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

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

MEĐUNARODNI NAUČNI SKUP
INTERNATIONAL SCIENTIFIC CONFERENCE

„DANI ARČIBALDA RAJSA“

“ARCHIBALD REISS DAYS”

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

TEMATSKI ZBORNIK RADOVA MEĐUNARODNOG ZNAČAJA

THEMATIC CONFERENCE PROCEEDINGS OF INTERNATIONAL SIGNIFICANCE

TOM III
VOLUME III

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

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

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

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

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

Computer Design
MILOŠ IVOVIĆ
JOVAN PAVLOVIĆ
DRAGOLJUB MILUTINOVIĆ

Impression
200 copies

Print
Univerzal, Čačak

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

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

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

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

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

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

Tehničko uređenje
MILOŠ IVOVIĆ
JOVAN PAVLOVIĆ
DRAGOLJUB MILUTINOVIĆ

Tiraž
200 primeraka

Štampa
Univerzal, Čačak

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

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

HONORARY COMMITTEE

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

International members

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

PROGRAMME COMMITTEE

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

PREFACE

Dear readers,

In front of you is the Thematic Collection of Papers presented at the International Scientific Conference "Archibald Reiss Days", which was organized by the Academy of Criminalistic and Police Studies in Belgrade, in cooperation with the Ministry of Interior and the Ministry of Education, Science and Technological Development of the Republic of Serbia, School of Criminal Justice, Michigan State University in USA, School of Criminal Justice University of Laussane in Switzerland, National Police Academy in Spain, Police Academy Szczytno in Poland, National Police University of China, Lviv State University of Internal Affairs, Volgograd Academy of the Russian Internal Affairs Ministry, Faculty of Security in Skopje, Faculty of Criminal Justice and Security in Ljubljana, Police Academy "Alexandru Ioan Cuza" in Bucharest, Academy of Police Force in Bratislava, Faculty of Security Science University of Banja Luka, Faculty for Criminal Justice, Criminology and Security Studies University of Sarajevo, Faculty of Law in Montenegro, Police Academy in Montenegro and held at the Academy of Criminalistic and Police Studies, on 7, 8 and 9 November 2017.

The International Scientific Conference "Archibald Reiss Days" is organized for the seventh time in a row, in memory of the founder and director of the first modern higher police school in Serbia, Rodolphe Archibald Reiss, after whom the Conference was named. The Thematic Collection of Papers contains 131 papers written by eminent scholars in the field of law, security, criminalistics, police studies, forensics, informatics, as well as by members of national security system participating in education of the police, army and other security services from Belarus, Bosnia and Herzegovina, Bulgaria, Bangladesh, Abu Dhabi, Greece, Hungary, Macedonia, Romania, Russian Federation, Serbia, Slovakia, Slovenia, Czech Republic, Switzerland, Turkey, Ukraine, Italy, Australia and United Kingdom. Each paper has been double-blind peer reviewed by two reviewers, international experts competent for the field to which the paper is related, and the Thematic Conference Proceedings in whole has been reviewed by five competent international reviewers.

The papers published in the Thematic Collection of Papers provide us with the analysis of the criminalistic and criminal justice aspects in solving and proving of criminal offences, police organization, contemporary security studies, social, economic and political flows of crime, forensic linguistics, cybercrime, and forensic engineering. The Collection of Papers represents a significant contribution to the existing fund of scientific and expert knowledge in the field of criminalistic, security, penal and legal theory and practice. Publication of this Collection contributes to improving of mutual cooperation between educational, scientific and expert institutions at national, regional and international level.

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

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

Belgrade, October 2017 *Programme and Organizing Committees*

TABLE OF CONTENTS

TOPIC V

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

Zoran Djurdjevic, Branko Lestanin
INTELLIGENCE-LED POLICING IN THE MINISTRY OF INTERIOR OF THE REPUBLIC OF SERBIA 3

Barbora Vegrichtová
INTERPRETATION OF CRIMINAL TATTO SYMBOLS IN PRISON FACILITIES 17

Mirko Kulić, Goran Milošević, Cvjetana Cvjetković
SUBJECTS IN TAX LAW RELATIONS IN THE REPUBLIC OF SERBIA 25

Slobodan Miladinovic
APPLICATION OF GEOINFORMATION TECHNOLOGIES AND GEOGRAPHIC METHODS IN ASSESSING THE VULNERABILITY OF POTENTIAL TERRORIST TARGETS IN THE LOCAL COMMUNITY 37

Marko Dimitrijević
THE CONTRIBUTION OF THE EUROPEAN COURT OF AUDITORS IN THE FIGHT AGAINST THE FINANCIAL CRIME 49

Suzana Dimić, Mirjana Đukić
TAX FRAUD AND PLEA BARGAINING 57

Dragomir Jovičić, Gojko Šetka
ORGANIZATION OF THE POLICE SYSTEM IN BOSNIA AND HERZEGOVINA 67

Dragan Cvetković, Marija Mićović, Marta Tomić
REPRESSIONOF CRIMINAL ACTS IN THE FIELD OF GREY ECONOMY IN THE REPUBLIC OF SERBIA 75

Ivica Lazovic
PRIVATIZATION AND GROWTH OF GREY ECONOMY AS FOLLOWERS OF TRANSITION 87

TOPIC VII

Cybercrime

Milan Čabarkapa, Milan Prokin , Goran Šimić, Nataša Nešković, Đurađ Budimir
INTERNET OF INSECURE THINGS 101

Dragan Randjelović, Aleksandar Miljković, Vladimir Stojanović, Vladimir Jovanović, Aleksa Maksimović
POSSIBILITIES FOR COMPARISON OF DATA RECOVERY SOFTWARE FOR MOBILE DEVICES 111

Srđan Milašinović, Zoran Jevtović
THE ROLE OF CYBER SPACE IN TRANSFORMING CONFLICT PARADIGM 131

Zoran Aracki, Ladin Gostimirović
SOCIAL NETWORKS AS A SAFETY FACTOR OF THE MIGRANT CRISIS..... 139

Natalia Khodyakova, Olga Krachinskaya
PREVENTION OF CYBERCRIME BY PEDAGOGICAL WAYS 151

Saša Živanović, Brankica M. Popović
NEW CHALLENGES IN FIGHTING FINANCIAL CYBERCRIME..... 159

Dalibor Vorkapić, Aleksandra Tomašević, Miljana Mladenović, Ranka Stanković, Nikola Vulović
DIGITAL LIBRARY FROM A DOMAIN OF CRIMINALISTICS AS A FOUNDATION FOR A FORENSIC TEXT ANALYSIS 169

Lepiokhin Alexander
THEORETICAL RESEARCH OF INFORMATION AND ITS PROPERTIES IN THE EXERCISE OF INFORMATION AND ANALYTICAL WORK..... 181

Bulai Iurie, Bulai Rodica
CYBERCRIME, AS WELL AS INTERNATIONAL CYBER THREATS AND THEIR SOLUTIONS 189

Mladen Živković, Petar Čisar, Imre Rudas
VULNERABILITY TESTING USING METASPLOIT FRAMEWORK 201

Petar Milić, Kristijan Kuk, Jelena Mišić, Stefan Kartunov
SECURITY ASSESSMENT OF UNIVERSITY WEBSITES IN SERBIA BY USING AUTOMATED BLACK BOX TESTING 211

Svetlana Nikoloska
CRIMINOLOGICAL AND CRIMINALISTIC CHARACTERISTICS OF COMPUTER CRIME IN THE REPUBLIC OF MACEDONIA 221

Dijana Jankovic
CYBER CRIME, VIRTUAL CURRENCIES AND FUTURE REGULATION..... 235

Jelena Matijašević-Obradović, Ivan Joksić
HOW DIFFICULT IS TO PROVE THE CRIMINAL ACTS IN THE FIELD OF CYBERCRIME?..... 249

Miladin Ivanović, Slobodan Nedeljković, Predrag Djikanović, Vojkan Nikolić
SPECIALIZED ICT SYSTEM FOR SAFE TRANSFER OF CONFIDENTIAL DATA BY APPLICATION OF CRYPTOGRAPHIC METHODS IN COMPUTER NETWORKS 263

Nebojša Jokić, Aleksandar Maksimović
THE IMPORTANCE OF EDUCATION AND RAISING AWARENESS AMONG CITIZENS ABOUT DIFFERENT FORMS OF ATTACKS IN CYBER SPACE 271

Qiang Fan
THE STUDY ON PREVENTION METHODS OF TELECOM FRAUD CRIME IN "INTERNET +" ERA 287

TOPIC VIII

Innovative Techniques and Equipment in Forensic Engineering

Andy Bécue
FINGERMARK DETECTION: SHOULD WE TAKE THE RED PILL OR THE BLUE PILL? 295

Aleksandra Vulović, Venezija Ilijazi, Stevo Jaćimovski
ANALYSIS OF TURBULENT DIFFUSION MODEL WITH VARIABLE COEFFICIENTS IN CASE OF STATIONARY POINT SOURCES 307

Anka Tutulugdžija, Radovan Radovanović, Jelena Lamovec
VISUALIZATION OF LATENT FINGERPRINTS BY ELECTROCHEMICAL DEPOSITION OF METALLIC THIN FILMS 321

Smilja Teodorović, Dejan Jović, Vera Raičević
THE ROLE OF MICROORGANISMS AS CRIME-FIGHTING TOOLS IN MODERN DAY FORENSIC SCIENCE 329

Nikola Milašinović, Bojana Vidović, Bojan Čalija
CHROMATOGRAPHIC TECHNIQUES AS RELIABLE TOOLS FOR AUTHENTICATION AND ADULTERATION OF DIETARY SUPPLEMENTS 339

Dmitry Sergeevich Korovkin
MODERN TECHNOLOGIES OF FORENSIC BALLISTICS EXAMINATIONS 353

Aleksandar Mićović, Stevan Jovičić, Nenko Brkljač
TESTING OF FIRE EXTINGUISHERS – BETWEEN EUROPEAN AND NATIONAL REGULATIONS 363

Biljana Koturević, Ana Branković
FORENSIC COURSE DEVELOPMENT. NEW DIRECTIONS IN FORENSIC EDUCATION 375

Feng Xu
RESEARCH ON HOW TO REMOVE BACKGROUND DISTURBANCE WITH SHORT-WAVE ULTRAVIOLET BASED ON FULL BAND CCD 383

TOPIC IX

Effects of Physical Activity on Anthropological Status in Security Agency Personnel

Milivoj Dopsaj, Marko Vuković
PERCENT OF BODY FAT STANDARDS FOR SERBIAN MALE POLICE OFFICERS 393

Bojan Mitrović, Goran Vučković
SPECIAL PHYSICAL EDUCATION AS A PART OF SPECIALIZED POLICE TRAININGS AT THE MINISTRY OF INTERIOR OF THE REPUBLIC OF SERBIA 403

Vladimir Timotijević, Nenad Koropanovski
POLICE ACADEMY STUDENTS INITIAL LEVEL OF FLEXIBILITY: A PILOT STUDY 413

Milos Mudric, Srecko Jovanovic, Aleksandar Nedeljkovic, Ivan Cuk, Slobodan Jaric
PERCEPTIVE ABILITIES IN DEFENSIVE TASKS AGAINST DIFFERENT ATACKS.....423

Aleksandar Cvorovic, Ahmad Al Maamari
DIFFERENCES IN KEY PERFORMANCE INDICATORS BETWEEN POLICE COLLEGE CADETS IN DIFFERENT SEMESTERS OF THEIR EDUCATION.....429

Filip Kukic, Mohammed Abdul Aziz Shamel Al Maamari
EVALUATION OF THE AEROBIC FITNESS IN ABU DHABI POLICEMEN.....439

Radivoje Janković
CORRELATION BETWEEN BODY COMPOSITION AND PHYSICAL FITNESS OF THE POLICE OFFICERS.....449

Raša Dimitrijević
CHANGES IN INDICATORS OF MUSCLE FORCE IN FEMALE STUDENTS OF THE ACADEMY OF CRIMINALISTIC AND POLICE STUDIES.....457

Velimir Jeknic, Milos Stojkovic
EFFECTS OF TWELVE-WEEK TRAINING PROGRAM ON FITNESS LEVEL AND ANTHROPOMETRIC STATUS OF POLICE COLLEGE STUDENTS.....469

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SPECIFICS OF CONFLICTS IN CYBERSPACE

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

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

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

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

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

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

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

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

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

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

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

SOCIAL NETWORKS AS POLYGONS OF CONFLICT

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

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

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

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

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

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

20 Group UMBRAGE, belonging to the CIA department for remote devices, collects and maintains huge file offensive techniques that are "stolen" from malware produced in other countries. Thus, the US can redirect the service identification of the perpetrator by leaving behind a "fingerprint" of the groups from which the attack technique is stolen.

cantly increased. It gives various offers of illegal trade matters, from narcotics, weapons and criminal services, to information about vulnerabilities or even service cyber-attacks, such as for example: *The Real Deal Market*, *Silk Road* and others. Digital markets are unlimited, hence they are dynamic due to the rapidly changing nature of crime sites, which is understandable because the same information that is the subject of trade has long life as it can be used only until being unknown. In practice, it is quite common that representatives of the intelligence and security agencies are involved in covert trade and monitoring activities on these forums.[21]

With the digitization, the sphere of security, particularly crime and terrorism, has undergone deep and significant changes since all common digital series of strikes have resulted in conflictological activities that disrupt the stability of other social subsystems. Hence, the semantic interpretation of reality turns into a specific power that breaks the security mechanisms of the state border or preventive barriers, directing the entire community to redefined patterns of behavior and safety culture. *YouTube*, *Facebook*, *MySpace*, *Twitter* and the like social networks, with the convergence of IT tools imperceptibly change the traditional communicational techniques whereby increasingly becoming the important sources of information, especially in crisis situations. Life in virtual communities is increasingly being reflected in developments in the real environment which in the field of security is reflected in the radicalization of information management and increasing tendency of terrorism, crime, violence and related forms of deviant behavior. Using new technologies, hostile attack or criminal activity can be realized from a long distance and hidden locations, with actors who have never met or known each other, which in practice results in new forms of conflict.

The amount of data in transnational environment in a short time has increased enormously, so that its processing requires specific tools, algorithms and programs that are constantly upgrading and improving. Digital sphere is not alienated from reality, because it exists where the information can create, store, disclose, send, receive, process and destroy the application of computer information systems within the electromagnetic fields. Their comprehensiveness, interactivity and invisibility in new forms of monitoring provide unimaginable scope because the chain of control increases with each contact "persons of special interests", constantly expanding the network structure. For example, if the operative person of interest has only 10 friends on *Facebook*, the analyst responsible for tracking personal contacts at the NSA or in some private agencies working for this service may without a writ follow the communication of friends of friends' friends, up to three "jumps" - as some 266.955 people.[22]With only 300 likes that someone left on the social network, an expert in the data science can create a psychological profile of all relevant data to be used for trade in the world's largest companies! *Instagram* uses a camera to take pictures and shots, *Gmail* has the access to our directory, *Viber* knows our exact location at any time, while *Facebook* can read all of our SMS messages. When WikiLeaks officially announced that the US intelligence services have developed effective methods for hacking devices such as *iPhone* and *Android phones* as well as *Samsung* "smart" TVs, allowing them to monitor communications even when the devices are turned off, the public was puzzled if that was true. Available documents also reveal malware, viruses and security holes called "zero days", along with hundreds of millions of lines of computer code used by the CIA, and the ability of its staff to hack devices and messages before they are encrypted by applications like *WhatsApp*, *Signal*, *Telegram*, *Confide* and others, for which the public feels that they are safe. This means that the Internet canceled the privacy of users, but also that the way of collecting, processing and diffusion of data is radically altered. Digitization has brought large amounts of trans-national data in the sphere of national security which

21 Andy Greenberg, „New Dark-web Market is Selling Zero-day Exploits to Hackers," Wired, April 17, 2015, http://www.wired.com/2015/04/therealdeal-zero-day-exploits/ (Accessed March 22, 2017).
22 "Three degrees of separation: breaking down the NSA's 'hops' surveillance method", *Guardian*, 28.october 2013.

has caused the national sovereignty to disappear, but at the same time blurring once solid line between law enforcement and intelligence and security service.

CONCLUDING REMARKS

Cyberspace is increasingly transforming the concept of modern conflictological paradigm, whereby the leading strategists of large states recognize that they are being actively involved in the new field of confrontation. The Russian Defense Minister Sergei Shoigu, referring, to the deputies of the Duma by the end of February this year announced the creation of "information-information unit", responsible for "counter-propaganda", with Russian media reporting that he used the term "cyber army". The first man of defense said that such forces are established "to defend Russia against cyber and propaganda attacks from the West" exclusively for defensive purposes, but some of the generals disagreed with that assessment considering that Russia must have the initiative even during the peace periods. President of the *Academy of Geostrategic Issues* Colonel-General Leonid Ivashov has proposed to establish a national center that will not deal only with the western counter-propaganda, but will plan information and psychological offensive operations because the image in the minds of people is more important than the armed conflict.

A completely new era is emerging in which the possession of real information including those in the private sphere mean the power to govern the political and security environment, but some people are of the opposite opinion. For example, during the decade of searching for terrorists suspected of killing a dozen Turkish citizens for religious reasons, the German intelligence officials intercepted more than 20 million mobile phone calls, collected the data on payment transactions of 13 million credit cards, controlled more than one million data of rent-a-car users' services, registered about three hundred thousand potential suspects, which means that they tracked at the same time about 30 million people! By following digital contacts, based on the analyzed "scheme of conduct" it can reliably be predicted when some person will become "potentially dangerous", as well as the moment when that person will become a "security risk"! Security of entire community is increasingly in direct conjunction with its power to create, control and manage information flows, which means that the crisis situation occurring at the scenario can be predicted in detail.[23]

Social networks are largely influenced by the mass, but also interpersonal forms of communication emphasizing the picture and its power in the subconscious, which also reveals the increasing number of false news. Nicola Mendelsohn, the vice president of *Facebook* for Europe, Middle East and Africa, a market that holds over 430 million users, indicated the trend in the way in which users increasingly communicate, noting the explosive growth of video materials (especially after the launch *live video* option) at the expense of text messages.[24] The number of video views during 2016 increased eight times compared to the previous year (from one to over eight billion) with almost twice reduced number of text messages and print status. In fact, this is not the result of *Facebook* forcing video material but the fact that users recognize the image as a way of better, more dynamic and concise way of conveying information. In the sphere of conflictology, this means that the visual information will gain importance, whereby the privacy and ethics will increasingly be less protected.

23 US NSA is already working on a program of the so-called "dark" or "deep" Internet, which hides encrypted communications and closed networks of other countries. In the desert of Utah a new super-secret center for cyber spying and cyber-security is being built, which will cost over ten billion dollars!
24 At the press conference held on January 19, 2017 she stated that Facebook users watched per day up to 100 million hours of video of various materials, which served her as the basis for the hypothesis that **in about five years, most of our communication could be in the form of video**!

In the future, we anticipate further expansion of information technologies; it will become more complex but also more vulnerable, which means that the number of conflicts in cyberspace will grow. The comprehensive repertoire of techniques is becoming more comprehensive, from the packing of large amounts of data with some having manipulative character through the development of quantum computing, robotics and artificial intelligence to the new forms of cyber-attacks. The best method of prevention of the effective opposition is the development of safety culture and hence, the cyber conflict can be viewed through the implementation of information security in order to manage information.

LITERATURE

1. Бајагић, М. (2007): *Основи безбедности*, Криминалистичко-полицијска академија, Београд.
2. Bek, U. (2001): *Rizično društvo*, FilipVišnjić, Beograd:.
3. Bžežinski, Z. (1999): *Velika šahovska tabla*, CID, Podgorica.
4. Kešetović, Ž. i Toth, I. (2012): *Problemi kriznog menadžmenta*, Veleučilište Velika Gorica, Visoka škola za sigurnost s pravom javnosti, Centar za međunarodne i sigurnosne studije i Fakultet političkih znanosti u Zagrebu, Velika Gorica.
5. Милашиновић, С. и Јевтовић, З. (2013): *Методологија истраживања конфликата и комуницирање у савременом друштву*, Криминалистичко-полицијска академија, Београд
6. Petković, D. (2007): Uticaj internet na tradicionalne medije. *Internet i javna sfera u Srbiji* (Sitarski, Milan), Beogradska otvorena škola, Beograd.
7. Policastri, J. and Sergio D. Stone, *International Humanitarian Law*, American Society of International Law (ASIL), https://www.asil.org/sites/default/files/ERG_International%20Humanitarian%20Law%20(test).pdf (2013).
8. Rossouw von Solms and Johan van Niekerk. "From Information Security to Cyber Security". *Computers and Security* 38, (October 2013)
9. Nye J., Jr. Think Again: *Soft Power* , Foreign Policy, 2006, February