active, and ultimately improve the efficiency of monitoring management.

Pudong International Airport Terminal T2 has an area of about 500,000 square meters. The terminal consists of three parts, including the main building, and waiting promenade connecting gallery. It has 42 airport gates, in addition, it has about 170,000 square meters of new integrated transportation center and corresponding elevated ground path. T2 terminal is designed according to the main building to meet the annual passenger throughput of 42 million passengers scale. The airport set up a lot of type's passenger traffic channels such as the customs, border control, inspection and quarantine, security and so on. From the airport's point of view, it security and orderly operation is the most important. So, the airports must be a full range of management.

The airport surveillance systems must have a unified management model, which is conducive to the overall planning, design, construction and use of the system. Pudong Airport T2 monitoring system identified this pattern that carried out in accordance with the functions of user management. In the design of the system, from the front-end cameras, encoders, switches to the back-end servers and storage devices are classified in accordance with 12 kinds of user type design and configuration. This plan is designed to facilitate the division of the network and manage inter-network calls, but also conducive to the management and maintenance in the future. Of course there are other mode selections, as in accordance with the regional management.

The pure digital video surveillance system does not reduce the workload of staff. And it also lacks intelligent function, cannot automatic analysis, identify and deals with the useful information and images. So it cannot do real-time alerts. The airport users need not only record what happened, but also hope that through the technical means to identify problems in real time, and prevent the occurrence of hazardous events. Intelligent as a hot technology, is being valued by more and more customers. But most of the intelligence analysis products in actual use is limited to environmental factors and the scene, cannot achieve satisfactory results. Therefore the users need to choose the intelligent analysis functions which both meet the needs of the management, and more practical. Some of the intelligent analysis functions used in Pudong airport are following.

Crowd counting

Crowd counting is a technique used to count or estimate the number of people in a crowd. By counting the people number (including forward and reverse) of important traffic channels and entrances, the system can real-time analysis the data, and release the information through the airport's information publish system. When the crowd density exceeds a certain limit, the system will automatically alert. The system displays the image on the corresponding monitor workstation. At the same time, remind assist managers to take the necessary intervention or initiate evacuation plans.

The linkage of access and monitoring

The number of the Pudong airport gateway is very large, and every entrance has installed a video camera to monitor people entering and leaving. We must continuously monitor the important or common used gateways. But there's no need to occupy the limited monitoring display equipment and human resources for a long time on the gateway infrequently used (Such as fire emergency channel, forbids any personnel access in the case of non-fire alarm according to the needs of management). Integration of access control and monitoring can be a good solution to this problem.

The access control room has three workstations: they are the access control workstation, the monitoring image workstation and the linkage workstation. The access control workstation display real-time access control reader event information and the monitoring stations can freely switch the display video according to the customer demand. If there is no access control action occurs, the monitoring screen displays nothing. When the access control action occurs (successful swipe, unsuccessful swipe, forced open, etc.), the access control workstation send commands to the linkage workstation, there will be corresponding video image

display in the client screen of the linkage workstation. The system will alert the operator to pay attention to the screen.[6]

Through the application of the intelligent video surveillance, airport surveillance system can provide more intuitive, timely and proactive management. In general, monitoring is a passive activity. But through integration with other systems, the efficiency of video surveillance system can be improved. Monitoring systems are becoming more intelligent

CONCLUSION

Intelligent Video Analysis combines machine vision, image processing, artificial intelligence and pattern recognition, bioinformatics and other disciplines; it is a new research direction. From the current development situation, make the intelligent video surveillance system popularization and application in the field of security, we also need to do a lot of work. There are a lot of problems waiting for us to solve, such as understanding and analyzing complex and abstract behaviors, combining visual information and other sensory information, realizing the networked remote monitoring, reconstructing the 3D scenes, and so on. On the whole, the intelligent video surveillance system has increasingly played a powerful role. It gradually become an important support and guarantee for modern public security system.

REFERENCES

1. Cheng gui xiang, The construction and management of the British video monitoring system [J]. China Security & Protection, 2010, (4):100-107.
2. Lipton A, Fujiyoshi H, Patil R. Moving Target Classification and Tracking from Real-time Video [C]. Proceedings of IEEE Workshop on Application of Computer Vision, 1998: 8-14.
3. Chang xiao feng, Fen xiao yi. A New Method of Detection Based on Background Subtraction and Spatial Temporal Entropy [J]. Computer Simulation, 2008, 25(4): 235-238.
4. Ray-I Chang, Te-Chih Wang, Chia-Hui Wang, Jen-Chang Liu, Jan-Ming Ho. Effective distributed service architecture for ubiquitous video surveillance [J]. Information systems frontiers, 2012, 14(3): 499-515.
5. WANG Yi-Jie, SUN Wei-Dong, ZHOU Song, PEI Xiao-Qiang, LI Xiao-Yong. Key Technologies of Distributed Storage for Cloud Computing [J]. Journal of Software, 2012, 23(4): 962-986.
6. Qian Yi bin, Lu Jian hang. Application of digital video surveillance system in Pudong airport terminal T2 [J]. Intelligent Building & City Information, 2008,8: 97-:99

6 WANG Yi-Jie, SUN Wei-Dong, ZHOU Song, PEI Xiao-Qiang, LI Xiao-Yong. Key Technologies of Distributed Storage for Cloud Computing [J]. Journal of Software, 2012, 23(4): 962-986.

UDC: 343.123.12:621.397.4

APPLICATION OF ABNORMAL DETECTION IN VIDEO INVESTIGATION

Feng Xu[1]

China Criminal Police University, Department of Forensic Science and Technology, Shanyang

Abstract: In recent years, video surveillance has become more and more important for enhanced security and it is indispensable technology for fighting against all types of crime with the construction of sky-net in China. Abnormal detection is the focus of intelligent video surveillance and the information of abnormal behavior can be used in the investigation of criminal cases, which combines computer vision and artificial intelligence technology and has wide application prospect in public security work. In this paper, first the current research situation of the intelligent surveillance system is introduced and then the method and work flow of video investigation based on the characteristics and function analysis of video investigation, the category of abnormal behavior detection is expounded. Finally the function module of abnormal detection system is designed and the key technology of moving target detection, target tracking and abnormality judgment is discussed in view of the actual situation of surveillance system in criminal cases.

Keywords: video surveillance, abnormal detection, moving target detection, target tracking.

INTRODUCTION

With the rapid development of video monitoring system in our country recent years, the video investigation has become an important tool to combat crime and it plays an increasingly important role in criminal detection and Law enforcement. Video monitoring system can directly display and objectively reflect the situation of crime scene, which has the function of real-time monitoring, providing clues, and locking target, fixing evidence and deterring crime. The new mode of investigation has been used in the practice of criminal investigation department. The method "from image to image" and "from image to people" has been developed. It can effectively expand the space-time of crime scene investigation, the investigation object, enrich the source of the case clues, improve the precision of the track block, enrich the composition structure of litigation evidence through comprehensive analysis of scene evidence information, personnel information, network information, communication information and vehicle information[2]. The video investigation has become the powerful weapon to precisely fight crimes for public security organ and it plays an irreplaceable and special role in criminal investigation.

With the development of sky-net project, the surveillance system has been spread all over the road, key departments, case prone areas, public areas and densely populated areas. But the artificial view video is low efficiency and long time for the huge data, which limits the further application. How to make full utilization of video data to enhance the detection technology level is the urgent problem for criminal science and technology to be solved.

Video surveillance systems are monitored by relatively small teams of human operators. Typically a human watches a set of screens which cycle from one camera to another every few seconds. In addition to problems of fatigue and boredom, the human attention span is limited both spatially and temporally. To overcome the practical problems in surveillance systems, such as low quality, huge data, complex content and difficult to provide valuable clues to cases and so on. In this paper, the research results of computer vision, image processing, artificial intelligence and so on are used in the police network video surveillance system. We design and develop the abnormal behavior detection system by using the computer to realize automatic analysis, automatic acquisition, tracking and automatic alarm for the abnormal and emergency in monitoring scene, which can finally provide clues and evidence for the investigation of criminal cases.

1 xufeng_ccpc@hotmail.com

2 Lai J L, Yi Y. Key frame extraction based on visual attention model. J. Vis. Commun. Image R.

VIDEO SURVEILLANCE SYSTEMS

Video surveillance system is safe guard system, which is an important part of a preventive ability of strong comprehensive system. Video monitoring is widely used in many occasions with its convenient, intuitive and abundant information content. With the development of modern science and technology in recent years, video surveillance technology also appeared a considerable development, video monitoring entered the digital network age. The development of video surveillance system is divided into three stages: digital monitor multimedia stage, digital monitor DVR stage and digital monitor network stage[3].

INTELLIGENT VIDEO SURVEILLANCE SYSTEM

Intelligent Video Surveillance (IVS) uses the technology of image processing, pattern recognition and computer vision, which has the powerful ability of computer data processing. It can filter out the useless or interference information, automatically identify different objects, analyze and extract useful information, fast and accurately positioning crime scene and judge abnormal situation in video picture by adding intelligent analysis module in surveillance system.

The overall structure of system is based on C / S (Client /Server) mode, including front-end monitoring point and back-end monitoring point. The overall structure of the system is showed in Figure 1.The front-end monitoring point's main job is to run the server software installed on the platform. The backend monitoring point's main job is to run client software installed on the client's computer. IVS can alarm or trigger other actions through all-day, all-weather and real-time in the earliest and best way. Compared to the traditional video surveillance system, it has the advantages as follows:

(1) all-weather and reliable work. The system can immediately alarm any suspicious events based on the automatic analysis of computer and camera. It completely abandoned the traditional control mode of manual operation and became more intelligent.

(2) Real-time response. The system has more powerful computing capability and can respond in real-time to the abnormal events. Intelligent algorithm can analyse the behavior pattern of current target, judge the potential abnormal behavior, warn before the incident, even prevent the abnormal events and reduce the loss to a minimum.

(3) High accuracy of the alarm. With the development of computer software and hardware, the system has more powerful ability of data processing and analysis. Analysis algorithm of the system is also more intelligent and the alarm accuracy can be significantly improved. It can be more precisely defined characteristics of event and intelligent analysis the features, so the probability of false positives and false negatives can be greatly reduced.

Because of wide application prospect and potential economic value of IVS, it has received considerable attention in the past few years. American DARPA established VSAM (Visual Surveillance and Monitoring) project in 1997[4], which consists of Carnegie Mellon University (CMU), Massachusetts Institute of Technology (MIT) and other colleges and universities. The W4[5] outdoor surveillance system not only can locate and segment part of the body, but also detect whether you have brought anything and separated it from human body, which is proposed by Haritaoglu and so on working for IBM in 2000. The ASVISOR (Annotated Digital Video for Intelligent Surveillance and Optimized Retrieval) system[6] can automatically analyze the dangerous or key events and generate the corresponding alarm while storing surveillance data. Facial recognition system developed by Beijing Tsingda New Technology Co. Ltd can analyze the facial features in screen and search all the recording data according to the feature for indexing. But these studies are mainly focused on security, banks and other special departments, it is difficult to provide valuable clues in the public security work.

DEVELOPMENT DIRECTION OF VIDEO MONITORING SYSTEM

Video digitizing, front integration, network, system integration is the development of video monitoring system and the digital is the premise of network. The network is the foundation of the system integration, so the biggest two characteristics are the digital and network[7].

3 Koene A R, Li Z P. Feature-specific interactions in salience from combined feature contrasts: evidence for a bottom-up saliency map in V1. Journal of Vision.
4 Robert T. Collins, Alan J. Lipton, Takeo Kanade, A system for video surveillance and monitoring. Technical report 2000
5 I Haritaoglu D Harwood L S Davis W4 real-time surveillance of people and their activities[J] IEEE Transactions on Pattern Analysis and Machine Intelligence.
6 Nils T Siebel, S Maybank The advisor visual surveillance system. ECCV 2004 workshop Applications of Computer Vision.
7 Shih H C. Key-frame extraction and key-frame rate determination using human attention modeling. Proceeding of ICME2011.

DIGITAL

Digital is the 21st century feature and it is the development inevitable trend of electronic technology based on information technology. Digital is the pass towards growth with the development of the times; our living environment will become more and more digital.

It is the priority work to digital of video surveillance system form simulation status to digital status, which includes Video, audio, control and so on. It completely breaks the structure of "the center of classic closed-circuit television system: the camera imaging" and fundamentally changes mode and structural form of video monitoring system from information acquisition, data processing, transmission and system control. The flow of information digitization, coding compression, and opening video monitoring system can make agreements with the security system between each subsystem realize seamless connection. It comprehends the management and control in the unified operation platform.

NETWORK

The network of video monitoring system means that the structure of system will transit from lumped type to centralized-distributed. Distribution system adopts the structure of multilayer; it can achieve the task scheduling algorithm of fast response with micro kernel technology of real-time multitasking, multiuser, distributed operating system. The hardware and software of distributing type monitoring system is designed to be standardized, modular and systematic. The system configuration of equipment has the advantage, such as good generality, openness, flexible system configuration, perfect control function, convenient data processing, friendly man-machine interface, system installation, debugging, maintains simple and fault tolerance and reliable. From the above we can see that the development of video monitor system has roughly experienced in analog video, network video and PC video three phases and depends on the technology of the network, communication and transmission platform.

THE WORKFLOW OF VIDEO INVESTIGATION

Video image detection (it is abbreviated image investigation or visual detection) refers to the investigation method in the process of criminal investigation, which can obtain the video image in accordance with the law and comprehensively use investigation measures based on video monitoring and identification technology, electronic information display technology, computer technology and other information capture technology and database technology. It can obtain the investigative clues and evidence through correlation analysis, comparison and collision. It can catch the suspect and confirm the purpose of prevent, control, expose and confirm the crime. From definition of the video image investigation we can see that the main body of video image investigation is specially exercise state indictment of the investigation organ and investigator. The content of the video image investigation is the concrete application of image technology in the investigation activities. The purpose of video image investigation to collect evidence and determine the criminal suspect based on the analysis of image.

VIDEO CRIME SCENE INVESTIGATION

Video surveillance system can record the dynamic process of event in the scope of monitoring as a product of modern science and technology development. It can provide effective information of criminal behavior and process, which is relevant in the case of the people, things and materials. It has become the new content of crime scene investigation for the criminal investigation department.

Video crime scene investigation can find and collect crime information by video monitoring, and expose the criminal behavior, which is based on the survey of video monitoring system, network and control range in the crime scene and related area. It includes three aspects:

(1) The work is to investigate the video monitoring (probe) of the crime scene and related area, understand the monitoring area and the surrounding site environment and grasp the situation of direction, angle, the scope of monitoring and blind area (monitor hole);

(2) The work is to master its working procedure and principle, evaluate its use value and prepare to search, view and collect the related information based on the understanding of control system and program;

(3) The related information of crime can be retrieved, viewed and gathered.

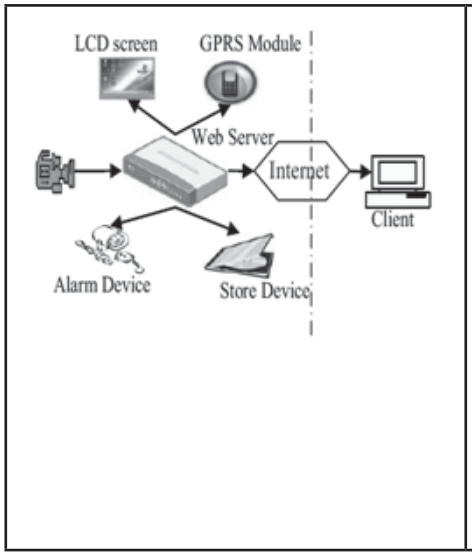


Figure 1 *The overall structure of the system*

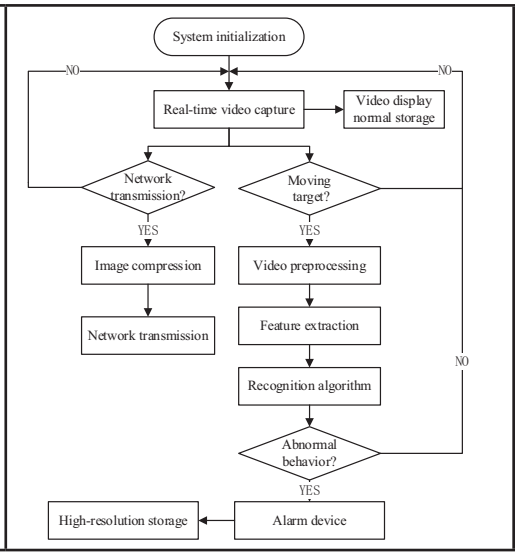


Figure 2 *The overall flow chart of system*

DESIGN AND IMPLEMENTATION OF ABNORMAL BEHAVIOR DETECTION SYSTEM – THE FUNCTION OF ABNORMAL BEHAVIOR DETECTION SYSTEM

The general sense of the abnormal behavior is referred to violate social civilization standards or groups of behaviors and the standard. The definition in criminal science is anomalous trajectory, the suspect's behavior, crime and other related actions based on language, text or image as the carrier. At present, the study on abnormal behavior is mainly concentrated in the human abnormal behavior, especially ATM and group events. We extend the research object, aggregate the case information and construct four functions of abnormal detection as follows.

1. Human abnormal detection

(1) Cover their faces

The system can identify the specific areas of human facial skin based on corresponding threshold, real-time alarm and record for hide or cover face.

(2) Climbing detection

The sensitive areas can be protect by setting virtual line. When the suspicious person climbs over the wall or fence of important venues, the system can real-time alarm, even detect in single direction or double direction.

(3) Fighting

The system can automatically adapt to the scene change, realize the full range of video detection, detect the fight event or sudden collapse and so on, and the first time automatic record and alert.

(4)Abnormal running or crowd

The system can detect fast motion of suspicious person in specified area, the crowd suddenly gathering and immediately alarm based on the dense degree of region population.

(5) Hovering detection

The suspects will observe the scene before the crime. They will appear multiple times in the monitoring area, the system can detect and alarm according to the trajectory, such as: horizontal, vertical, left and right, circling and so on.

2. Vehicle anomaly detection

With the rapid development of transportation, the suspect often use the vehicle during the crime which occurred before, the process of committing crimes and escaping from the crime scene, so the anomaly detection vehicle is becoming more and more important. This paper defines the vehicle abnormal be-

havior, it mainly includes shading license plate, entering green grassland, sidewalks, parking zone, retrograde, over speed, slow speed, turn around suddenly, hovering, blocking vehicles, dangerous driving and so on. The system will automatically recognize and alarm during the above mentioned behavior.

3. Equipment anomaly detection

At present, the anti-reconnaissance consciousness of suspect strengthens gradually in order to cheat the law. They will destroy surveillance equipment during the crime which occurred before or the process of committing crimes. In view of this situation and the wear and tear of the equipment, the systems focus on the great change of the video image, such as shielding camera, greatly moving and so on. It can automatically recognize and real-time alarm when the equipment is destroyed or disturbed by ED.

4. The other anomaly detection

It can real-time alarm and detect the explosives or suspicious item occurring more frequently in case, throwing articles from vehicle, knives, guns and other dangerous tools.

THE OVERALL FLOW CHART OF SYSTEM SOFTWARE

The overall flow chart of system software is showed in Figure 2. After system booting, server obtains real-time data stream from the camera, displays on the LCD screen and normal storage. The main program detects whether there are network transmission commands; if yes, the system transfer the compression image data through network. Moving target detection program can detect whether there are moving targets in the video. If not, the system continues to loop and detect without any treatment; on the contrary, the system starts video preprocessing, feature extraction and recognition algorithm calculation. Then the system detects whether there is abnormal behavior; if not, the system continues to loop; on the contrary, the program will alarm and storage in high-resolution.

THE KEY TECHNOLOGY OF VIDEO SURVEILLANCE

The key technology of abnormal detection consists of moving object detection, target tracking and behavior analysis. Moving target detection belongs to the low-level vision module of computer vision technology, the detection results are very important to future work. Target tracking and behavior analysis respectively belongs to middle level and high-level vision module.

MOVING TARGET DETECTION

Moving object detection can accurately extract the moving objects from the background in video sequence and get the target regional or outline, which is the foundation of target tracking and behavior analysis. At present, there are mainly four kinds of moving target detection method: frame difference method, background difference method, optical flow method and the method based on characteristic.

1. Frame difference method

The frame difference method can get target image through subtracting two consecutive frames of the video sequence. When there are abnormal moving objects in the monitoring region, two consecutive frames will have great differences. We can get the corresponding pixel gray difference absolute value by comparing the threshold, judge whether a target in the background and finally separate moving target region from background. This method can quickly separate the moving object region from the background, has a variety of complex environmental adaptability is better and high robustness. But it can't extract all relevant feature points and easily produce cavitation by the movement of target speed.

2. Background difference method

Background difference method can identify the moving target by subtracting the current continuous image and background images. It compares the current video frame with the constructed background model. The region which exceeds threshold value is target and the other one is background. It can extract the moving target fast and completely, but it will affect by the background illumination conditions, environmental interference and video acquisition error.

3. Optical flow method

Optical flow is the change in brightness of the image as a vector field to determine the target motion analysis. Optical flow field contains the object dynamic behavior and surface structure information, the pixel space of the moving objects in the observation plane motions will produce instantaneous velocity

field, flow field calculates every frame image and detects the moving target by combining with the moving characteristics. In most cases, we can use this method to judge whether the object is in motion or not. The current shortcomings of optical flow method is the large amount of computation, it needs higher hardware configuration and is not suitable for real-time processing.

4. The method based on characteristic

There are lots of methods based on characteristic according to the different situations of different monitoring objects. It can recognize and detect based on the shape, color and even biological characteristics and so on. This method has great flexibility and generally higher recognition rate, but identification method is different in occasions, so it is not universal adaptability.

TARGET TRACKING

Target tracking is to determine the position target in each frame and get temporal trajectory of moving target. It has two main methods: one is based on prior knowledge of the detection and suitable for simple environment; another does not rely on prior knowledge and requires testing to correction. It can be divided into the following four categories based on the expression of target motion and similarity measurement.

1. Tracking based on active contour

Active contour model (Snake model) can define deformable curves by minimizing the energy function in the image domain and gradually adjust the dynamic shape consistent with the target contour, which is proposed by Kass. The Snake technology can manage any deformation processing of arbitrary shape; firstly it segments the object boundary as the initial template tracking, then determines the target function representation of objects real boundary and finally gets the real object boundary movement by lowering the value of the objective function. This method considers not only the gray information from the image, but also the overall contour geometric information. But the drawback is the large amount of computation, and poor effect for target movement speed.

2. Tracking based on feature

Tracking based on feature only considers some remarkable characteristics of the target image and ignores the whole characteristics of the target. This method includes feature extraction and feature matching two aspects. The advantages are less sensitive to the moving object scale, deformation and brightness. It can get a part of the features and complete the tracking task even if the target is a partially obscured. But the effect of extraction of image features is dependent on various extraction operator and parameter settings for the image blur and noise sensitive. It is difficult to determine the relationship of continuous frames because of missing features.

3. Tracking based on region

The basic idea of the algorithm is first to get the target template and then track the correlation target in the image sequence. The advantage of this method is high accuracy and very stable when the target has not been blocked. But the first disadvantage is time-consuming when the search area is larger, then the target will miss when the target deformation is big and has big block. How to deal with the situation when the template change is the main work for the tracking method based on region.

4. Tracking based on model

The tracking based on model can establish the model through prior knowledge and then real-time update through matching tracking target model. It can realize the tracking target for rigid object, the state of which is motion transformation, mainly translation and rotation. This method is not easily affected by the observation angle of view, strong robustness, high tracking precision and strong anti-interference ability, which is suitable for the various changes of movement, but the computational analysis is complex, slow computing speed, model updating is more complex and poor real-time performance.

BEHAVIOR ANALYSIS

Behavior analysis is the recognition and understanding, it is based on moving target detection and tracking. It can improve the level of intelligent video surveillance system by using effective algorithm to analyze and recognize action mode. Abnormal behavior recognition is the key problem of behavior analysis, how to define and judge the abnormal behavior is the main work. The main methods can be divided into two categories, behavior analysis method based on model and behavior analysis method based on similarity.

1. Method based on model

Method based on model can first determine predetermined criteria for some abnormal behavior and then extract feature information from video sequence according to the criterion such as the shape of moving objects, motion feature and so on. We can establish the models of normal behavior by using the obtained feature information from semi supervised or artificial method. In practical application, this method has better detection performance if the monitoring system can establish the model of human motion, but it is difficult to establish model and decrease detection effect when modelling time is longer, the number of normal behavior is great.

2. Method based on similarity

Method based on similarity doesn't need to define the human behavior model in advance and find abnormal behavior through the automatic learning of normal behavior from an image sequence because the abnormal behavior is hard to define and easy to find. We stage threat according to certain rules and extract feature vectors from the video sequence segmentation, finally the few categories of video is abnormal.

According to the actual situation of public security work, we choose background difference method for moving detection, the Kalman filtering method for tracking and Hidden Markov models for behavior analysis.

CONCLUSION

Digital, networked and intelligent is the inevitable trend of video surveillance. In this paper, the current research situation of the intelligent surveillance system is introduced, then we study the method and work flow of video investigation and design the function module of abnormal behavior detection. Finally we discuss the key technologies according to the research status of intelligent monitoring, which can improve the ability of video surveillance system, improve the effect of video resources and finally provide the evidence and the clue for crime case.

ACKNOWLEDGMENT

This research work is supported by the Natural Science Foundation of Liaoning Province, China under contract No. 2013020008.

REFERENCES

1. Koene A R, Li Z P. Feature-specific interactions in salience from combined feature contrasts: evidence for a bottom-up saliency map in V1 [J]. Journal of Vision, 2007, 7(7): 1-14.
2. Lai J L, Yi Y. Key frame extraction based on visual attention model [J]. J. Vis. Commun. Image R, 2012, 23(1): 114-125.
3. Robert T.Collins. Alan J.Lipton.Takeo Kanade. A system for video surveillance and monitoring[R].Technical report. 2000.
4. I. Haritaoglu. D.Harwood. L. S. Davis. W4. real-time surveillance of people and their activities[J] IEEE Transactions on Pattern Analysis and Machine Intelligence. 2000. 22(8). 809-830.
5. Nils T Siebel, S Maybank. The advisor visual surveillance system[C]. ECCV 2004 workshop Applications of Computer Vision(ACV). 2004.
6. Shih H C. Key-frame extraction and key-frame rate determination using human attention modeling [C]. Proceeding of ICME2011. Barcelona, Spain: IEEE, 2011:1-4.

UDC: 343.983:613.83
543.544.5

DETERMINATION AND QUANTITATIVE ANALYSIS OF DESIGNER DRUGS BY GAS CHROMATOGRAPHY-MASS SPECTROMETRY

Xueguo Chen[1]
Zhang Ting
Hongyang Wen
National Police University of China, Department of Forensic Chemistry, Shenyang

Abstract: A robust gas chromatography-mass spectrometry (GC-MS) method was employed for the determination and quantitative analysis of four designer drugs in human blood. Designer drugs, including methcathinone (MC), 3.4-methylenedioxymethcathinone (MDMC), 4'-methyl-α-pyrrolidinopropiophenone (MPPP) and methylenedioxy-pyrovalerone (MDPV) were analyzed by GC-MS under the optimal chromatographic separation conditions. Liquid-liquid small volume extraction was utilized in the pretreatment of human blood sample, and the ensuing method was validated with good analytical results including high extraction efficiency, low limits of detection and good linearity throughout the studied concentration ranges. The method exhibited good accuracy and precision in the determination of designer drugs in human blood. The obtained results also showed the potential in the determination of trace evidence identification in forensic science.

Keywords: Gas Chromatography-Mass Spectrometry; Designer Drug; Synthetic Cathinones; Blood.

INTRODUCTION

Designer drugs, also named synthetic drugs or novel psychoactive substances are synthesized to enhance the pharmacological activities of already known drugs[2]. Typically, they are made by modifying the molecular structures of existing drugs to varying degrees. Designer drugs have appeared on the illicit drug market and are available illicitly in tablet or powder form in many countries, and they are sold as 'legal highs' or 'bath salts' in all regions[3]. Synthetic cathinones were the typical favorite class of designer drugs in China. Aiming to aid law enforcement and to understand what kind of potential candidates may the abusers be, their analysis is a necessary task. Several available analytical methods have been applied in the determination of designer drugs in pharmaceutical samples and biomaterials, such as thin layer chromatography[4], gas chromatography-mass spectrometry (GC-MS)[5], liquid chromatography-mass spectrometry[6], capillary electrochromatography[7] and Fourier transform infrared spectroscopy[8].

In the present study, a specific and sensitive method utilizing GC-MS has been applied for the simultaneous analysis of four designer drugs in human blood. The obtained results have not only exhibited the good accuracy and precision of the approach, but have also showed the potential application for trace evidence identification in forensic science.

1 dicpchenxg@hotmail.com
2 A.M. Leffler, P.B. Smith, A. Armas, F.L. Dorman. The analytical investigation of synthetic street drugs containing cathinone analogs. Forensic Sci. Int., 2014, 234: 50-56.
3 E. Smolianitski, E. Wolf, J. Almog. Proactive forensic science: A novel class of cathinone precursors. Forensic Sci. Int., 2014, 242: 219-227.
4 N.N. Daeid, K.A. Savage, D.Ramsay, C. Holland, O.B. Sutcliffe. Development of gas chromatography-mass spectrometry (GC-MS) and other rapid screening methods for the analysis of 16 'legal high' cathinone derivatives. Sci. Justice, 2013, 54 (1): 22-31.
5 A.C.S. Lucas, A.M. Bermejo, M.J. Tabernero, P. Fernandez. Use of solid-phase micro-extraction (SPME) for the determination of methadone and EDDP in human hair by GC-MS. Forensic sci. int., 2000, 107 (1-3): 225-232.
6 V. Uralets, S. Rana, S. Morgan, W. Ross. Testing for designer stimulants: metabolic profiles of 16 synthetic cathinones excreted free in human blood. J. Anal. Toxicol., 2014, 38 (5): 233-241.
7 Z. Aturki, M.G. Schmid, B. Chankvetadze, S. Fanali. Enantiomeric separation of new cathinone derivatives designer drugs by capillary electrochromatography using a chiral stationary phase, based on amylose tris (5-chloro-2-methylphenylcarbamate). Electrophoresis, 2014, 35 (21-22): 3242-3249.
8 K.M. Abdel-Hay, J. DeRuiter, C.R. Clark. Regioisomeric bromodimethoxy benzyl piperazines related to the designer substance 4-bromo-2,5-dimethoxybenzylpiperazine: GC-MS and FTIR analysis. Forensic Sci. Int., 2014, 240: 126-36.

EXPERIMENTAL

Chemicals and reagent

Methcathinone (2-(methylamino)-1-phenyl-propan-1-one, MC), 3,4-methylenedioxymethcathinone (2-Methylamino-1-(3,4-methylenedioxyphenyl)propan-1-one, MDMC), 4'-methyl-α-pyrrolidinopropiophenone (1-(4-methylphenyl)-2-(1-pyrrolidinyl)-1-propanone, MPPP) and methylenedioxy-pyrovalerone (1-(Benzo[d][1,3]dioxol-5-yl)-2-(pyrrolidin-1-yl)pentan-1-one, MDPV) standards were all provided by Public Security Bureau of Nantong (Nantong, China) for research purposes and the purities were all above 95%. *N*,*N*-dimethylaniline, cyclohexane, other common chemicals and solvents were all of analytical reagent grade and purchased from Guoyao Group Chemical Reagent Shenyang Co., Ltd (Shenyang, China).

Preparation of standard solution and blood samples

Stock solutions of MC, MDMC, MDPV and MPPP were individually prepared in deionized water with the concentration of 1.0 mg/mL. The concentration of stock solution of internal standard *N*,*N*-dimethylaniline was 20 μg/mL in methanol. Spiked blood samples with MC, MDMC, MDPV and MPPP were prepared by sequential dilution of stock solutions in human drug-free blood.

Treatment of blood samples

Fifty microliters Na_2CO_3-$NaHCO_3$ buffer (pH=10.8), 50 mg NaCl, 0.5 mL cyclohexane and 50 μL *N*, *N*-dimethylaniline stocking solution were added to 5 mL human blood in sequence and vortex-mixed for 3 min, and then were centrifuged at 5000 rpm for 10 min. The supernatant were delivered, and an aliquot of 1 μL was injected to the GC-MS system for the qualitative and quantitative analysis.

GC-MS conditions

GC-MS analysis was performed using POLARIS Q gas chromatography-mass spectrometer (Thermo Fisher, USA) equipped with a manual injection and split liner. Separation was achieved with a HP-5 MS capillary column (30 m × 0.25 mm i.d., 0.25 μm) with helium as the carrier gas at a constant flow rate of 1.0 mL/min. The column oven temperature program started at initial temperature 60 ☒, held for 1 min, and increased to final temperature 280 ☒ at a rate of 20 ☒/min, and then held at 280 ☒ for 10 min. 1 μL aliquot of sample was injected with a split ratio of 10:1. The injector and the GC interface temperatures were maintained at 280 ☒ and 250 ☒, respectively. Electron ionization (EI) ion source was utilized in the mass spectrometer, the energy was 70 eV and the ion source temperature was maintained at 250 ☒. Acquisition mode was SCAN with the range of m/z 50~m/z 500. Data acquisition and instrument control were performed using Xcalibur software (Thermo Fisher, USA).

RESULTS AND DISCUSSION

Optimization of GC-MS conditions

MC, MDMC, MDPV and MPPP are four typical designer drugs[9],[10],[11],[12], belong to cathinones, and the structures of them are very similar as shown in Fig. 1. Column oven temperature program was optimized by comparing the peak resolutions of four designer drugs and international standard (IS) obtained from different programs according to the corresponding reports in literature[13]. The re-

9 M. Coppola, R. Mondola. Synthetic cathinones: chemistry, pharmacology and toxicology of a new class of designer drugs of abuse marketed as "bath salts" or "plant food". Toxico. Letters, 2012, 211: 144-149.
10 R. López-Arnau, J. Martínez-Clemente, M.I. Carbó, D. Pubill, E. Escubedo, J. Camarasa. An integrated pharmacokinetic and pharmacodynamic study of a new drug of abuse, methylone, a synthetic cathinone sold as "bath salts". Pro. Neuro-psychoph., 2013, 45: 64-72.
11 M.R. Meyer, P. Du, F. Schuster, H.H. Maurer. Studies on the metabolism of the α-pyrrolidinophenone designer drug methylenedioxy-pyrovalerone (MDPV) in rat and human blood and human live rmicrosomes using GC-MS and LC-high-resolution MS and its detectability in blood by GC-MS. J. Mass Spectrom., 2010, 45: 1426-1442.
12 D. Springer, G. Fritschi, H.H. Maurer. Metabolism of the new designer drug α-pyrrolidinopropiophenone (PPP) and the toxicological detection of PPP and 4'-methyl-α-pyrrolidinopropiophenone (MPPP) studied in rat blood using gas chromatography-mass spectrometry. J. Chromatogr. B, 2003, 796: 253-266.
13 A.M. Leffler, P.B. Smith, A. de Armas, F.L. Dorman. The analytical investigation of synthetic street drugs containing cathinone analogs. Forensic Sci. Int., 2014, 234: 50-56.

tention times of these four designer drugs and IS under the optimized column oven temperature program were 5.97 min, 9.60 min, 10.61 min, 8.57 min and 4.11 min, respectively, and a typical chromatogram is presented in Fig. 2.

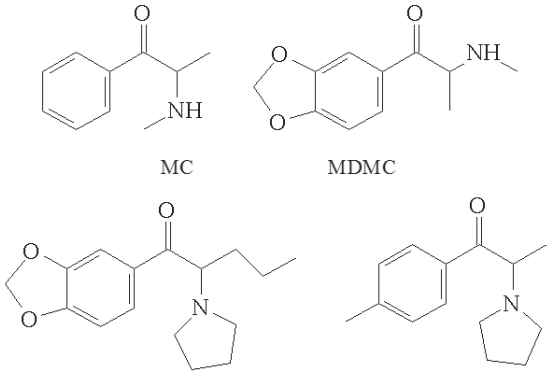


Figure 1 *Chemical structures of MC, MDMC, MDPV and MPPP*

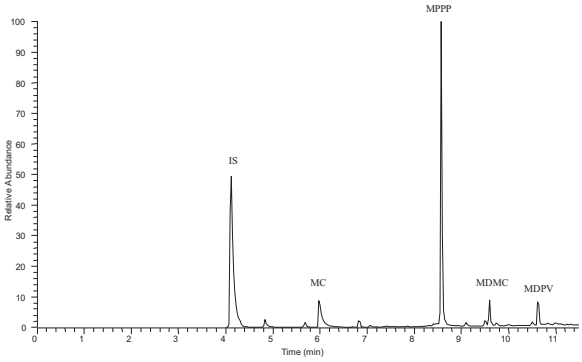


Figure 2 *GC-MS chromatograms of four designer drugs*

Selection of extraction procedure

Generally, a sample pretreatment step is commonly necessary in the determination of analytes in blood with GC-MS, up to now, there are many methods have been established applied in the approach, such as liquid-liquid extraction (LLE)[14], solid-phase extraction (SPE)[15] and so on[16]. Small volume liquid-liquid extraction was proved to be simple, rapid and sparing of solvent and experimental time comparing to regular volume LLE, and it has been applied in the determination of drugs[17]. Small volume liquid-liquid extraction was employed in our study. As we know, ethyl ethanoate, benzene, cyclohexane, toluene are commonly extract solvents utilized in the extraction procedure, they were examined in our study and the results showed that the extraction efficiency of cyclohexane was higher than others, so it was employed as the extractant in the LLE of designer drugs in human blood. Furthermore, the usage of cyclohexane, salting-out effect, sample pH and extraction time were all tested and optimized by comparing the extraction efficiency of these designer drugs in human blood, thus the pretreatment procedure of the blood was obtained.

14 S.M. Christner, R.A. Parise, E.D. Levine, N.A. Rizvi, M.M. Gounder, J.H. Beumer. Quantitative method for the determination of iso-fludelone (KOS-1803) in human plasma by LC-MS/MS. J. Pharm. Biomed. Anal., 2014, 100: 199-204.
15 K. Saito, Y. Kikuchi, R. Saito. Solid-phase dispersive extraction method for analysis of benzodiazepine drugs in serum and blood samples. J. Pharm. Biomed. Anal., 2014, 100: 28-32.
16 P. Xiang, M. Shen, X.Y. Zhuo. LC-MS and application in the analysis of medicine and abused drugs, Shanghai Science and Technology Press, Shanghai, China, 2009.
17 P.J. Meng, Y.Y. Wang, D. Zhu. Small volume liquid extraction of amphetamines from bio-samples and GC/MS analysis. Chinese J. Appl. Chem., 2008, 25 (12): 1449-1455.

Characteristic of designer drugs with GC-MS

In order to determine the characteristic mass fragments, the primary EI mass spectra and the product spectra of four designer drugs were recorded in full scan mode with GC-MS. The character fragment ions could be observed in the EI spectra of MC, MDMC, MPPP and MDPV, respectively. Two of the fragment ions were chosen for the confirmation of designer drugs, which are shown in Table 1. Furthermore, the postulated fragment ions of these four designer drugs were also benefit to the qualities analysis of designer drugs in forensic science.

Table 1 *Retention times and ions for the analysis of four desiger drugs*

Compound	Retention time (min)	Ions for qualitative analysis (m/z)	Ion for quantitative analysis (m/z)
MC	5.97	58, 121	58
MDMC	9.60	149, 121	149
MDPV	10.61	126, 84	126
MPPP	8.57	98, 112	98

Moreover, calibration linearity of the method was investigated by analyzing different concentrations of human urine with designer drugs. The calibration curves were obtained by plotting the peak-areas of designer drugs against the concentrations of them in human blood. Good linearity was obtained in the range of 0.01 μg/mL-5.0 μg/mL. In order to estimate the limit of detection (LOD) and the limit of quantization (LOQ), spiked samples at different concentrations were analyzed. The LODs and LOQs of designer drugs developed in the present work are shown in Table 2, respectively, which were calculated on the basis of the chromatographic peak for which the signal-to-noise ratio was 3 (S/N=3) for qualitative and 10 (S/N=10) for quantitative. Moreover, recovery tests were also carried out by spiking 0.5 μg/mL, 1.0 μg/mL and 2.0 μg/mL designer drugs solutions and the average recoveries are also shown in Table 2.

Table 2 *Linearity equations, coefficients, linearity ranges, LODs and LOQs of four designer drugs*

Name	Linearity equation	Coefficients (r)	Linearity range (μg/mL)	LOD (μg/mL)	LOQ (μg/mL)
MC	Y=1300X-570	0.9917	0.05-5.00	0.02	0.05
MDMC	Y=5500X-120	0.9912	0.03-5.00	0.01	0.03
MDPV	Y=3500X-410	0.9968	0.01-5.00	0.003	0.01
MPPP	Y=3600X-380	0.9915	0.05-5.00	0.02	0.05

CONCLUSION

A GC-MS method has been established for the simultaneous determination of four designer drugs in human blood in this study. The selective, sensitive, robust analytical procedure has been successfully applied for the analysis of spiked human blood samples of MC, MDMC, MDPV and MPPP, the experimental results have been satisfactory and showed that the potential advantages in the identification and quantitative analysis of designer drugs in addicted relevant cases.

ACKNOWLEDGEMENT

The financial support of the Faculty Research Grant from Key Laboratory of Evidence Science (No. 2014KFKT05) in this study is acknowledged.

REFERENCES

1. A.M. Leffler, P.B. Smith, A. Armas, F.L. Dorman. The analytical investigation of synthetic street drugs containing cathinone analogs. Forensic Sci. Int., 2014, 234: 50-56.
2. E. Smolianitski, E. Wolf, J. Almog. Proactive forensic science: A novel class of cathinone precursors. Forensic Sci. Int., 2014, 242: 219-227.
3. N.N. Daeid, K.A. Savage, D.Ramsay, C. Holland, O.B. Sutcliffe. Development of gas chromatography-mass spectrometry (GC-MS) and other rapid screening methods for the analysis of 16 'legal high' cathinone derivatives. Sci. Justice, 2013, 54 (1): 22-31.
4. A.C.S. Lucas, A.M. Bermejo, M.J. Tabernero, P. Fernandez. Use of solid-phase microextraction (SPME) for the determination of methadone and EDDP in human hair by GC-MS. Forensic sci. int., 2000, 107 (1-3): 225-232.
5. V. Uralets, S. Rana, S. Morgan, W. Ross. Testing for designer stimulants: metabolic profiles of 16 synthetic cathinones excreted free in human blood. J. Anal. Toxicol., 2014, 38 (5): 233-241.
6. Z. Aturki, M.G. Schmid, B. Chankvetadze, S. Fanali. Enantiomeric separation of new cathinone derivatives designer drugs by capillary electrochromatography using a chiral stationary phase, based on amylose tris (5-chloro-2-methylphenylcarbamate). Electrophoresis, 2014, 35 (21-22): 3242-3249.
7. K.M. Abdel-Hay, J. DeRuiter, C.R. Clark. Regioisomeric bromodimethoxy benzyl piperazines related to the designer substance 4-bromo-2,5-dimethoxybenzylpiperazine: GC-MS and FTIR analysis. Forensic Sci. Int., 2014, 240: 126-36.
8. M. Coppola, R. Mondola. Synthetic cathinones: chemistry, pharmacology and toxicology of a new class of designer drugs of abuse marketed as "bath salts" or "plant food". Toxico. Letters, 2012, 211: 144-149.
9. R. López-Arnau, J. Martínez-Clemente, M.I. Carbó, D. Pubill, E. Escubedo, J. Camarasa. An integrated pharmacokinetic and pharmacodynamic study of a new drug of abuse, methylone, a synthetic cathinone sold as "bath salts". Pro. Neuro-psychoph., 2013, 45: 64-72.
10. M.R. Meyer, P. Du, F. Schuster, H.H. Maurer. Studies on the metabolism of the α-pyrrolidinophenone designer drug methylenedioxy-pyrovalerone (MDPV) in rat and human blood and human livermicrosomes using GC-MS and LC-high-resolution MS and its detectability in blood by GC-MS. J. Mass Spectrom., 2010, 45: 1426-1442.
11. D. Springer, G. Fritschi, H.H. Maurer. Metabolism of the new designer drug α-pyrrolidinopropiophenone (PPP) and the toxicological detection of PPP and 4'-methyl-α-pyrrolidinopropiophenone (MPPP) studied in rat blood using gas chromatography-mass spectrometry. J. Chromatogr. B, 2003, 796: 253-266.
12. A.M. Leffler, P.B. Smith, A. de Armas, F.L. Dorman. The analytical investigation of synthetic street drugs containing cathinone analogs. Forensic Sci. Int., 2014, 234: 50-56.
13. S.M. Christner, R.A. Parise, E.D. Levine, N.A. Rizvi, M.M. Gounder, J.H. Beumer. Quantitative method for the determination of iso-fludelone (KOS-1803) in human plasma by LC-MS/MS. J. Pharm. Biomed. Anal., 2014, 100: 199-204.
14. K. Saito, Y. Kikuchi, R. Saito. Solid-phase dispersive extraction method for analysis of benzodiazepine drugs in serum and blood samples. J. Pharm. Biomed. Anal., 2014, 100: 28-32.
15. P. Xiang, M. Shen, X.Y. Zhuo. LC-MS and application in the analysis of medicine and abused drugs, Shanghai Science and Technology Press, Shanghai, China, 2009.
16. P.J. Meng, Y.Y. Wang, D. Zhu. Small volume liquid extraction of amphetamines from bio-samples and GC/MS analysis. Chinese J. Appl. Chem., 2008, 25 (12): 1449-1455.

UDC: 343.983:621.397.42
343.982.5

IMAGE RESOLUTION ENHANCEMENT BASED ON COMPLEX WAVELET TRANSFORM AND ITS APPLICATION

Feng Qingzhi
National Police University of China
Department of Audial and Visual Material Examination Technology, Shenyang

Abstract: Image resolution enhancement is also named image interpolation, which means to magnify the image without loss in its clarity. In this paper, a complex wavelet-domain image resolution enhancement algorithm based on the estimation of wavelet coefficients is proposed. The method uses a forward and inverse complex wavelet transform to construct a high-resolution image from the given low-resolution image. By the inverse complex wavelet transform, the high-resolution image is reconstructed from the low-resolution image with a set of wavelet coefficients. The set of wavelet coefficients is estimated from the complex wavelet transform decomposition of the rough estimation of the high-resolution image. Experimental results are presented and discussed on the vehicle image captured from the video surveillance system, through comparisons between state-of-the-art resolution enhancement methods. It can be concluded that the image resolution enhancement based on complex wavelet transform demonstrated higher performances in terms of image resolution and visible quality than other methods, but at increased computational costs. Future developments of the proposed method may be adapted to real-time low resolution images enhancement.

Keywords: video surveillance system, image resolution enhancement, complex wavelet transform, image interpolation.

INTRODUCTION

Image resolution enhancement is a usable preprocess for many forensic image analysis and examination applications, such as face recognition, human action recognition, vehicle feature examination and so on. Image resolution enhancement techniques can be categorized into two major classes according to the domain that they are applied in: the space domain and the transform domain [1]. The techniques in the space domain use the statistical and characteristic data directly extracted from the input image itself, while the techniques in the transform domain use transformations such as discrete wavelet transform (DWT) to achieve the image resolution enhancement.

The DWT has been widely used for performing image resolution enhancement [2-4]. A common assumption of DWT-based image resolution enhancement is that the low-resolution (LR) image is the low-pass-filtered subband of the wavelet-transformed high-resolution (HR) image. This type of approach requires the estimation of wavelet coefficients in subbands containing high-pass spatial frequency information in order to estimate the HR image from the LR image. In order to estimate the high-pass spatial frequency information, many different approaches have been introduced. In [2] and [3], only the high-pass coefficients with significant magnitudes are estimated as the evolution of the wavelet coefficients among the scales. The performance is mainly affected from the fact that the signs of the estimated coefficients are copied directly from parent coefficients without any attempt being made to estimate the actual signs. This is contradictory to the fact that there is very little correlation between the signs of the parent coefficients and their descendants. As a result, the signs of the coefficients estimated using extreme evolution techniques cannot be relied upon. A hidden Markov tree-based method in [2] models the unknown wavelet coefficients as belonging to mixed Gaussian distributions which are symmetrical about the zero mean. The above models are used to determine the most probable state for the coefficients to be estimated. The performance also suffers mainly from the sign changes between the scales. The DWT is not shift invariant, and as a result, suppression of wavelet coefficients introduces artifacts into the image which manifest as ringing in the neighborhood of discontinuities. In order to combat this drawback in DWT-based image resolution enhancement, a cycle-spinning methodology was adopted in [4]. The perceptual and objective quality of the resolution-enhanced images by their method compares favorably with that in recent methods.

A complex wavelet transform (CWT) is introduced to alleviate the drawbacks caused by the decimated DWT [5]. It is shift invariant and has improved directional resolution when compared with that of the DWT. Such features make it suitable for image resolution enhancement. In this paper, a complex wavelet-domain image resolution enhancement algorithm based on the estimation of wavelet coefficients at HR scales is proposed. The initial estimate of the HR image is constructed by applying a cycle-spinning methodology [4] in the CWT domain. It is then decomposed using the one-level CWT to create a set of high-pass coefficients at the same spatial resolution of the LR image. The high-pass coefficients, together with the LR image, are used to reconstruct the HR image using inverse CWT. This paper is organized as follows: Section II gives a brief review of the CWT. Section III describes the proposed CWT-domain vehicle feature image resolution enhancement algorithm. Section IV provides some experimental results of the proposed approach and comparisons with other approaches including bilinear interpolation, bicubic interpolation and DWT-based interpolation. Section V concludes this paper.

COMPLEX WAVELET TRANSFORM

The complex wavelet transform is a combination of two real-valued discrete wavelet transforms. The ordinary DWT is shift variant due to the decimation operation exploited in the transform. As a result, a small shift in the input signal can result in a very different set of wavelet coefficients. For that, a new kind of wavelet transform is introduced in [5], called the CWT which exhibits shift-invariant property and improves directional resolution when compared with that of the DWT.

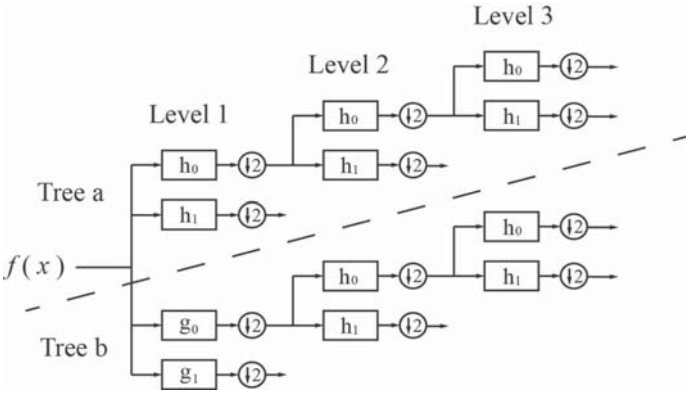


Figure 1 *the Dual-Tree Complex Wavelet Transform, comprising two trees of real filters, a and b, which produce the real and imaginary parts of the complex coefficients*

The CWT also yields perfect reconstruction by using two parallel decimated trees with real-valued coefficients generated at each tree. The 1-D CWT decomposes the input signal $f(x)$ by expressing it in terms of a complex shifted and dilated mother wavelet $\Psi(x)$ and a scaling function $\varphi(x)$, i.e.,

$$f(x) = \sum_{l \in Z} s_{j0,l} \phi_{j0,l}(x) + \sum_{j \geq j0} \sum_{l \in Z} c_{j,l} \psi_{j,l}(x) \tag{1}$$

And

$$\begin{cases} \phi_{j0,l}(x) = \phi^{r}_{j0,l}(x) + \sqrt{-1}\phi^{i}_{j0,l}(x) \\ \psi_{j,l}(x) = \psi^{r}_{j,l}(x) + \sqrt{-1}\psi^{i}_{j,l}(x) \end{cases}$$

Where Z is the set of natural numbers, j and l refer to the index of shifts and dilations, respectively, $s_{j0,l}$ is the scaling coefficient, and $C_{j,l}$ is the complex wavelet coefficient and the superscripts r and i denote the real and imaginary parts, respectively. In the 1-D CWT case, the set $\{\phi^{r}_{j0,l}, \phi^{i}_{j0,l}, \Psi^{r}_{j,l}, \Psi^{i}_{j,l}\}$ forms a tight wavelet frame with double redundancy. As an example, the dual-tree complex wavelet transform is described in fig.1. The real and imaginary parts of the 1-D CWT are computed using separate filter banks with filters h_0 and h_1 for the real part, g_0 and g_1 for the imaginary part.

Similar to the 1-D CWT, the 2-D CWT decomposes a 2-D image *f(x,y)*.through a series of dilations and translations of a complex scaling function and six complex wavelet functions $\Psi^{\theta}_{j,l}$, i.e.,

$$f(x,y) = \sum_{l \in Z^2} s_{j0,l} \phi_{j0,l}(x,y) + \sum_{\theta \in \Theta} \sum_{j \geq j0} \sum_{l \in Z^2} c^{\theta}_{j,l} \psi^{\theta}_{j,l}(x,y) \qquad (2)$$

Where $\theta \in \Theta = \{\pm 15^{\circ}, \pm 45^{\circ}, \pm 75^{\circ}\}$ provides the directionality of the complex wavelet function. In other words, the decomposition of *f(x,y)* by exploiting the CWT produces one complex-valued low-pass subband and six complex-valued high-pass subbands at each level of decomposition, where each high-pass subband corresponds to one unique direction θ.

PROPOSED METHOD

Let us consider the unknown *2H x 2W* HR image X_H and the known *H x W* LR image X_L. The aim of image resolution enhancement is to generate an estimated HR image X_H of the unknown HR image X_H using the known LR image X_L. Let us further assume that the one-level complex wavelet transform decomposition of a *2H x 2W* HR image *X* results in a matrix of *CWT (X)* = ($[LP_x\ HP_x]$), and the inverse complex wavelet transform of $[LP_x\ HP_x]$ reconstructs the image *X* perfectly, i.e., $ICWT([LP_x\ HP_x])=X$. LP_x is a matrix of size *H x W* which is the complex-valued low-pass subband resulting from the one-level *CWT* decomposition of image *X*, and HP_x is a matrix of size *H* x *W* x *6* which is the collection of all six complex-valued high-pass subbands resulting from the one-level CWT decomposition of image *X*.

For a given LR image X_L, the proposed resolution enhancement method is made up of the following four main steps: 1) generate the initial estimate *Y* of the HR image; 2) decompose *Y* using one-level CWT to create a low-pass and high-pass matrix structure $[LP_y\ HP_y]$; 3) formulate a matrix structure $[X_L\ HP_y]$using $[LP_Y\ HP_Y]$ and the input LR image X_L; and 4) generate the HR image by employing ICWT on $[X_L\ HP_Y]$.

The first step employs the cycle-spinning algorithm [4] in the CWT domain to create an initial estimate *Y* of the unknown HR image. The second step is the estimation of the high-pass coefficients for the input LR image X_L. The initial estimate *Y* is decomposed using the one-level CWT to create one complex-valued low-pass subband and six complex-valued high-pass subbands with the same spatial resolution as that of X_L, i.e., $CWT(Y) = [LP_Y\ HP_Y]$. In the final step, the input LR image, together with the complex-valued high-pass subbands HP_Y extracted from the one-level CWT decomposition of *Y* is used to create the HR image by employing ICWT, i.e.,

$$\hat{X}_H = ICWT([X_L\ HP_Y]) \qquad (3)$$

EXPERIMENTAL RESULTS

In the experiments, the natural-color (R, G, and B) vehicle image captured from the video surveillance system is used. The image recorded the vehicle running through the campus of NPUC, Shenyang on September 4, 2014. A test image of size 356 × 512 pixels is cropped from the raw image, as shown in Fig. 2(a), and is used as the reference image. In order to obtain a performance metric in addition to visual assessment of the results using different resolution enhancement methods, we take a 356 × 512 image X_H, filter it with a 3 × 3 averaging (low-pass) filter, and down sample it to obtain two available LR images $X^{(2)}$ and $X^{(4)}$of sizes 178×256 and 89 × 128 pixels, respectively. The available LR images are shown in Fig.2 (b) and Fig.3 (b). The superscripts 2 and 4 denote the downsample factor. The resolution enhancement methods are applied on LR images $X^{(2)}$ and $X^{(4)}$ to reconstruct an estimate X_H of the known HR image X_H. The original HR image X_H and the reconstructed HR image X_H are then compared qualitatively and quantitatively. In this paper, images consisting of three spectral bands that correspond to the R, G, and B channels in a natural color image representation, i.e., $X_H = \{X^{(R)}_H, X^{(G)}_H, X^{(B)}_H\}$ and $X_L = \{X^{(R)}_L, X^{(G)}_L, X^{(B)}_L\}$ are used, and resolution enhancement methods are applied to each spectral band of LR image X_L independently to reconstruct an estimate of the reference image.

The quality of the resolution-enhanced images is estimated using several metrics from the remote sensing community. Let the reference HR image X_H and the reconstructed HR image X_H be of size *H* x *W* pixels and consist of three spectral bands, i.e., *R, G* and *B*. The following quantitative metrics are used to compare X_H and X_H.

1) Quality index [6] is obtained through the use of a correlation coefficient between hyper complex numbers that represent spectral vectors. Quality index is made up of different components (factors) to take into account the correlation: the mean of each spectral band, the intraband local variance, and the spectral angle. The highest value of Quality index is one, which is obtained if and only if the resolution-enhanced image is equal to the reference image.

2) Root-mean-square error (RMSE) is the RMSE between the reference image and the resolution-enhanced image, i.e.,

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\Delta\left(X_H^{(i)}, \hat{X}_H^{(i)}\right)^2} \tag{4}$$

Where

$$\Delta\left(X_H^{(i)}, \hat{X}_H^{(i)}\right) = \sqrt{\frac{1}{HW}\sum_{x,y}\left(X_H^{(i)}(x,y) - \hat{X}_H^{(i)}(x,y)\right)^2}$$

The RMSE value should be as close to zero as possible..

3) Relative dimensionless global error (ERGAS) [7] is the normalized version of the RMSE designed to calculate the spectral distortion between the reference image and the resolution-enhanced image, i.e.,

$$ERGAS = 100\frac{h}{l}\sqrt{\frac{1}{N}\sum_{i=1}^{N}\Delta\left(X_H^{(i)}, \hat{X}_H^{(i)}\right)^2 / M_i^2} \tag{5}$$

Where h/l is the ratio between the pixel sizes of the reference HR image and the LR image and is the mean radiance of the th spectral band in the reference image. The ERGAS should be as close to zero as possible.

4) is the correlation between each band of the reference image and the resolution-enhanced image, i.e.,

Where $v^{(i)}$ and $v^{(i)}$ are the mean values of the corresponding spectral band. The *CC* value should be as close to one as possible.

$$CC = \frac{1}{N}\sum_{i=1}^{N}\frac{\sum_{x,y}\left(v^{(i)}(x,y) - \bar{v}^{(i)}\right)\left(\hat{v}^{(i)}(x,y) - \bar{\hat{v}}^{(i)}\right)}{\sqrt{\sum_{x,y}\left(v^{(i)}(x,y) - \bar{v}^{(i)}\right)^2\sum_{x,y}\left(\hat{v}^{(i)}(x,y) - \bar{\hat{v}}^{(i)}\right)^2}} \tag{6}$$

Experiments are conducted to compare the performance of the proposed approach with bilinear interpolation, bicubic interpolation and DWT-based interpolation. In the first experiment, we test the performance of different methods on enhancing the resolution of the input LR image by a factor of two in both spatial dimensions. For this, the ones in Fig. 2(a) and (b) are used as the reference HR image and the input LR image, respectively. Different resolution enhancement methods are applied to that in Fig. 2(b) to estimate the reference HR image, as shown in Fig. 2(a). Fig. 2(c), (d), (e), and (f) show the subimages cropped from the results of different resolution enhancement methods. The spectral distortions on the enhanced images can be noticed. It can be observed that wavelet-domain methods achieve better visual quality than that of the spatial-domain methods. To evaluate the spectral quality quantitatively, the aforementioned metrics are calculated for different methods, and the results are shown in Table I. It is clear that the values of the metrics get closer to the optimal one when using the proposed method.

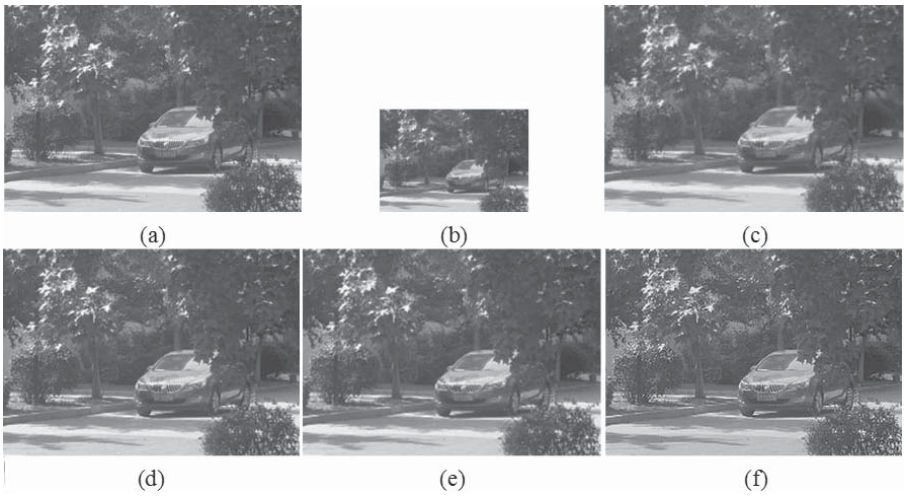


Figure 2 *Results of spatial resolution enhancement with a factor of two in both spatial dimensions. (a) Reference HR test image. (b) LR image of (a) with a downsampling factor of two. (c) Resolution-enhanced image using bilinear interpolation. (d) Resolution-enhanced image using bicubic interpolation. (e) Resolution-enhanced image using DWT-based interpolation. (f) Resolution-enhanced image using the proposed method.*

Table 1 *Spectral Quality Metrics for Fig.2 Using Different Resolution Enhancement Methods*

	Quality Index	RMSE	ERGAS	CC
Reference values	1.0000	0.0000	0.0000	1.0000
Bilinear interpolation	0.5988	32.5969	6.1660	0.9328
Bicubic interpolation	0.6081	32.1703	6.0853	0.9547
DWT-based interpolation	0.7689	23.2654	4.4009	0.9768
Proposed method.	0.8415	18.4968	3.5402	0.9814

In the second experiment, the resolution enhancement methods are applied twice to the LR input image, as shown in Fig. 3(b), to test their performances when the spatial resolution enhancement factor is four in both spatial dimensions. The subjective results are shown in Fig. 3(c), (d), (e), and (f), and the corresponding quantitative results computed using the aforementioned metrics are shown in Table II. The spectral deformations resulted from using the spatial-domain methods are apparent. Such deformations are reduced by employing the wavelet-domain methods. Furthermore, it is clear that the proposed resolution enhancement method shows better performance than that of the other methods.

In the second experiment, the resolution enhancement methods are applied twice to the LR input image, as shown in Fig. 3(b), to test their performances when the spatial resolution enhancement factor is four in both spatial dimensions. The subjective results are shown in Fig. 3(c), (d), (e), and (f), and the corresponding quantitative results computed using the aforementioned metrics are shown in Table II. The spectral deformations resulted from using the spatial-domain methods are apparent. Such deformations are reduced by employing the wavelet-domain methods. Furthermore, it is clear that the proposed resolution enhancement method shows better performance than that of the other methods.

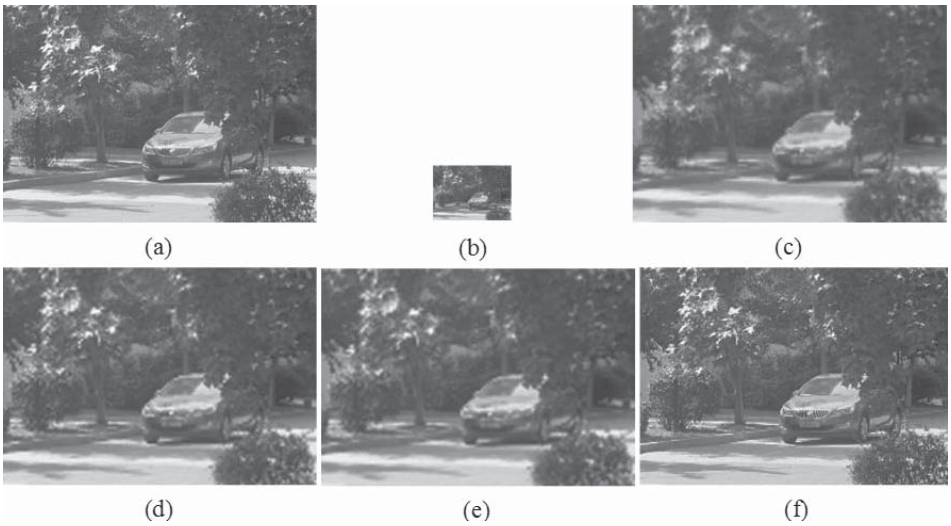


Figure 3 *Results of spatial resolution enhancement with a factor of four in both spatial dimensions. (a) Reference HR test image. (b) LR image of (a) with a downsampling factor of four. (c) Resolution-enhanced image using bilinear interpolation. (d) Resolution-enhanced image using bicubic interpolation. (e) Resolution-enhanced image using DWT-based interpolation. (f) Resolution-enhanced image using the proposed method.*

We compare the computation times required by each of the image resolution enhancement methods in generating the HR image using the input LR image, as shown in Fig. 2(b), on a laptop which is operated by 32-bit Windows7 with 3.3 GHz Intel Dual Core 4 CPU and 2 GB RAM. The methods presented in this paper are implemented in MATLAB7.0. It takes 4, 10, 39, and 58 s for bilinear interpolation, bicubic interpolation, DWT-based interpolation and the proposed method, respectively, to produce the resultant HR image. It is not difficult to find out that the proposed method has a higher computational cost.

Table 2 *Spectral Quality Metrics for Fig.3 Using Different Resolution Enhancement Methods*

	Quality Index	RMSE	ERGAS	CC
Reference values	1.0000	0.0000	0.0000	1.0000
Bilinear interpolation	0.4096	36.9070	7.9112	0.9090
Bicubic interpolation	0.4126	35.0248	7.8361	0.9085
DWT-based interpolation	0.4024	37.1817	6.2643	0.9073
Proposed method.	0.5015	33.8993	5.2569	0.9289

CONCLUSION

A method for image resolution enhancement from a single LR image using the complex wavelet transform has been presented. The initial rough estimate of the HR image is decomposed to estimate the complex-valued high-pass wavelet coefficients for the input LR image. The estimated complex wavelet coefficients are used, together with the input LR image, to reconstruct the resultant HR image by employing the inverse complex wavelet transform. Extensive tests and comparisons with other methods show the superiority of the method presented in this paper. The proposed resolution enhancement method retains both intensity and features of the LR image.

REFERENCES

1. L. Zhang and X. Wu. An edge-guided image interpolation algorithm via directional filtering and data fusion. *IEEE Trans. Image Process.,* 2006,15(8): 2226–2238.
2. K. Kinebuchi, D. D. Muresan, T. W. Parks. Image interpolation using wavelet-based hidden Markov trees. *Proc. IEEE Int. Conf. Acoustic, Speech, Signal Process.*, 2001:1957–1960.
3. S. Chang, Z. Cvetkovic, M. Vetterli. Locally adaptive wavelet-based image interpolation. *IEEE Trans. Image Process*., 2006, 15(6): 1471–1485.
4. A. Temizel and T. Vlachos. Wavelet domain image resolution enhancement using cycle-spinning. *Electron. Lett*., 2005, 41(3): 119–121.
5. N. Kingsbury. Complex wavelets for shift invariant analysis and filtering of signals. *Appl. Comput. Harmonic Anal*. 2001, 10(3): 234–253.
6. L. Alparone, S. Baronti, A. Garzelli, and F. Nencini. A global quality measurement of pan-sharpened multispectral imagery. *IEEE Geosci. Remote Sens. Lett*., 2004, 1(4): 313–317.
7. L. Wald. Quality of high resolution synthesized images: Is there a simple criterion?. in *Proc. Int. Conf. Fusion Earth Data*, 2000: 99–103.
8. MATLAB Indexing. Mathworks. Subscripted Indexing Available: http: //www. mathworks. cn/ support/ tech-notes/1100/1109. html, March 24, 2012

UDC: 343.982.34

THE RESEARCH OF EFFECT FACTORS ON DEVELOPING LATENT FINGERPRINTS USING THE 1,2-INDANEDIONE REAGENT

Limei Zhang[1]
Zhongliang Zhang[1]
National Police University of China, Department of Trace Inspection Technology, Shenyang
Dongdong Zhang[2]
National Police University of China, Department of Public Security Intelligence, Shenyang

Abstract: 1,2-Indanedione is an emerging finger mark reagent used on porous surfaces. The general consensus is that this reagent is at least as sensitive as DFO, with some research showing higher sensitivity for 1,2-indanedione as opposed to DFO. The experiments undertaken in this study are aimed to investigate the influence of the external factors, such as the coating of surfactant, zinc chloride solution concentration and ambient humidity on developing latent fingerprints using the 1,2-indanedione reagent. By comparing the developing performance of the 1,2-indanedione reagent with different experimental conditions, the optimized formula was obtained.

Keywords: forensic science, fingerprints, 1,2-indanedione, humidity.

INTRODUCTION

Since the discovery of 1,2-indanedione in 1912 and its reaction with amines and amino acids to yield fluorogenic products, this reagent has earned a prominent position in forensic chemistry.[1-2]The 1,2-indanedione reagent was initially trialled as a latent finger mark reagent after it was isolated as an intermediate in the production of 5-methylthioninhydrin.[3] Following the publication of this initial study, several research groups conducted further trials to determine the suitability of 1,2-indanedione as a luminescent alternative to ninhydrin for fingerprint detection on paper substrates.[4–6]

Previous studies into the optimization and evaluation of the 1,2-indanedione reagent indicated that the reaction between 1,2-indanedione and amino acids is highly sensitive to the chemistry of the paper substrate, procedure, zinc chloride solution concentration, ambient humidity and the application of heat.[7-8] Research into the 1,2-indanedione reagent by the University of Technology, Sydney (UTS) in conjunction with the Australian Federal Police (AFP) indicated that the performance of the reagent reduced dramatically in low relative humidity conditions, leading to the inference that the reaction requires the presence of water in a similar manner to that of ninhydrin.[9] Furthermore, the addition of a 1:25 molar ratio of ethanolic zinc chloride solution to1,2-indanedione in the working solution was shown to significantly improve the performance of the 1,2-indanedione reagent in low humidity environments.[10] Zinc ions were initially considered to form a complex with Joullie's pink in the same manner as for the ninhydrin reaction product when applied as a post treatment, with research by Ramotowski et al. and Hauze et al. demonstrating a darkening of indanedione-developed finger marks upon the application of ethanolic zinc chloride solution.[11]

The experiments undertaken in this study are aimed to investigate the influence of the external factors on developing latent fingerprints using the 1,2-indanedione reagent. By comparing the developing performance of the 1,2-indanedione reagent with different experimental conditions, such as the coating of surfactant, zinc chloride solution concentration and ambient humidity, the ultimate objective of this study was to optimize the 1,2-indanedione reagent using in developing latent fingerprints.

EXPERIMENT

Collection of latent finger mark samples

Latent finger mark impressions were taken from a single donor, unless otherwise stated. When replicates of latent impressions were required from a single donor, they were collected periodically over a 7 h

period. Finger marks were collected after carrying out a grooming procedure developed for the study prior to laying down the finger marks. This was intended to mimic natural behaviour and minimize variability due to exogenous sources. The grooming procedure was as follows: (1) hands were washed three times thoroughly with soap; (2) fingers were then gently wiped across the forehead; (3) latent finger marks were deposited onto the paper substrates lightly with good quality.

Development of Latent finger mark samples

Latent fingerprint samples developed by dipping and heat treatment were dipped into a working solution, allowed to air dry in the fume cupboard, then heat treated in drying cabinet (100., 15-20min).

Photography of samples

Samples were photographed in both absorbance (white-light) mode and luminescence mode using a Nikon D60 digital camera. Illumination in absorbance mode was achieved using incandescent light bulbs with no camera filter attachments. Illumination in luminescence mode was achieved using a RofinPolilight^{R} PL500 (Rofin, Australia), with an excitation wave length of 505 nm and an orange camera filter attachment (550 nm barrier filter).

RESULTS AND DISCUSSION

Effect of surfactant on the 1,2-indanedione reagent

Four groups of experiment were designed to investigate the influence of the surfactant on developing performance of the 1,2- indanedione reagent.

1: 0.03g 1,2-indanedione+27ml ethyl acetate+4mlglacial acetic acid+29ml trichlorotrifluoroethane

2: A Liquid: 0.03g 1,2-indanedione+27ml ethyl acetate

B Liquid: 0.24ml PE-68+2ml ethanol

Working Solution: A+B Liquid+4mlglacial acetic acid+26ml trichlorotrifluoroethane

3: A Liquid: 0.03g 1,2-indanedione+24ml ethyl acetate

B Liquid: 0.24ml PE-68+2ml ethanol

Working Solution: A Liquid+B Liquid+4mlglacial acetic acid+29ml trichlorotrifluoroethane

4: A Liquid: 0.03g 1,2-indanedione+27ml ethyl acetate

B Liquid: 0.24ml PE-68+2ml ethanol

Working Solution: A+B Liquid+2mlglacial acetic acid+29ml trichlorotrifluoroethane

The following Table 1 shows the developing performance of the four groups' reagent. The performances of the first and fourth working solutions appear better. Therefore, surfactant have little effect on the performance of the 1,2 indanedione reagent.

Table1 *Developing performance of the four groups*

Groups / Substrates	1	2	3	4
Printing paper	+++	++	++	++
Newspaper	++	++	++	++
Pictorial paper	+++	+	++	+++
Envelope Paper	++	-	++	++

Notes: The signal "+++" Shows the better performance, the coherent and clear finger ridge and the strong fluorescent solution; The signal "++" Shows the coherent and clear finger ridge and the strong fluorescent solution; The signal "+" Shows the coherent or clear finger ridge; The signal "-" Shows the common performance, the vague finger ridge.

Effect of zinc ionon the 1,2- indanedione reagent

The addition of Zn^{2+} to 1,2-indanedione processing, be it as a post treatment application or integrated within the solution itself, has proven to enhance the fluorescence results obtained with the reagent. It has been postulated that this may result from Zn^{2+} serving as a Lewis Acid, thereby accelerating the reaction. Additionally, the stabilization of the fluorescent dipole results from addition of this metal, increasing the longevity of the print once developed. Secondary application of $ZnCl_2$ to a 0.5% w/v working solution (0.03 g 1,2-indanedione + 27 ml ethyl acetate + 4 ml glacial acetic acid + 28 ml trichlorotrifluoroethane) results in very chromatic, pink visible colour development and strong fluorescence. However, the integration of $ZnCl_2$ into the working solution is desirable in that it decreases processing time and complexity. Therefore, various levels of $ZnCl_2$ were evaluated to determine if any afforded the same strength of colour and fluorescence as did the post treatment process. Levels of 10, 20, 30, and 40% v/v were added to0.5% w/v stock solution and this combined formulation used in the processing of prints. Comparisons were then made among stock solution, stock solution with a secondary application of $ZnCl_2$, and the aforementioned combined formulations, shown as Table 2.

Table 2 *Developing performance of the six groups*

Concentration / Substrates	Stock solution	10	20	30	40	Secondary process
Printing paper	+++	+++	++	+	++	+++
Newspaper	++	+++	+++	++	++	+++
Pictorial paper	++	+++	++	++	+	+++
Envelope Paper	++	+++	+	+	+	++

Notes: The signal "+++" Shows the better performance, the coherent and clear finger ridge and the strong fluorescent solution; The signal "++" Shows the coherent and clear finger ridge and the strong fluorescent solution; The signal "+" Shows the coherent or clear finger ridge; The signal "-" Shows the common performance, the vague finger ridge.

A decrease in performance was realized when this concentration was increased to the levels of 10% and 40%. Therefore, for the subsequent comparisons with the stock solution, the 10% formulation (1 mL of ZnCl2 per 10 mL of stock solution) was utilized.

Effect of humidity on the 1,2- indanedione reagent

1,2-Indanedione has been noted to perform inconsistently among laboratories worldwide. Table 3 shows the performance of the 1,2- indanedione reagent in different air humidity.

Table3 *Developing performance of the two groups*

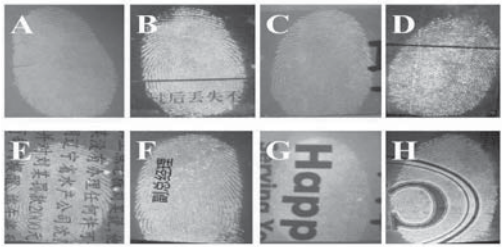
Humidity / Substrates	20%	60%
Printing paper	+++	+++
Newspaper	+++	+++
Pictorial paper	+	+++
Envelope Paper	+	+++

Notes: The signal "+++" Shows the better performance, the coherent and clear finger ridge and the strong fluorescent solution; The signal "++" Shows the coherent and clear finger ridge and the strong fluorescent solution; The signal "+" Shows the coherent or clear finger ridge; The signal "-" Shows the common performance, the vague finger ridge.

During the process of developing, the temperature remained relatively constant, the % RH ranged from 40% to 70%. When the % RH was relatively low, prints processed using the laboratory oven method showed little colour development, although fluorescence was typically adequate for identification purposes. However, when the % RH was relatively high, the samples processed using this same method demonstrated dark colour development and strong fluorescence. This finding corresponded with the observations of Wallace-Kunkelet al., in which performance differences were noted concerning two locales, one with a higher % RH than the other.[8] The potential impact of humidity exposure to print quality when using 1,2- indanedione as a reagent was mentioned in the work of Azoury et al., to be potentially attributable to a complex phenomenon involving paper, sweat, reagent, and water .[12]

Optimization of 1,2- indanedione reagent

By comparing the developing performance of the 1,2-indanedione reagent with different experimental conditions, such as the coating of surfactant, zinc chloride solution concentration and ambient humidity, the optimized experimental conditions were obtained. The next figure shows the fluorescence results of the optimized formula on different paper substrates.



Fluorescence results of the optimized formula on different paper substrates: A printed paper; B bill; C pictorial; D deposit slip; E newspaper; F business card; G cups; H admission ticket.

CONCLUSION

The optimization and evaluation of the 1,2-indanedione reagent indicated that the reaction between 1,2-indanedione and amino acids is highly sensitive to zinc chloride solution concentration and ambient humidity. A decrease in performance was realized when this concentration was increased to the 10% and 40% levels. The performance of the reagent increased dramatically in high relative humidity conditions. The optimized formula (10% zinc chloride solution concentration, 60% relative humidity) was obtained.

REFERENCES

1. Hansen, D. B.; Joullié, M. M., Chem. Soc. Rev. 2005, 34, 408.
2. Hauze, D. B.; Petrovskaia, O.; Taylor, B.; Joullie, M. M.; Ramotowski,R.; Cantu, A. A., J. Forensic Sci. 1998, 43, 744.
3. R. Ramotowski, A. Cantu, M. Joullie, O. Petrovskaia, 1,2-indanediones: a preliminary evaluation of a new class of amino acid visualizing compounds, Fingerprint World 23 (1997) 131–140.
4. J. Almog, E. Springer, S. Wiesner, A. Frank, O. Khodzhaev, R. Lidor, E. Bahar, H.Varkony, S. Dayan, S. Rozen, Latent fingerprint visualization by 1,2-indanedioneand related compounds: preliminary results, J. Forensic Sci. 44 (1999) 114–118.
5. S. Wiesner, E. Springer, Y. Sasson, J. Almog, Chemical development of latent fingerprints: 1,2-indanedione has come of age, J. Forensic Sci. 46 (2001) 1082–1084.
6. C. Roux, N. Jones, C. Lennard, M. Stoilovic, Evaluation of 1,2-indanedione and 5,6-dimethoxy-1,2-indanedione for the detection of latent fingerprints on porous surfaces, J. Forensic Sci. 45 (2000) 761–769.
7. R. Jelly, E. L. T. Patton, C. Lennard, S. W. Lewis and K. F. Lim, The Detection of Latent Finger marks on Porous Surfaces Using Amino Acid Sensitive Reagents: A Review, Anal. Chim. Acta, 2009, 652, 128–142.
8. C. Wallace-Kunkel, C. Lennard, M. Stoilovic and C. Roux, Optimisation and evaluation of 1,2-indanedione for use as a finger mark reagent and its application to real samples, ForensicSci. Int., 2007, 168, 14–26.
9. C. Wallace-Kunkel, Thesis Evaluation of Reagents for the Chemical Enhancement of Finger marks on Porous Surfaces: Optimisation and Characterisation of the 1,2-indanedione Technique Type thesis, University of Technology, Sydney (Ultimo),2008.
10. M. Stoilovic, C. Lennard, C. Wallace-Kunkel, C. Roux, Evaluation of a 1,2-indanedioneformulation containing zinc chloride for improved finger mark detection on paper, J. Forensic Ident. 57 (2007) 4–18.
11. D.B. Hauze, O. Petrovskaia, B. Taylor, M.M. Joullie, R. Ramotowski, A.A. Cantu, 1,2-indanediones: new reagents for visualizing the amino acid components of latent prints, J. Forensic Sci. 43 (1998) 744–747.
12. Azoury M, Gabbay R, Cohen D, Almog J. ESDA processing and latent fingerprint development: the humidity effect. J Forensic Sci2003;48(3):564–70.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

343.85(082)
343.98(082)
343.533::004(082)

MEĐUNARODNI naučni skup "Dani Arčibalda Rajsa" (2015 ; Beograd)

Thematic Conference Proceedings of International Significance. Vol. 3 / International Scientific Conference "Archibald Reiss Days", Belgrade, 3-4 March 2015 ; [organized by] Academy of Criminalistic and Police Studies ; [editors Đorđe Đorđević ... et al.] = Tematski zbornik radova međunarodnog značaja. Tom 3 / Međunarodni naučni skup "Dani Arčibalda Rajsa", Beograd, 3-4. mart 2015. ; [organizator] Kriminalističko-policijska akademija ; [urednici Đorđe Đorđević ... et al.]. - Belgrade : Academy of Criminalistic and Police Studies = Beograd : Kriminalističko-policijska akademija, 2015 (Belgrade : Official Gazette = Beograd : Službeni glasnik). - XIV, 468 str. : ilustr. ; 24 cm

Tiraž 200. - Preface: str. IX. - Napomene i bibliografske reference uz tekst. - Bibliografija uz svaki rad.

ISBN 978-86-7020-321-1
ISBN 978-86-7020-190-3 (za izdavačku celinu)

1. Up. stv. nasl. 2. Kriminalističko-policijska akademija (Beograd)
a) Криминалитет - Сузбијање - Зборници b) Криминалистика - Зборници
c) Полиција - Зборници

COBISS.SR-ID 217206284