Editors
Svetlana Stanarević
Goran J. Mandić
Ljubinka Katić

THE PROCEEDINGS OF HUMAN SECURITY AND NEW TECHNOLOGIES

4TH INTERNATIONAL ACADEMIC CONFERENCE ON HUMAN SECURITY

Belgrade, 2018

THE PROCEEDINGS OF HUMAN SECURITY AND NEW TECHNOLOGIES

4TH INTERNATIONAL ACADEMIC CONFERENCE ON HUMAN SECURITY

Publisher

University of Belgrade – Faculty of Security Studies
Human Security Research Center

For The Publisher

Vladimir N. Cvetković PhD
Dean of the Faculty of Security Studies

Editors

Svetlana Stanarević, Goran J. Mandić, Ljubinka Katić

Proofreading

Danijela Nejković, Jelena Bošnjak
Faculty of Security Studies

Graphics Design

Print

Čigoja
S T A M P A

Edition

200 copies

ISBN 978-86-80144-30-6

Note

The Scientific Committee and Reviewers:

Dr Božidar Banović, Full Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Zoran Keković,** Full Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Slađana Jović,** Full Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Goran Stojanović,** Full Professor, Faculty of Technical Sciences, University of Novi Sad, Serbia; **Dr Rastko Močnik**, Full Professor, University of Ljubljana, Slovenia; **Dr Jovan Cvetić,** Full Professor**,** The Department of Microelectronics and Technical Physics, School of Electrical Engineering, University of Belgrade, Serbia; **Dr Marina Mitrevska,** Full Professor, Institute for Security, Defence and Peace Studies, UKIM, Faculty of Philosophy, Skopje, Macedonia; **Dr Bojan Radak**, Assistant Director General, Vinca Institute of Nuclear Sciences, University of Belgrade, Serbia; **Dr Oesten Baller**, Institut für Verwaltungsmodernisierung und Polizeireform in Mittel-und Osteuropa, Berlin School of Economics and Law, Berlin, Germany; **Dr Danijela Miljković**, Senior Research Associate, Department of Evolutionary Biology, Institute for Biological Research „Siniša Stanković", University of Belgrade, Serbia; **Dr Danimir Mandić,** Full Professor, Teacher Education Faculty, University of Belgrade, Serbia; **Dr Mladen Vuruna,** Full Professor, Rector, University of Defence, Belgrade, Serbia; **Dr Minas Samatas,** Full Professor, The Sociology Department, University of Crete, Greece; **Dr Nehir Varol,** Associate Professor, Ankara University – Head of Disaster and Emergency Management Department, Turkey; **Dr Bülent Sarper Ağır**, Associate Professor, Aydın Faculty of Economics, Adnan Menderes University, Turkey; **Dr Marija Babović,** Full Professor, Faculty of Philosophy, University of Belgrade, Serbia; **Dr Vesela Radović,** Senior Research Associate**,** Institute for Multidisciplinary Research, University of Belgrade, Serbia; **Dr Nada Sekulić**, Full Professor, Faculty of Philosophy, University of Belgrade, Serbia; **Dr Marijana Sumpor**, Senior Research Associate, The Institute of Economics, Zagreb, Croatia; **Dr Aleksandra Đukić,** Associate Professor, Faculty of Architecture, University of Belgrade, Serbia; **Dr Srđan Korać,** Research Fellow, Institute of International Politics and Economics, Serbia; **Dr Ivica Đorđević**, Associate Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Zoran Jeftić,** Associate Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Sanja Bijelović,** Associate Professor, Institute of Public Health, Faculty of Medicine, University of Novi Sad, Serbia; **Dr Nenad Putnik,** Associate

Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Goran J. Mandić,** Associate Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Mladen Milošević,** Associate Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Ana Kovačević,** Associate Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Jasmina Gačić**, Associate Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Vanja Roković**, Associate Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Svetlana Stanarević**, Associate Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Petar Stanojević**, Associate Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Đorđe Krivokapić**, Assistant Professor, Faculty of Organisational Sciences, University of Belgrade, Serbia; **Dr Vitomir Kovanović**, Research Fellow, School of Education Data Scientist, Teaching Innovation Unit, University of South Australia; **Dr Tomáš Strémy**, Assistant Professor, Faculty of Law,Comenius University in Bratislava, Slovakia; **Dr Filip Ejdus**, Assistant Professor**,** Faculty of Political Science, University of Belgrade, Serbia; **Dr Ljubinka Katić**, Assistant Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Milan Lipovac,** Assistant Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Danijela Spasić,** Assistant Professor, The Academy of Criminalistic and Police Studies, Serbia; **Dr Mirjana Laban**, Assistant Professor, Disaster Risk Reduction Research Centre, Department of Civil Engineering and Geodesy, Faculty of Technical Sciences, University of Novi Sad, Serbia; **Dr Milena Panić,** Research Associate, Geographical institute “Jovan Cvijić" Serbian Academy of Sciences and Arts, Serbia; **Dr Aleksandra Stupar**, Associate Professor, Faculty of Architecture, University of Belgrade, Serbia; **Dr Milena Vukmirović**, Assistant Professor, University of Belgrade, Faculty of Forestry, Serbia; **Dr Aleksandra Ilić,** Assistant Professor, University of Belgrade, Faculty of Security Studies, Serbia; **Dr Matija Zorn**, Assistant Professor, “Anton Melik” Geographical Institute, Research Centre of the Slovenian Academy of Sciences and Arts, Slovenia.

TABLE OF CONTENTS

EDITORIAL 9

PROBLEMS OF HUMAN SECURITY IN THE CONTEXT OF HYBRID AGGRESSION 11
Konstantin N. LOBANOV, Boris N. SELIN

A HISTORICAL OVERVIEW OF THE RELATION BETWEEN TECHNOLOGICAL DEVELOPMENT AND THE ABILITY TO MANAGE PERCEPTION DURING ARMED CONFLICTS 17
Nenad PUTNIK

HOW HUMAN SECURITY COULD BE A BENEFICIARY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY 25
Ivica Lj. ĐORĐEVIĆ, Ozren DŽIGURSKI

NON-LETHAL WEAPONS IN DOMESTIC LAW ENFORCEMENT: SOME LEGAL AND ETHICAL ASPECTS 39
Adelina TUMBARSKA

OPEN DATA AND AVAILABLE RESEARCH ON DEPLETED URANIUM WEAPONS – REASONS FOR CONTROVERSY (YUGOSLAVIA 1999 - CASE STUDY) 47
Nada SEKULIĆ

MASS SURVEILLANCE THROUGH RETAINED METADATA: AN OVERVIEW 59
Bojan PERKOV, Danilo KRIVOKAPIĆ, Andrej PETROVSKI

INTERCEPTION OF ENCRYPTED TELECOMMUNICATION AND THE SO-CALLED ONLINE SEARCH OF IT SYSTEMS FOR THE PURPOSE OF CRIMINAL PROSECUTION 67
Jan Dirk ROGGENKAMP

IMPACT ANALYSIS OF THE APPLICATION OF THE GDPR REGULATION ON THE FUNCTIONING OF THE INFORMATION AND COMMUNICATION SYSTEM OF THE MOI OF THE REPUBLIC OF SERBIA 75
Milan GLIGORIJEVIĆ, Radosav POPOVIĆ, Aleksandar MAKSIMOVIĆ

INTERNATIONAL INTELLIGENCE SHARING: KEY PRECONDITIONS FOR AN EFFECTIVE OVERSIGHT 83
Luka GLUŠAC

TECHNOLOGIES AND DEVELOPMENT IN VIEW OF TAX CRIMINAL OFFENCES 89
Tomáš STRÉMY, Natália HANGÁČOVÁ

JUVENILES INSIDE THE TERRORIST GROUPS 97
Božidar BANOVIĆ, Višnja RANĐELOVIĆ

PERSONALISED SECURITY: A STEP TOWARDS APPLIED HUMAN SECURITY 107
Savvas E. CHRYSOULIDIS, Phaedon KYRIAKIDIS

PERMISSION TO KILL? THE DISREGARD OF THE LEGAL REGULATIONS ON THE USE OF FIREARMS BY THE (BERLIN) POLICE AND THE ILLEGAL POLICE SHOOTING TRAINING 117
Oesten BALLER

LOCAL GOVERNMENTS' ENGAGEMENT IN INTEGRATING EMERGENCY AND ICT POLICYMAKING 127
Venelin TERZIEV, Vesela RADOVIĆ, Ekaterina ARABSKA

FLOOD RISK REDUCTION AS A CRITERION FOR VALIDATING TECHNOLOGICAL INNOVATION STRATEGIES WITH RESPECT TO HUMAN SECURITY 133
Zoran KEKOVIĆ, Jelena DINIĆ

INCREASE IN CLIMATE CHANGE AND ITS IMPACT ON THE VULNERABILITY OF SOCIAL COMMUNITIES 141
Miloš TOMIĆ, Sandra TOŠIĆ

EVACUATION CALCULATION AND MODELING: THE NEED FOR IMPROVING HUMAN LIVES SAFETY IN CASE OF FIRE 149
Mirjana LABAN, Slobodan ŠUPIĆ, Suzana DRAGANIĆ, Sanja MILANKO

CONTEMPORARY CBRN (CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR) THREATS AND ADEQUATE RESPONSE – REAL SITUATION TRAINING 159
Boris RAJČIĆ, Gvozden TASIĆ, Vladimir KARIĆ, Bojan RADAK, Dubravka MILOVANOVIĆ

SOCIAL MEDIA AS AN EMERGENCY MANAGEMENT TOOL IN THE CONTEXT OF HUMAN SECURITY 167
Nevena ŠEKARIĆ, Filip STOJANOVIĆ

THE ROLE OF MEDIA IN VIOLENCE PREVENTION 175
Aleksandra ILIĆ

USAGE OF MODERN WIRELESS TECHNOLOGIES FOR CHILDREN'S PRESENCE AND LOCATION ANALYTICS AT EDUCATIONAL INSTITUTIONS - TECHNICAL, SECURITY AND LAW DILEMMAS 183
Milenko MARKOV, Nenad PUTNIK, Mladen MILOŠEVIĆ

THE PROPAGANDA OF THE RIGHT-WING EXTREMISM ON THE INTERNET 191
Marija ĐORIĆ

ADOPTING THE ISLAMIC STATE'S INTERNET PROPAGANDA METHOD: THE CASE OF BOKO HARAM 197
Tanja MILOŠEVIĆ

SOCIOCULTURAL COMPONENT IN PATTERN OF CROSS-EUROPEAN MIGRANT INTEGRATION POLICIES 203
Fatima RAMAZANOVA

DISASTER RISK REDUCTION - GENDER ASPECTS 209
Zorica MRŠEVIĆ, Svetlana JANKOVIĆ

IMPACT OF THE GENDER DIGITAL DIVIDE ON SECURITY AND WOMEN'S HUMAN RIGHTS 217
Ksenija ĐURIĆ-ATANASIEVSKI, Brankica POTKONJAK-LUKIĆ

THE LOCAL PERCEPTION OF URBAN SAFETY IN OPEN PUBLIC SPACES AS A PARAMETER FOR TOURIST ATTRACTIVENESS IN THE HISTORIC CORE OF SMEDEREVO, SERBIA 225
Aleksandra ĐUKIĆ, Milica RISTOVIĆ , Branislav ANTONIĆ

SMART CITY ICT SOLUTIONS FOR ENHANCING HUMAN SECURITY 241
Ana PARAUŠIĆ

HUMAN SECURITY – DEFINING AND APPLYING THE CONCEPT 249
Emil Sloth PEDERSEN

EDITORIAL

Human security is one of the least studied areas within the large, all-embracing theoretical framework of security studies. Important scholarly work has been produced on the political, cultural, economic, environmental, educational and other aspects of security in line with the new trend of focused security research. Human security is evidently surrounded by numerous threats. The intensity of old threats has increased (different forms of violence), new ones have emerged, while at the same time, challenges of globalisation, urbanisation and technological (ICT) revolution have underlined the inability of states and governments to develop new policies. It has turned out that the world is not prepared for many of these threats. A wave of new technologies is moving fast and causing changes on a global level, simultaneously affecting every individual human being and every community, whereas the fusion of technologies has resulted in a "blurred line between physical, digital and biological sphere".

At the beginning of the 21st century, predictions from the end of the past century have been not only fulfilled, but far exceeded in many aspects – the number and types of problems accompanying every technological development are increasing exponentially. The topics we suggested in our invitation for the 4th International Academic Conference on Human Security were therefore intended to reach and propose some solutions to the current and pressing problems pertaining to technology-human being relation from a human security perspective and within the context of its multifaceted nature. What are the ethical aspects of the use of drones in modern warfare, is artificial intelligence leading us into a new age founded on new conceptions of state and nation, are the open data uncovering enough or maybe too much, do we have (the right to) privacy in the era of digital footprint, and other interesting, provoking and pressing issues – these were the questions we wished to address by inviting authors from around the world to share their papers and latest research results in the fields of human security and new technologies.

The Proceedings of Human Security and New Technologies are the result of the research efforts presented at the 4th International Academic Conference on Human Security held November 2–3 in Belgrade, which was organized by the Human Security Research Center of the Faculty of Security Studies – University of Belgrade.

This conference provided a forum for scientists and researchers to present and offer possible ways in which new technologies could help international actors, government organizations and civil society organizations to prevent violence, conflicts and other disputes that are referred to as "security". Researchers from Serbia, as well as Greece, Bulgaria, Croatia, Germany, Turkey, the United States, the Russian Federation, Slovakia, Cyprus and Denmark presented the results of their research, which sought to enhance our knowledge of the complex field of human security with contemporary scholarly work.

The twenty-nine thematically diverse papers in the Proceedings either explore previously unused sources or provide an innovative interpretation of topics that have already been discussed. Most papers combine themes from the wide-ranging area of human security and new technologies, opening up numerous ethical and normative issues for researchers as

well as policymakers. Some papers deal with general theoretical considerations of human security and diverse human security settings while others examine practical issues such as the impact of technological development on people's perceptions of armed conflicts, perceptions of depleted uranium weapons use or local perceptions of urban safety and security in open public spaces. The topics put under the researchers' microscope include personal data, privacy, surveillance, human rights, disasters and the role of new technology, ICTs and violence prevention (social media), the gender digital divide and gender aspects of disasters.

With these Proceedings, we want to establish and preserve continuity in the study of human security. We therefore wish to pay due respect to our predecessors but also to use a new methodological approach and new topics to motivate current and future researchers not to grow tired of or discouraged from dealing with these important topics

Editors:

Svetlana Stanarević
Goran J. Mandić
Ljubinka Katić

UDK 351.78:355.48
DOI https://doi.org/10.18485/fb_ic4hs.2018.1

PROBLEMS OF HUMAN SECURITY IN THE CONTEXT OF HYBRID AGGRESSION

Konstantin N. LOBANOV*, Boris N. SELIN**

Abstract: Transformation of technologies and specific character of social, economic and political conditions of the world community development influence the ways and features of contemporary geopolitical confrontation. In conditions of inevitable threat of global war it has become necessary to use other means that have not caused negative global consequences and that are aimed to resolve emerging contradictions on the world stage. A hybrid warfare or aggression has become a means by which combined, integrated military, political, economic, ideological and psychological measures could be confronted in the form of low-intensity and even latent conflicts. The most important component of the hybrid aggression is a psychological warfare, which involves the conduct of cyber-media and -psychological attacks, propaganda, etc. with the aim to suppress the psychological ability of an object of aggression to resist in case of armed conflict resolution scenario. The main tasks of the hybrid aggression include the creation of nervous and non-spiritual environment in society, immersion in the state of permanent social and political confrontation, destruction of the state authority, initiation of mass protest actions and street riots. Taking into consideration that hybrid aggressions implement brand new IT resources and suitable technologies, firstly, to cover mass audience, secondly, to impact on people's consciousness and subconsciousness, thirdly, to manage and manipulate the motivation and behaviour of large groups of people, this can pose a real threat to public and national security, to physical and mental health and life of citizens of those countries which are subjected to hybrid attacks. All aims, tasks and means of hybrid aggression mentioned above have already been tested and implemented on vast Eurasian and post-Soviet territories. The current article aims to investigate issues concerning protection of people from external hybrid aggression and addresses challenges of ensuring a comprehensive response to these threats.

* Doctor of Political Sciences, Belgorod Law Institute of the Ministry of the Interior of Russia named after I.D. Putilin, lobanov.politika@gmail.com

** Associate Professor, PhD, Belgorod Law Institute of the Ministry of the Interior of Russia named after I.D. Putilin, selin-boris@yandex.ru

Keywords: human security, physical and mental health of people, threat to human security, hybrid aggression, national state security system

1. INTRODUCTION

In modern realities, for all subjects of social activity – an individual, society and the State, the problem of ensuring safe existence and development requires special urgency. First of all, this is connected with the negative impact of the globalisation phenomenon on the livelihood of these subjects which has deep objective foundations. The globalisation as a process of global integration and unification, which originates from informational, financial and economic spheres, has captured rather quickly the scope of public relations and institutions and then inflicted their erosion. States have begun to lose a significant part of their sovereignty and to delegate it in favour of other supra-national actors, social organisation of a society has become deprived of its traditional grounds and acquired more and more internationalised character and, finally, the persons who lost their habitual political and social environment have become more vulnerable than ever before. Another crucial factor for the security of all actors of social life in the era of globalisation has been the surge of armed and non-armed violence in the world, caused by the escalation of regional and global geoeconomic and geopolitical competition. The former system of international relations with its mechanisms of checks and balances has collapsed, and the factor of force and dictate has become decisive in world politics. Since the end of 'the Cold War' there has been a multiple increase in armed conflicts with at least 35 million people killed (Сытник, 2012). As a result, the safe space of a human becomes more and more limited and this problem requires an adequate reflection and response.

2. TRANSFORMATION OF VIOLENCE AND AGGRESSION IN THE MODERN WORLD

Military conflicts in the era of globalisation have significantly evolved in terms of content and forms of conduct. Thus, the conflict interaction does not mean an immediate destruction or suppression of an enemy in the course of direct encounter, but rather activation and management of development of internal mechanisms of self-destruction. In this case, the use of physical weapons is not necessary as the conflict involves an entire arsenal of destructive influence on the opposing side (Hoffman, 2009). Violence and aggression in conflicts are carried out in the form of combined application of the means of economic, political, technological, ideological, psychological and other influences on the sensitive objects of an opponent – the state system, fundamentals of social structure, physical and psychological wellbeing of population (McCuen, 2008). The new tactic of aggression is called a 'hybrid warfare' and has been used since that time with high efficiency. Since 1989, no less than 25 attempts of using hybrid technologies in internal and external conflicts have been recorded, 13 of which have been successfully completed (Lobanov and Selin, 2017).

The most common variation of hybrid aggression is a 'colour' revolution whose main target is to undermine the system of state power in a particular country implementing a combination of means used to influence consciousness and to control behaviour of population (Luttwak, 1968; Sharp, 2005). Such way of dealing with unfavourable political

regimes is widely employed by the USA in order to implement its global project of a monopolar world order (Brzezinski, 1997).

3. MECHANISMS OF HYBRID AGGRESSION AND THEIR EXPRESSION DURING 'COLOUR' REVOLUTIONS

The implementation of hybrid technologies is stipulated by certain logical actions which are sufficiently described in literature (Luttwak, 1968; Helvey, 2004; Sharp, 2005; Гапич и Лушников, 2010). Let's illustrate this process on the example of the next 'colour' project that was prepared and accomplished in Armenia in 2018 by the collective West headed by the United States. Since the beginning of 2010 this Transcaucasian Republic has been the stage where the latent programme of the national security destruction has been activated. With the support of the US State Department and the US Embassy in Armenia (one of the world's most numerous)[1], specially trained personnel were promoted to various positions in civil authorities and law enforcement agencies (Григорян, 2018). Majority of these officials have already had some connections abroad[2], while the others, as a rule, have been motivated financially.

When the number of latent and real oppositionists in the state apparatus increased enough to be able to disrupt the functioning of power institutions and, above all, those that provided protection of the state order, open and mass subjects of protest became the focus of the case. In Armenia this role was performed by the "Elk" ("Exit") party that initiated a series of continues rallies in March-April 2018 with the demand for the Government's resignation. From the very beginning, this small party positioned itself as the protest avant-garde and developed a vigorous activity to involve the population in opposition activities (Григорян, 2018). With the help of populism schemes and new information technologies (the Internet, telephony, social networks), the "Elk" party and its leader N. Pashinyan managed, within a few days, to gather large groups of people dissatisfied with the government policy and to bring them to the anti-regime meetings and protest marches (Гасанов, 2018). Actually, the official authorities, having lost reliable support in the republican Government and Parliament, didn't decide to use adequate measures in order to protect constitutional orde and they were practically paralysed and helpless in the face of irritated population skilfully managed by the opposition and its foreign coordinators. The hybrid aggression implemented in Armenia has resulted in the change of elites, the reversal of foreign policy of the country towards the Western world, economic crisis and permanent political turbulence.

---

[1] With the population of Armenia estimated to be about 3 million, the official staff the US Embassy in this Republic comprise 1200 members, i.e. 1 employee accounts for 2500 citizens, which once again emphasises the exceptional importance of this Transcaucasian republic in the US geopolitical calculations.

[2] For example, all 23 members of the new Government of Armenia, who came to power in May 2018, were educated or worked in state authorities, public organisations, private companies abroad, mainly in the USA. See: Сафарьян, А. (2018). Новые министры Пашиняна: кто они? Sputnik Армения. https://ru.armeniasputnik.am/review/20180513/12001323/novye-ministry-pashinyana-kto-oni.html 20/08/2018.

4. HYBRID AGGRESSION AND HUMAN SECURITY THREATS

Analysing the effects of hybrid aggressions on state and public security, it's impossible not to notice the effects that these aggressions have on the security of an individual. In literature, this phenomenon of individual security is described as a human condition when the action of external and internal factors doesn't lead to a poor state, to deterioration of the functioning and development of physique, consciousness, mentality and a human in general, and doesn't prevent him or her to achieve certain desirable purposes (Заплатинський, 2012). On the contrary, it is possible to acknowledge, that hybrid technologies as a set of aggressive, opposing to normal physical and psychological event of the individual factors, comprise harm to such event, since assume conscious deprivation or threat of deprivation of life of people, destruction of consciousness and pressure on psyche. Hybrid aggression combines different forms of armed and non-armed violence and, therefore, it poses an inevitable danger for human life. 'Colour' revolutions have been accompanied by mass riots, rampart crime, provocations, assassinations of leaders, consumer and food famine, and have often resulted in peoples' deaths3, and the overwhelming mass of the population have significantly suffered a declining in living standards. It is necessary to recognise that in many countries that have undergone hybrid aggression, a large proportion of citizens have neglected the danger to their lives in their willingness to support the destructive opposition by assisting in the confrontation with the authorities, as it was observed, for example, in Armenia and Ukraine.

Such temporary symbiosis of the peaceful population and rival opposition can be explained only by one thing – the 'colour' revolutions had been made in people's minds long before street protests. People's consciousness was transcoded into desirable direction and they began to act in accordance with new stereotypes and patterns of behaviour. Therefore, the psychological warfare as the most important component of the hybrid aggression was put into effect in order to achieve such a result (Sharp, 2005). With the help of modern information and communication technologies, the means of such warfare have been significantly improved in recent decades. Thus, the Internet and social networks make possible an on-line broadcasting of ideological content and engage in 'brain-washing' of a huge audience. The networks give also an opportunity to control this zombied part of the audience and using simple technologies of network marketing to gather quickly people in mobile teams with the aim of setting up protest marches under guidance of team coordinators (so-called 'beacons').

The process of this psychological manipulation aims to commit severe violent actions against the inner world of a person: suppression of the ability of critical thinking and of analysing the events, delaying the mechanism of self-control of his or her own actions, disabling the congenital reflexes of self-preservation. In such a state people can easily turn into an object of manipulation from outside, and this opportunity, in our opinion, is the major challenge to the security of a human. So, this threat should not be underestimated as the outcome of the struggle for minds, for the inner world of a person determines largely

[3] During the "Maidan" revolution in Ukraine, 77 civilians and 12 law enforcers were massacred. The mass death of people was used by the "Euromaidan" facilitators to foster the coup d'état.

the success or failure of implementing the attempts of hybrid aggression in a particular country.

5. PROVISION OF HUMAN SECURITY IN THE CONTEXT OF HYBRID AGGRESSION

Nowadays, the autarchy of physical space and especially the inner world of a person is not possible by definition, therefore, no one, even the most perfect state system is able to reach an absolute level of safety of population. Open borders and the universal access to information resources make citizens of any country vulnerable to external influence. In addition, hybrid aggression is not among the internal chronic threats to human security (famine, diseases), which the public and state system of each country are more or less ready to resist. This type of aggression represents the so-called sudden and painful change, the adequate reaction to which from the part of society and the State is less predetermined and depends on the set of certain conditions (Белов, 2012).

Thus, in order to fight effectively against a hybrid aggression launched from the outside, it is important to acquire: firstly, sufficient resources to establish and enable normal functioning of the national security system; secondly, stability of economic and political systems, diminishing the reasons for internal conflicts in communities; thirdly, high level of stress resistance of state and social systems to withstand extreme and crisis situations; fourthly, made up and nationwide implemented set of measures aimed to protect and maintain the physical and mental health of the nation, which in its turn is the most essential requirement of its civil condition.

The combination of all the above-mentioned terms would obviously represent a reference sample which in real practice is elusive even for the developing democracies of the Eurasian and post-Soviet states region. However, these countries must be anxious to achieve and maintain an acceptable level of security for their society, the State and an individual, that, in the face of increased risks and threats to global development, is an equivalent to their survival.

6. CONCLUSION

a) The age of globalisation increases risks and threats to human security significantly, and the security space itself is becoming drastically limited;

b) Conventional physical violence, used for the resolution of social contradictions during previous times, is now giving way to new improved methods of conflict interaction;

c) Hybrid aggression as a combination of different and mostly non-armed ways of pressure is widely used by the collective West headed by the United States against unfavourable political regimes in the Eurasian and post-Soviet states region in the course of the so-called ‘colour’ revolutions;

d) An important component of hybrid technologies is the psychological warfare, which is carried out with the help of new information technologies (the Internet, telephony, social networks) and is aimed to change the consciousness and behaviour of large masses of a community by force;

e) The hybrid aggression is targeted to harm physical and mental health of a person as far as it is based on violent infringement of rights and personal freedom of people, it means an aggressive interference in the nature and inner world of an individual with the purpose of mindset manipulation and actions for the sake of political benefits;

f) In order to neutralise the potential and real threats and risks to human security emanating from the hybrid aggression acting from the outside, the society and the State need to build and maintain a system that will be able to provide the national security – a set of economic, political, social, military, legal, informational, health means, forces and conditions guaranteeing normal functioning of community and providing its members with the protection from external and internal cataclysms.

7. REFERENCES

Белов, С.В. (2002). Основные понятия, термины и определения в безопасности жизнедеятельности. Безопасность жизнедеятельности, 2, 37-40; 3, 37-43.

Brzezinski, Z.K. (1997). The Grand Chessboard: American Primacy and Its Geostrategic Imperatives. Published by Basic Books, A Member of the Perseus Books Group.

Гапич, А.Э., Лушников, Д.А. (2010). Технологии «цветных революций». РИОР.

Гасанов, К. (2018). «Бархатная революция» в Армении: Пашинян победил. Что дальше? Царьград. https://tsargrad.tv/articles/barhatnaja-revoljucija-v-armenii-pashinjan-pobedil-chto-dalshe_130673 21/08/2018.

Григорян, С.Г. (2018). Армянская «бархатная» революция. Эдит Принт.

Helvey, R.L. (2004). On Strategic Nonviolent Conflict: Thinking About the Fundamentals. Albert Einstein Institution.

Hoffman, G.F. (2009). Hybrid Warfare and Challenges. Joint Force Quarterly, 52, 34-48.

Заплатинський, В.М. (2012). Логіко-детермінантні підходи до розуміння поняття «Безпека». Вісник Камянець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоровя людини, 5, 90-98.

Lobanov, K.N., Selin, B.N. (2017, November). Hybrid and «colour» technologies as a threat to the national security. In Proceedings of the POKO 2017 scientific conference «Impact of Changes in Operational Environment on Preparation and Execution (Design) of Operations» (pp. 293-307).

Luttwak, E.N. (1968). Coup d'Etat: a Practical Handbook. The Pinguin Press.

McCuen, J.J. (2008). Hybrid Wars. Military Review, 88 (2), 107-113.

Сафарьян, А. (2018). Новые министры Пашиняна: кто они? Sputnik Армения. https://ru.armeniasputnik.am/review/20180513/12001323/novye-ministry-pashinyana-kto-oni.html 20/08/2018.

Sharp, G. (2005). From Dictatorship to Democracy A Conceptual Framework for Liberation. Albert Einstein Institution.

Сытник, Г.П. (2012). Государственное управление в сфере национальной безопасности. Русское слово, 40.

UDK 355.48:623.4(091)
https://doi.org/10.18485/fb_ic4hs.2018.2

A HISTORICAL OVERVIEW OF THE RELATION BETWEEN TECHNOLOGICAL DEVELOPMENT AND THE ABILITY TO MANAGE PERCEPTION DURING ARMED CONFLICTS

Nenad PUTNIK *

Abstract: From a historical perspective, advanced technologies are developed under the auspices of armies and for military purposes. The new technical and technological inventions find their immediate application in military activities, increase the power of the warring parties, change the way in which wars are planned and thus have a direct impact on the dynamics, communication, coordination, choice of strategies, and outcome of conflicts.

A particular aspect of the impact of new technological achievements on the outcome of conflicts can be traced through their indirect impact on social conflicts since they enable new ways of spreading propaganda and disinformation and perception management before, during, and after the conflict.

The manner of presenting conflicts to the public has changed significantly over time, following the evolution of means of communication. In the first wars of the second half of the nineteenth century, the availability of information was very limited – it was reduced to reporting via printed media whose dissemination was very slow. The invention of the telegraph was a step forward in information transmission because the transmission time was reduced from several weeks to several seconds. The application of more modern technological innovations in armed conflicts such as the radio (at the beginning of the twentieth century), television (in the 1960s) and, finally, the Internet additionally increased the speed of information transmission, yet it also increased the possibilities for information manipulation. This paper discusses and analyzes the impact of information and technological means during armed conflicts, following the historical development of new technologies from the second half of the twentieth century to date.

Keywords: social conflicts, warfare, information and communication technologies, propaganda

---

* Associate Professor, PhD, University of Belgrade Faculty of Security Studies, nputnik@fb.bg.ac.rs

1. INTRODUCTION

In the mid-nineteenth century, the first essential change happened in the ability to communicate. This change continued over the next one hundred and fifty years in so many varieties and modalities that it took on revolutionary characteristics. For this reason, this period can be viewed either as a unique information revolution, evolutionary in character, or as three separate periods of time, equally important and considered as separate revolutions (Papp, Alberts, Tuyahov, 1997).

The first information revolution began in the mid-nineteenth century and lasted for one century. Typical communication tools of this period were the telegraph, the radio and the telephone.

The next revolution began in the mid-twentieth century and ended in the early eighties. Its assets were television, first-generation computers and satellites. Television was a step-up in comparison to the radio, with its ability to transmit more information in a more efficient format. Computers, on the other hand, increased the ability to collect, analyze and use information, while satellites created the global telecommunications infrastructure.

By the end of the 1980s and the beginning of the 1990s, modern information systems based on personal computers and computer systems appeared. The development and application of informatics and information and communication systems overshadowed everything that had been achieved in the two previous revolutions in the field of information exchange and defined the Third Information Revolution.

The technology developed in the Second and Third Information Revolution significantly strengthened the ability to use and exchange information, and freed communicators from the constraints of time, distance, and their location.

The information revolution has transformed the way wars are waged in the information era, causing changes in how societies engage in conflicts, how their armed forces wage armed conflicts, etc. Until recently, going into combat required previously obtaining enough information on the opponent's strength, one's own forces, the space and the weather. Specific knowledge of the opponent's strength, and spatial and weather characteristics are necessary for success in waging any war. However, they are not enough. Nowadays, the first task is to inform the public (the public at home, the opponent's public, and the public of the countries which are not directly engaged in the conflict) about the reasons for the conflict, its goals, and its outcome. In these activities, modern armed forces rely heavily on the latest technological achievements in the field of information and communication technologies.

Therefore, it is important to emphasize that wars are not waged only with military means and weapons, but also via information broadcast by mass media. From war zones, reporters send striking images, information and messages, which can be more or less objective. This content influences public opinion, usually serving the governments of the warring parties. Sometimes, however, it does not match the official policy of the warring parties.

2. THE VIETNAM WAR – THE FIRST "TELEVISION WAR"

Marshall McLuhan, one of the greatest media scholars, called the Vietnam War the first television war. McLuhan is known for his view that there is a correlation between war and technology, and that all the wars in history were waged with the latest technologies available to each culture at the time (McLuhan, 2008). This observation is correct to include communication technologies, since all the major wars of the twentieth century favored technological advances in the field of media, and vice versa – they were conditioned by changes in the ways of communication.

During the war in Vietnam (1962–1975), television changed the relationship between military strategies and the media. Gardner notes that it was during this conflict that war was shown on television in a negative context for the first time, through short segments of ugly and unedited low-resolution black and white photographs. The impression they left was heavy and effective. The viewer had the impression that he was a direct witness to the war. The way television depicted the war idealized the conflict and glorified the American hero. New technology enabled the transmission of a vast amount of information. Receiving numerous visual and auditory stimuli, the viewer needed a sublimated interpretation of the events. This is why the reports were accompanied by comments which simplified understanding. The narrative model of stories from folk tradition was applied, where the warring sides were divided into heroes and antiheroes. At first, the war was presented as a conflict with a cruel and fanatical enemy. Some kind of identification with American ideals was being created, so the media became promoters of official government policy. Therefore, in this war, the media did not suffer any pressure or censorship. They were authorized to monitor military troops in Vietnam and had formal autonomy in reporting (Gardner, 2009).

The tacit agreement between the media and political power was breached after the Tet Offensive, and the loss of confidence in institutions helped the emancipation of television. It was only between 1968 to 1973 that television documented and broadcast the cruel truth of the war to the American public, in the foreground and in color, causing disappointment in institutions, the moral collapse of the nation, and antimilitarism of the public (Gardner, 2009).

In June 1971, the New York Times challenged the government to publish the truth about the war contained in the so-called "Pentagon papers" (US Department of Defense secret documents), including frauds during the military attack on Vietnam. Basically, the US media did not completely stop supporting the establishment, but could not avoid showing the shaken administration (Weiskopf, Willmott, 2013).

In the final years of the war, media coverage was declining and almost stopped. With the gradual withdrawal of American troops, the viewers and the readers were losing interest in this topic, as the nation had already been brought into a state of apathy towards the war.

3. "INVISIBLE WARS" – FROM THE FALKLAND ISLANDS TO THE FIRST GULF WAR

American and British conservative governments learnt from the Vietnamese lesson – they realized that no rhetorical skill can make up for the loss of loved ones, except in the context of total war, which would bring into question the survival of the society itself. The war, therefore, had to be presented as total and inevitable, highly technologized, without images of destruction, blood and death. In other words, it had to become "invisible".

The Falklands War (1982) was the first "invisible" war in the television era (Gardner, 2009). From the very beginning of the conflict, the British government introduced information control. British correspondents' reports were subjected to double censorship – the Ministry of Defense controlled the materials before they were sent, and again upon their arrival in London (Savarese, 1992).

In the second half of the 1980s, television entered its mature phase. With the development of electronic technologies and the diffusion of geostationary satellites, the number of reports and direct transmissions increased significantly. Television instrumentation led to more dramatization, which is the basis of modern political television journalism.

The First Gulf War started with the Iraqi invasion of Kuwait. When the US representatives and the Iraqi Foreign Minister failed to reach an agreement on January 9, 1991, talks began in Geneva about the upcoming war. The media were well-prepared for the beginning of this conflict.

In this war, television triumphed as a means of communication and diplomacy. Television broadcast the message based on dramatization, on events directing and the construction of characters, and symbols translated into television-effective faces and images.

In order to avoid the dangerous influence of journalists on public opinion, the US Military Command used two traditional instruments: censorship and the production of an alternative flow of information (Čomski, 2008). There was hence a return to information control similar to the one used during the war in Vietnam.

Many events were covered up which makes this war the most invisible war of the twentieth century (Savarese, 1992). A large number of independent media were completely excluded from the Pentagon Information Consortium. The absolute control over information allowed the Pentagon to construct and propagate a so-called painless, high-tech war without images of destruction, blood and death. It was a war dominated by images of the battle between the "evil" and the "good", with the good always emerging victorious (Barbulović et. al., 2004).

4. NATO AGGRESSION ON THE FR YUGOSLAVIA AND THE SECOND GULF WAR – BEGINNINGS OF THE "INTERNET WAR"

Incapable of producing a military response to the air attacks launched by NATO in 1999, FR Yugoslavia turned to asymmetric means to counter the Alliance. While being exposed to aggression, FR Yugoslavia actively used its own mass media, foreign journalists and the Internet to influence public opinion all over the world with a view to achieving its political goal – the preservation of its sovereignty and territorial integrity.

At first glance, it may be difficult to see the manipulation of the media and the exploitation of the Internet as a coherent campaign of information operations ran by the FRY government. The efforts the Yugoslav government made at the time to shape domestic and international public opinion look primitive in comparison with the possibilities of modern information operations, which are based on cyber weapons and attacks on computer networks (Vuletić, 2017). Nevertheless, these efforts proved effective.

In order to achieve "information security", the Yugoslav establishment resorted to the strategy of media censorship and counter-propaganda management. Applying the Law on Public Information, adopted immediately before the bombing, the government suppressed several independent media operating in Serbia with the aim of preventing its citizens from accessing information from external sources (Larsen, 2000). Also, at the very outset of the war, the broadcasting of programs from Western television stations was suspended. However, the regime could not prevent the reception of these programs via satellites and the Internet, so it started a fierce counter-propaganda campaign to discredit their credibility.

The FRY government used its own media resources to present the Yugoslav perspective on the war to foreign audiences. Through the leased EUSat communication link, RTS was able to cover the whole Europe and re-broadcast the state television program in the United States (Larsen, 2000). In this way, the regime attempted to undermine the moral and legal authority of NATO through carefully selected messages.

The government also used propaganda weapons to discredit the main reason for NATO engagement – the alleged ethnic cleansing in Kosovo and Metohija. The exploitation of so-called "collateral damage" incidents was another aspect of the information operations campaign intended to discredit NATO.

In order to reach a wider audience, the establishment turned to a completely new medium for its offensive operations – the Internet.

During the first two weeks of the war, ten regime-supporting websites appeared in English. Some of these websites were privately owned, but most were run by the Federal Ministry of Information and the Yugoslav army. In addition, security services secretly seized the web address of B92, which had been known since 1997 as the "source of independent reporting in Yugoslavia" (Larsen, 2000: 19).

Campaigns of targeted e-mail delivery, executed by the Ministry of Information, were an absolute novelty. The Minister of Information at the time, Nikola Marković, appealed to Internet users to "respect Internet ethics by sending short messages without insulting words. Messages must be sent to target groups with as many images as possible of the crimes committed. He added that the foreigners are most interested in amateur videos

because they represent authentic footage from the field. The truth must reach influential people, politicians and business people. For that reason, messages must be sent via e-mails" (Larsen, 2000:18).

Since NATO managed to gradually stop television communication inside the country and with other countries, Internet sites became the primary instrument of the regime propaganda.

State services and individuals in Serbia used e-mails to inform foreign media and the global public about cases of so-called "collateral damage". For example, within 15 minutes after the Chinese Embassy was bombed, the company for geopolitical research and analytics, Stratford, received five e-mails describing attacks from people living near the embassy building (Stratford, 1999).

E-mails also became an integral part of the early warning network. The moment NATO aviation took off from Avian or other locations, Yugoslav army associates, who were stationed around the air bases, sent e-mails with information about the type of planes, their number, quantity of weapons, and their numerical designation. These pieces of information provided timely warnings to the Yugoslav Air Defense (Wall, 1999: 102).

In addition to using the Internet for public relations and for propaganda purposes, the citizens of Serbia used it to carry out information attacks against NATO countries. In the first week of bombing, more than 2000 emails infected with a virus were sent to NATO addresses in only one day (Hubbard, 1999: 11). The Alliance website was also cyber-attacked by domestic hackers who managed to temporarily disable it (Putnik, 2009).

When the United States attacked Iraq on March 20, 2003 on the pretext of neutralizing weapons of mass destruction, the existing differences between the European powers became evident. Several countries of the old continent not only distanced themselves from the United States but also resolutely stood up to the armed intervention led by George Bush, holding it illegitimate for not being supported by the UN. Of course, these divisions also reflected on the way mass media reported on this war.

The presentation of the war prepared by the American media was a purified version of the conflict. The television broadcasts were mainly shot from a great height or from a distance, showing the fiery sky above Baghdad or the flat landscape of the desert along which the contours of tanks and armored vehicles were moving – more like a video game than a war.

American war reporters, the new protagonists of war journalism, protected and assisted by the army, became one of the strongest American weapons for winning the sympathy of the domestic public. Regardless of the unconditional support of most major US news networks, however, international public opinion remained rather skeptical about the necessity of military intervention (Herman, Mekčesni, 2004).

In an interview for *Le Monde*, Paul Virilio, a famous French philosopher, commented on the Second Gulf War by saying: "Previous conflicts were of a different nature due to the simple fact that televisions did not have the possibility to broadcast live. The real problem lies in today's speed and confusion of images." When it comes to refusing to show the horrors of war, he says: "Keeping the anonymity of victims is theatrical, it is a way of acting, a new kind of pseudo-humanitarian camouflage…we are witnessing a war of lies, a lost perception of the true and the false. The bluff is of global proportions and it is broadcast live" (Le Monde, 2003). On several occasions, Virilio has reiterated his

criticism of the way information is spread, his thesis that the boundaries between facts and propaganda are becoming less and less defined, that technology is leading an invisible war against humanity, that there have been no differences between war and peace after World War II, and that "accidents" are the inevitable result of every technological advancement (Virilio, Lotringer, 2012).

In this conflict, the Internet had an important role as well. This time, however, it was a completely new role. During the Second Gulf War, the phenomenon of blogs came to the fore. The publishing of blogs – notes and personal diaries from war-affected areas, the description of the cruelty of the war, the interpretation of activities on the ground and the discovery of their own "truths" – had become so pervasive that Iraq had to completely abolish access to the Internet.

5. CONCLUSION

In modern conflicts, the winning side is the one that is faster in collecting, exploiting and manipulating information. We can say that information has become a strategic resource. Domination in the information sphere has, therefore, become the necessary precondition for success and victory in a conflict.

Becoming dominant in the information sphere is now possible because of different techniques for manipulating the content of information systems – the information which is transferred and its "package" – the tools used to shape the information and send it to the user. For this reason, certain armed conflicts, like the Gulf War, are a triumph of information, rather than arms, strategies, or the troops' morale.

And yet, it is interesting that in the second half of the twentieth and the beginning of the twenty-first century, governments did not always manage to control and adapt the informative apparatus according to their own needs owing to new media like television and the Internet. Television and the Internet changed the way news was "consumed". They transmitted events almost instantly and offered to the recipient a distinct feeling that he or she was a direct witness to war events.

More than the radio, television changed the relationship between military activities and strategies and communication resources, increasing the visibility of events. Television did not invent war, but it has become its sublimation, a necessary instrument for confirming or refuting the very causes of conflict (Remondino, 2002). Television can be said to have triumphed by imposing its model of narration and aesthetics in the conflicts that have taken place in the last decade. Before the fascinating synchronized flow of images and sounds, the viewer gets the impression that he has direct access to reality and truth. However, this is often just a misleading impression. Baudrillard, a renowned French sociologist and philosopher, speaks of television as an instrument capable of producing a reality more realistic than the real – a simulacrum, i.e. a copy of a never-existing original.

The Internet is an absolute novelty among various sources of information in contemporary conflicts. In contrast to traditional media where communication is one-way – from the sender to the recipient (the radio and television), the global computer network has enabled two-way communication. This means that, by its own nature, the medium of Internet

allows each user to be not only the consumer, but also the creator of information. During the First Gulf War, the Internet was still underdeveloped. Only a few years later, it enabled offensive and defensive information operations in the fifth battlefield – the infosphere. In addition, the Internet has led to a revolution in the sphere of communication enabling interaction between non-state and state actors in inter-state conflicts, and the diffusion of official and unofficial, imposed and arbitrary "truths".

6. REFERENCES

Barbulović, S., Jevtović, Z., Lakićević, R., Popović, M. (2004). *Amnezija javnosti – od propagande do terorizma*. Beograd: Grafo-komerc.

Čomski, N. (2008). *Kontrola medija*. Novi Sad: Rubikon.

Gardner, H. (2009). "War and the media paradox". In: Athina Karatzogianni (Ed), *Cyber Conflict and Global Politics*. pp. 13-31. Abingdon: Routledge.

Herman, E., Mekčesni R. (2004). *Globalni mediji – novi misionari korporativnog kapitalizma*. Beograd: Klio.

Hubbard, Z. (1999). Information Warfare in Kosovo. *Journal of Electronic Defense*, Vol. 22, No. 11, pp. 57-60.

Larsen, A. W. (2000). *Serbian Information Operations During Operation Allied Force*. Alabama: Air Command and Staff College.

Le Monde, retrieved April 4, 2003, https://www.lemonde.fr/

McLuhan, M. (2008*). Razumijevanje medija*. Zagreb: Golden Marketing i Tehnička knjiga.

Papp, D. S., Alberts, D., Tuyahov A. (1997). "Historical Impacts of Information Technologies: An Overview". In: David S. Alberts and Daniel S. Papp (Eds.), *The Information Age: An Anthology on Its Impact and Consequences*, vol. I, pp. 13-36. Publication Series.

Putnik, N. (2009). *Sajber prostor i bezbednosni izazovi*. Beograd: Univerzitet u Beogradu – Fakultet bezbednosti.

Remondino, E. (2002). *La televisione va alla guerra*. Roma: Sperling & Kupfer.

Savarese, R. (1992). *Guerre intelligenti*. Milano: Franco Angeli.

Stratford, "Good morning America" interview with George Friedman, retrieved 15.06.1999, http://www.stratfor.com/media/ television/990615.asp

Virilio, P., Lotringer, S. (2012). *Čisti rat*. Beograd: Makart

Vuletć, D. (2017). Upotreba sajber prostora u kontekstu hibridnog ratovanja. *Vojno delo*, 7/2017, 308-325.

Wall, R. (1999). USAF Expands Infowar Arsenal. *Aviation Week and Space Technology*, Vol. 151, Issue 20.

Weiskopf, R., Willmott, H. (2013). "Ethics as Critical Practice: The 'Pentagon Paper', Deciding Responsibly, Truth-telling, and the Unsettling of Organizational Morality". *Organization studies*, Volume 34 (4), pp. 469-493

.

UDK 351.78:004
https://doi.org/10.18485/fb_ic4hs.2018.3

HOW HUMAN SECURITY COULD BE A BENEFICIARY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Ivica Lj. ĐORĐEVIĆ[*], Ozren DŽIGURSKI[**]

Abstract: The invention and application of new technologies have always been important development triggers and indicators. Today, the results of technological progress, among others, mostly depend on the structure and efficiency of modern communication tools. Obviously, in our globalized world, the availability and use of information and communications technologies (ICTs), in addition to the positive effects, is also a potential source of risk for their users. In addition to great development potential of the ICTs, with appropriate access, they can contribute to raising the level of security of people in unstable regions and vulnerable social groups.

The potential of information and communications technologies to support economic development is widely recognized. On the one hand, industrial technologies through economic growth influence the increase and pollution of the environment, and on the other hand, the ICT can increase the efficiency of production processes and business organization by reducing the negative effects of economic activities. For this reason, many international and state institutions in their activities and documents promote the need to build a more humane environment – an inclusive, open and development oriented society in which everyone can create, access, use and participate in the exchange of information and knowledge.

Threats to citizens' safety due to the omnipresence of the ICTs are mostly related to the threat to individual human rights, cyber threats, identity theft, hate speech, child pornography, racism, blocking and filtering of the Internet, misuse of personal data, etc. On the other hand, the protection and security of citizens as members of the information society is predominantly based on directives, recommendations and various initiatives. In addition, technical means of protection, which are realized through commercial offers by certain specialized companies, are available to a certain extent.

This paper shows that in addition to various types of threats and inadequate protection, there are opportunities and resources that can raise the level of security of citizens as members of the emerging global information society. To this end, benefits are shown in different domains - the

[*] Associate Professor, PhD, University of Belgrade Faculty of Security Studies, djivica@gmail.com

[**] Retired Associate Professor, PhD, University of Belgrade Faculty of Security Studies, odzigurski@gmail.com

dimensions of human security (HS), with an emphasis on the economic sphere, upon which depends the situation in other dimensions of the HS to a certain extent.

Finally, some informational and technical tools that can be found in the field of HS are presented: information systems, networks, databases, mobile and other relevant IC technologies.

Keywords: human security: threat, protection, benefits; information and communications technologies

1. INTRODUCTION

The potential of the ICT-driven changes induces different reactions in humans. Many are afraid of the negative effects of the spontaneous spread of the ICT as well as of its speed, that is, the comprehensiveness of change. The unevenness of spreading positive effects endangers not only individual existence but also community stability (from local to global). The positive effects of the ICT depend on the ability to anticipate the process and adapt the institutional mechanisms to new tendencies. The problem of the modern world is that the analyses are mainly limited to the growth of the average income per capita and the amount of realized profit as the most common indicators on the basis of which the effects of global processes are evaluated. However, growth often does not mean development, but the deepening of the gap between the poor and the rich, that is, the winners and losers of global processes.

Security aspects of the ICT are usually analysed in the context of human rights violations and privacy while neglecting a rather wide range of other effects on citizens' safety. There are two main directions in the analysis of the effects of the ICT: a non-critical relationship that glorifies positive effects as opposed to the emphasis on negative aspects of the ICT and underestimation of the potential of positive changes in the wake of technological development. The truth is, as usually, somewhere in between. Undoubtedly, there are possibilities for positive changes based on the application of the ICT in practice, however, the impact of the ICT on socio-economic flows depends on the degree of control of institutions over the computerization of human activities. The domination of the monopoly and the financial power arising from this position undermines the ultimate impact of the ICT on the quality of life of people of the modern era.

Due to its holistic approach based on the seven-dimensional conceptual model, the concept of human security (HS) enables a qualitative analysis of the process and an insight into the impact of the ICT on the quality of life of modern man and their community. The ICT is all-embracing and its impact on changes in all HS segments can be identified: starting from its application in the economic sphere where the automation of production activities and service provision is increasingly present, through a healthcare system that acquires new tools and procedures based on the ICT to its influence on political systems and democratic processes that obtain new forms.

2. THE CONCEPT OF HUMAN SECURITY AS AN ANALYTICAL FRAMEWORK

Since the fall of the Berlin Wall, contradictory processes have been taking place in the countries of former Eastern bloc. The so-called transitional countries exposed to the processes of initial capital accumulation have experienced a drastic fall in the quality of

life of their citizens. Instead of the expected progress, we have witnessed a regression in every way. The dysfunction of institutions and their exploitation for the interests of the owners of large-scale capital from abroad and local tycoons (former communist apparatchiks) have caused the fall in living standards, the increase of the unemployed and the collapse of the then social systems (Đorđević, 2013:71-72).

Recognizing the negative effects of the transition, the United Nation Development Programme (UNDP) experts who participated in the writing of the 1994 Development Report offer the concept of Human Security as an analytical framework that should point to the shortcomings in the functioning of the institutional system in order to improve the quality of life of citizens (UNDP, 1994). The concept is universal and its quality is also reflected in the fact that it is not rigid with conservatively set rules, but is adapted to the conditions that are current and within the focus of the analysis. For example, security challenges in developed countries are associated with anomalies in the functioning of democratic electoral procedures, while in developing countries the biggest security challenge is the lack of food or dysfunctionality of the educational and health system.

It is precisely the insensitivity of the existing system to social differences within developed countries and the specificities of underdeveloped countries that make the gap between the rich and the poor (developed and underdeveloped) deeper without any hope of decreasing it. The HS concept provides an analytical framework that allows the identification of anomalies in the existing system of socio-economic relations. By establishing the parameters on the basis of which we can quantify the quality of life of citizens and classify them into seven dimensions[1], the concept of HS makes a qualitative shift in the critical attitude towards the current system. The definition of a seven-dimensional model allows comparison of the quality of life of people in different countries irrespective of the geographical location and degree of development expressed through classical statistical indicators. Often economic statistics blur the image and do not reflect the real situation. In many analyses, data on economic growth are often mistaken for development, resulting in a wrong perception of current trends.[2]

The HS Syntagm comes with the idea of drawing attention of relevant actors to the need for a critical attitude towards the current system.[3] Pondering the collapse of the bipolar structure of world power and its impact on the former socialist countries, i.e. developing countries, the UN experts estimated that corrective mechanisms were needed in order to stop the initial negative trends. Security in the title of the concept emphasizes the importance and urgency of the need, and Human is imposed in order to indicate the difference in relation to state security, which has the preservation of territorial integrity and institutions protection in its focus. Of course, here we should emphasize that the

[1] The Human Development Report for 1994 provides an overview of the HS concept based on the following seven dimensions: Economic, Food Quality, Health System Status, Ecological Situation, Individual Security, Community Security and the Political System (UNDP, 1994: 24-25).

[2] Growth of statistical indicators does not necessarily mean raising the quality of people's lives. Growth is a quantitative category while development refers to the qualitative aspects of the process.

[3] In this case, the process of securitization (adhering to security content) was used to indicate the importance of the area for the functioning of the system.

concept of HS is not in conflict with classical state or national security. On the contrary, the idea is to draw attention to the shortcomings of the existing system and to use its mechanisms to protect the interests of citizens living in the area under the control of state institutions. It should also be said that the HS concept cannot take effect in practice without the support security systems such as the military, the police, and intelligence and counter-intelligence systems. A qualitative difference with respect to classical security instruments is only in the approach and institutional control that should put those systems in the function of citizens' interests.

3. SECURITY OF CITIZENS IN THE CONTEXT OF INFORMATION REVOLUTION

The omnipresence of the ICT affects each of the HS dimensions, whether the effects will be positive or negative depends primarily on the ability of state institutions to control and direct their application. In this context, we think of a state as a representative of the interests of citizens living on its territory. The first of the effects we are talking about here is the impact on the implementation of democratic procedures that ensure the representativeness of the legislature. The ICT as a tool can be misused for electoral will manipulation, which allows for the establishment of a political order that is inconsistent with the interests of a democratic majority.[4] At the same time, if there are clearly defined rules with the appropriate system of control and sanctioning, the potential of the ICT can contribute to the greater interest and participation of citizens in election processes, thus ensuring the legitimacy of the system. Unfortunately, as can be seen from the Figure 1, the global trend shows a decrease in the number of citizens who use their voting rights.

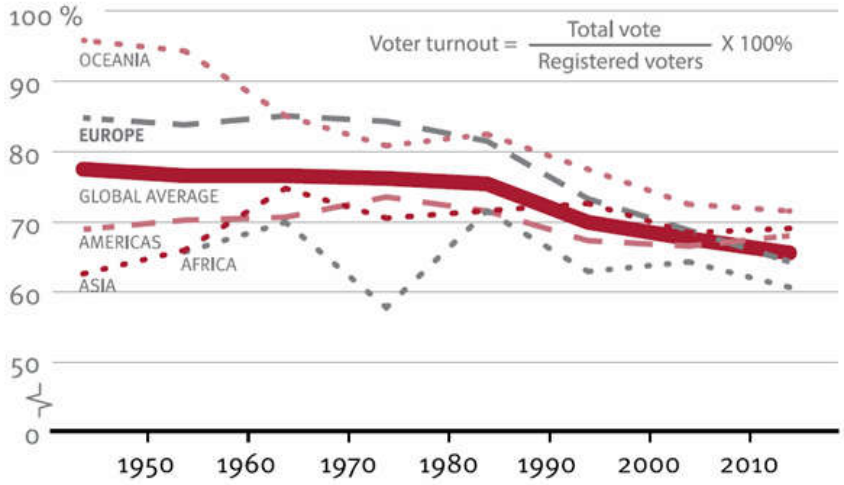


Figure 1. Global voter turnout by region, 1945–2015.

[4] The still-present affair with the Cambridge analyst shows the great power of manipulation with the voting body (Bartlett, 2018: 46-63).

Source: Abdurashid Solijonov (2016): *Voter Turnout Trends around the World*, International Institute for Democracy and Electoral Assistance, Stockholm. pg.25. Based on: Voter Turnout Database, www.idea.int/data-tools/data/voter-turnout

Government structure influences all other areas considered important for the quality of life of people living within the jurisdiction of these state institution controlled by the elected citizens' representatives. In the field of food production and distribution, the ICTs have a significant place through the process of organizing and implementing agricultural production, as well as control of the distribution system. In the field of health, there is already a qualitative improvement in the implementation of procedures and diagnostic methods, but there remains considerable scope for manipulation and abuse. Security at the personal and group level, or community, can also be viewed from two aspects. Positive shifts are evident in the area of technical means of surveillance and protection, but at the same time this mechanism can be a source of privacy disruption as well as a tool for conducting criminal activities. Thanks to the Internet, we are nowadays witnesses of the emergence of a global community of people who are gradually becoming aware of the dangers of a global character that can endanger the survival of the living world on the planet. However, due to the lack of regulation and control of activities on the Internet, there is enough space for extremist activities who can manipulate far easier a greater number of people turning them against members of other social groups.

Military systems have become far more efficient thanks to the ICT, however, there is a danger of anomalies in a system that can lead to cataclysm of global proportions. For example, the approach to the use of drones and other automated assets in military operations causing collateral damage, which is a euphemism for human victims in the conduct of combat operations, is utterly ethically questioned.

In the end, not without reason we want to present economic effects that can be interpreted as twofold: as a cause and consequence. Namely, the bulk of practical implementation of the ICT is inspired by the increase in the earnings of company owners and research centres. The effects upon population are extremely controversial because many workers have lost their jobs due to the introduction of robots and automated production lines (see Figure 2.). There is a huge number of people who, instead of the positive effects of the ICT implementation, have become social welfare beneficiaries and have been declared a surplus due to their inability to adapt to new trends. Generations that are no longer able to re-qualify for service activities, that is, to become program developers at 50 or more years of age are mostly affected by this process. The effects of the ICT applications in the economic sphere have a significant impact on the political situation, the citizens' attitude to participation in election processes and thus lead to retrograde phenomena. Disenchantment in relation to one's own situation leads to the election of right-wing populists, and endangered citizens become more susceptible to manipulations by electoral headquarters of political actors, which again brings us back to the beginning of a story related to the electoral environment. Data presented in the figures point to the dramatic situation, as the forecasts are such that in some professions there will be no need for human labour in the near future.

Figure 2. Probability of a job becoming automatable

Reif L. Rafael (2018): A survival guide for The Fourth Industrial Revolution, Davos: World Economic Forum. Based on: University of Oxford, Morgan Stanley. https://www.weforum.org/agenda/2018/01/the-fourth-industrial-revolution-a-survival-guide/

4. SECURITY OF PEOPLE IN GLOBALIZATION CONDITIONS

The ICT has dramatically accelerated the process of globalization of human activities. There has always been a tendency to connect known space into one whole. World imperators have always wanted to be at the forefront of a global empire, religious leaders have dreamed of the universality of their religions, and philosophers have had a tendency toward cosmopolitanism. Only with the development of the ICT have the conditions for the establishment of global business and social networks been created, which has both its advantages and disadvantage i.e. risks the world has not found a response to yet.

The expansion of human activities beyond the borders of national states entails certain risks and threats that are not entirely new, but are gaining new dimensions. Due to the fact that global practice has not received appropriate institutional attention and response, phenomena such as privacy threats, the spread of extremism and various criminal activities are gaining in their severity, as the range of actions of national institutions is limited to the area within state borders (Kamei, 2012). Thanks to the use of the ICT, criminal organizations spread their activities across national borders using their porosity. Using the liberalization of cross-border traffic, criminal and extremist organizations create collaborative networks across the entire planet.

The lack of institutional response to changing environment and current global practice have become serious also due to the fact that national states have been their power under

enormous pressure by large capital whose exponents are transnational companies (TNC). The monopolization of economic activities in global proportions shifts the power from state institutions to the hands of large capital managers. Driven exclusively by maximizing profits as the only benchmark of success, the TNCs delegitimize the political system and institutional levers of government are being exploited for their own needs. Imperative growth of profit rates makes the classical mechanisms of controlling cross-border human trafficking, goods and finances unsustainable. In order to remain efficient, long-term and complex procedures are not practiced any more since they slow down the cross-border flow, which creates conditions for intensifying criminal activities such as human trafficking, dangerous substances and narcotics smuggling, and various products that infringe intellectual property rights and pose a danger to users due to poor quality. Financial markets are becoming a major source of economic instability because transfers are no longer related to the needs of the real economy, but are largely driven by stock-market speculation[5]. The speculations lead to the collapse of large transnational systems, but also to instability at the level of a state, that is, a region and globally. The subject of speculation is not only the shares of corporations, but also the value of national currencies.

Under the pressure of blackmail, the poor and underdeveloped countries agree to lower standards in protecting workers' rights and the environment. Disadvantageous arrangements are being worked out and they break down the standard of the local population, devastate natural assets and resources as well as existing infrastructure. Using the system of TNCs transfer pricing, they avoid liabilities towards local communities, thereby increasing their own profits.

Large fluctuations of people and goods increase the likelihood of global epidemics. The health systems of underdeveloped countries are unable to apply health care standards that have been met in the developed world. There are evident pests that transmit various diseases through container transport, but climate change also creates conditions for the spread of insects and rodent habitats to the northern parts of the planet that have been previously out of their range.

High degree of corruption as a result of the collapse of national institutions leads to the loss of citizens' confidence in such institutions and creates a suitable environment for provoking intolerance towards members of other nations and religions, which significantly affects security within national borders, but also at the regional or global level. The described situation can additionally deteriorate due to the possibilities provided by the ICT, by which the population of developing countries acquires an idealized image of the West that is far from realistic living conditions. At the same time, the Internet becomes a channel that allows fundamentalist organizations to exploit the sense of those being deprived as the losers of globalization and successfully promote their ideas in order to gain new supporters.

[5] According to data for 2011, it is estimated that at least 80% of transactions in the global capital market are motivated by speculation, that is, only 0.6% of financial transactions are directly related to trade, production and services. (Andreou, 2013)

5. POSSIBLE CONTRIBUTION OF THE ICT TO HUMAN SECURITY

Modern ICT-based technologies have led to dynamic changes that affect human safety. In addition to exacerbating some of the negative phenomena of the ICT, thanks to the use of new techniques and data processing tools, experts can improve their work and, through risk identification, raise the level of security for vulnerable groups. Database creation and data mining raise the level of efficiency of the fight against human trafficking, unsafe migrations, cyber warfare, the use of unmanned aircraft, research in the field of human rights and violence policies. (Latonero and Gold, 2015). The collection and analysis of large amounts of data through advanced searches, pattern recognition and visualization enable the identification of relevant parameters that reveal social relationships and characteristics the very subjects (groups and individuals) that are being monitored are often not aware of.

The information obtained from the analysis of the collected data can play a major role in the decision-making processes that are important for the level of citizen security. New technologies also enable new approaches in policy making and faster than ever intervention in the physical, social and political environment. Organizations and institutions dealing with security issues through the use of advanced foresight techniques can create models for the development of possible conflicts and crisis situations, which makes it possible to make better decisions based on an early warning system.

Below the text we will present several examples of different levels of the ICT application in the field of human security, ranging from standard databases and information systems to the application of artificial intelligence in this field.

Database of HS indexes

The significance of information tools for human security can be illustrated through an example of a project aimed at determining the indicators for the assessment of the level of human security. Project Human Security Index was realized in the period 2008-2010 and encompassed more than 200 countries and territories. The HSI shows the individual security of citizens in cities, at the state level and globally. The HSI includes the analysis of three main domains: economic, environmental and social in terms of sustainable development, social responsibility and other relevant areas. Due to the number of individual indicators, this project is technically realized in open-source software, which enables the definition of new, modification and reconfiguration of existing indicators and creation of a new composite index HSI. The HSI project is aimed at supporting the use of existing and development of new indicators by analysts and policy makers of urban planning and development in the domain of human security (Hastings, 2011).

Visualization in the domain of HS data

The efficient application of complex HS indexes can be achieved using the visualization process. Visualization is a large amount of data analysis technique that permits the perception of internal relationships and the perception of different forms of data configurations. Visualization in the field of human security can help analysts,

in addition to presenting the current state, identify potential problems and threats that can possibly occur.

An example of the use of visualization in the domain of human security can be found in the document: *Assessing Human Insecurity Worldwide: The Way to a Human Security Index*, (Werthes, 2011). The document displays a multi-dimensional index [Human (In) Security Index], which allows the assessment of appropriate levels of human (non) security. The operationalization process is applied to all dimensions of human security in order to reach the global index and is one of the possible conceptual approaches for analysing the current situation and potential threats in the field of human security. An example of a visual representation of the Global Index of Human Security is presented in Figure 3.

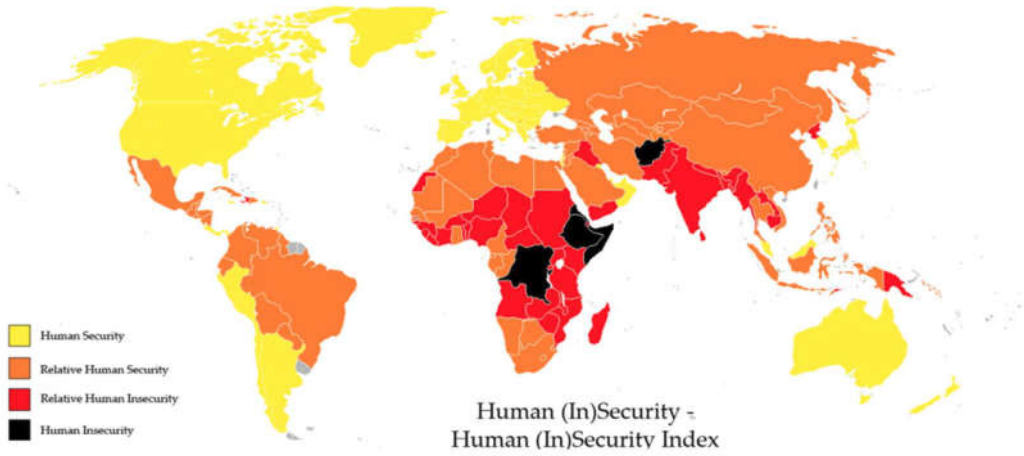


Figure 3: World Map – Human (In)Security

Source: Werthes, S., Heaven C. Vollnhals S. (2011): Assessing Human Insecurity Worldwide: The Way to A Human (In)Security Index. Institute for Development and Peace, University of Duisburg - Essen (INEF - Report 102/2011) pg.40.

HS Networks

Among numerous applications of the ICT in the field of human security a significant place is given to an activity taking place on the Internet through the development of websites and the creation of networks by institutions and interested groups of citizens. One of the most important networks is the *Human Security Network* (HSN), whose activity is coordinated by the United Nations.

The Human Security Network consisting of 12 countries aims at promoting the concept of human security as relevant to the creation of national and international policies. Of particular importance is the fact that the activities of the network take place within the United Nations through cooperation with academic institutions and civil society

organizations. The network was established in 1999 after successful cooperation between Austria, Norway and Canada in order to achieve an international ban on anti-personnel mines. Current members of the Network are: Austria, Chile, Costa Rica, Greece, Ireland, Jordan, Mali, Norway, Panama, Slovenia, Switzerland and Thailand, and South Africa has an observer status. The activity of the network is coordinated by the Special Representative of the Secretary General for Human Security and the Human Security Unit. (https://www.un.org/humansecurity/), and each year the work of the Network is chaired by one of the network members. The Network's activity is aimed at familiarizing the UN member states with the significance of applying the concept of human security in the work of the United Nations. (Fuentes, 2009).

Human security & artificial intelligence

The application of Artificial Intelligence (AI) technology is one of the positive effects of ICT that provides an efficient response in real time to various human security related issues. (Roff, 2017). Achievements in AI's development allow the international community, governments and civil society to anticipate and prevent various forms of threats to human security. AI applications related to the search, classification, and recognition of threat indicators can help analyse correlations and extract content from multiple sources as well as based on large amounts of data.[6]

The potential for AI application is particularly evident in situations such as complex humanitarian crises where there is a combination of the negative effects of political and natural factors. In these situations, data on available resources can be processed and satellite-based real-time monitoring of terrain can be used, overcoming the time constraints for emergency interventions, and thus reducing the number of casualties or material damage. Preventive measures can be taken using the advantages of mobile networks and various media. For example, permanent monitoring of problem areas or environments of companies that can be a source of pollution provides an adequate and timely response in the field of environmental protection.

By combining sensors and video devices to collect information from the environment, AI applications raise security at the individual level, that is, they prevent the endangerment of people in public areas and in their homes. In addition, processing information about persons under judicial supervision of the AI allows for predicting potentially violent behaviour by monitoring their field activities.

In the field of health care, there are many advantages of using AI. The ability of AI to classify and identify medical data and recordings allows the recognition of complex

[6] "The new IBM X-Force Threat Management Services uses an artificial intelligence (AI) engine to automate active threat management. The platform compares security incidents against 600,000 historical use cases, and can help automate parts of the threat management process that would typically require human intervention, according to the release. The new Resilient Incident Response Platform can help security analysts orchestrate and automate hundreds of repetitive, complicated response actions that previously required a lot of time. It also offers enterprise-grade integrations out of the box, according to the release, and a drag-and-drop business process management notation workflow engine" (DeNisco Rayome, 2018).

correlations and the establishment of medical diagnostics much faster and more precisely in relation to a process that depends exclusively on human factors.

A good example of application of AI in the field of human security is a digital food safety information portal that consolidates data from international food agencies, food alert systems, news sources, food manufacturers and social media, into a single access point. For the first time the entire food value chain and any associated health risks in one single place are presented. The service is designed to increase transparency across the food value chain – protecting consumers and the reputation of brands. Internet portal *Safefood.ai* can be customized to ensure to stay up-to-date with all public food safety risks, relevant to the raw materials and ingredients, covered by supply chains (Selz, 2018).

In the field of economic security, the application of AI in the new economic development paradigm called *The Economics of Abundance* (Hoeschele, 2010) is interesting. The *Economics of Abundance* is based on a critique of the current economic system based on the exhaustion of natural resources, which results in devastation of the living environment. The application of the new economic paradigm can be spurred largely by digital communications, using renewable energy sources and efficient means of transport. Companies and institutions that operate on new principles in theory are recognized as *software-driven entities*. AI's application of management and control in resource exploitation, as well as the achievement of optimum working conditions can significantly contribute to the safety of people.

6. CONCLUSION

The security environment that arises with the 4te Industrial Revolution (4IR) drastically differs from the conditions in which an existing institutional model based on national states and the current world order based on the Westphalian agreement emerged. A system based on the achievements of the first industrial revolution is unable to satisfy the needs of modern actors of the new era. It is in the interest of all actors to find a new model of functioning of modern civilization because they are exposed to new risks and threats due to the lack of a global institutional system. In the current circumstances, the power of practical action is on the side of the controllers of large capital, but citizens can still influence the creation of new conditions through the current democratic system. The concept of human security is precisely reminiscent of the obligation of states to protect their citizens.

The concept of human security reminds us that the interests of states and economic entities cannot be protected by endangering the basic human rights. Protection of human rights is a basic premise of the existing UN system and represents an international obligation all countries have to comply with. The undertaken measures in emergency conditions must be in accordance with international conventions and must not jeopardize the human rights of the affected population. To that end, the European Parliament has adopted certain codes of conduct and guidelines for the implementation of human rights obligations when undertaking restrictive and security measures. (Council of Europe, 2002). In the given context, the adoption of the Charter on Human Rights and Principles for the Internet, which is based on the Universal Declaration of Human Rights, provides a comprehensive

approach to the interpretation of human rights in information societies. (Charter on Human Rights and Principles for the Internet, 2018). The Council of Europe has taken a leading role in the development of guidelines, code of conduct and recommendations on the preservation of public services on the Internet, especially in the context of human rights. (Kettemann, Matthias, 2011).

It should be emphasized that the ICT and AI provide certain opportunities, but do not have ready solutions for all problems in the field of Human Security. Through a multidisciplinary approach, AI can contribute to understanding the process through modelling and replication of cognitive processes. Based on various computer, logical and natural principles, the application of AI can raise the level of efficiency in solving certain security tasks. However, the ICT with the use of AI is not able to completely replace people's decision-making, but it can help achieve the goal of reducing human insecurity by maximizing the positive and reducing the negative effects of applying existing human knowledge. The requirement for positive effects of the ICT implementation is transparent and responsible behaviour in the field of Human Security, which can be followed by strict rules with an appropriate system of controlling their application. Establishing a new global institutional system based on democratic traditions is the only acceptable path to a sustainable global community of people on the planet earth.

7. REFERENCES

Andreou, A. (2013). The rise of money trading has made our economy all mud and no brick. *The Guardian*, Wed 20 Nov. Visited 09.VIII 2018. on: https://www.theguardian.com/commentisfree/2013/nov/20/money-trading-economy-foreign-exchange-markets-economy

Bartlett, J. (2018). *The People vs. Tech: How the Internet is Killing Democracy.* New York: DUTTON.

Bellamy, A. J. (2009). *Responsibility to* P*rotect: The Global Effect to End Genocide and Mass Atrocities*. Cambridge: Policy Press.

Benedek, W. (2012). Human Security in the Information Society. *Human Security Perspectives*, Volume 9, Issue 1, 1-14.

Council of Europe (2002). *Guidelines On Human Rights And The Fight Against Terrorism*, 11 July. Strasbourg.

DeNisco Rayome, A. (2018). *How IBM's new cyber tools use AI to make human security pros more effective.* TechRepublic, April 16. Visited 19.IX 2018. on: https://www.techrepublic.com/article/how-ibms-new-cyber-tools-use-ai-to-make-human-security-pros-more-effective/

Đorđević, Lj. I. (2013). *Ljudska bezbednost – globalni kontekst i primena u Srbiji*. Beograd: Dosije Studio i Institut za uporedno pravo.

Franklin, M., Bodle, R. and Hawtin, D. eds. (2018). *Charter on Human Rights and Principles for the Internet.* Internet Rights & Principles Coalition. UN Internet Governance Forum. Visited 19.VIII 2018. on: http://internetrightsandprinciples.org/site/wp-content/uploads/2018/01/IRPC_english_5thedition.pdf

Fuentes, C. and Brauch, H. (2009). *The Human Security Network: A Global North-South Coalition*. Berlin Heidelberg: Springer-Verlag.

Fukuda-Parr, S. (2003). New Threats to Human Security in the Era of Globalization. *Journal of Human Development*, Vol. 4, No. 2, July.

Hastings, D. A. *(2011). Human Security Index: Update and New Release*, Visited 19. IX 2018. on: http://www.humansecurityindex.org/wordpress/wp-content/uploads/2011/03/hsiv2-documentation1.pdf

Hoeschele, W. (2010). *The Economics of Abundance: A Political Economy of Freedom, Equity, and Sustainability*. Aldershot: Gower Publishing.

International Commission on Intervention and State Sovereignty - ICISS (2001). *Responsibility to Protect.* Ottawa: International Development Research Centre.

Kamei, K. (2013). Human Security and Globalization. *Journal of Poole Gakuin University,* Vol. 54, 63 – 76.

Kettemann, C. M. (2010). Ensuring Human Rights Online: An Appraisal of Selected Council of Europe Initiatives in the Information Society Sector in 2010. in: Benedek, W.; Benoit-Rohmer F.; Wolfram, K. and Manfred, N. (eds.) (2011). *European Yearbook On Human Rights*, Vienna: Intersentia. 248-267.

Latonero, M. and Gold, Z. (2015). *Data, Human Rights & Human Security.* New York: Data & Society Research Institute.

Reif, L. R. (2018). *A survival guide for The Fourth Industrial Revolution*, Davos: World Economic Forum. Visited 19.VIII 2018. on: https://www.weforum.org/agenda/2018/01/the-fourth-industrial-revolution-a-survival-guide/

Roffm, H. (2017). *Advancing Human Security through Artificial Intelligence.* Research Paper. London: Chatham House, the Royal Institute of International Affairs.

Selz, D. (2018). *Launch of Safefood.ai – The world's first AI driven Food Safety Intelligence Service*. June 12. Visited 19.VIII 2018. on: https://squirro.com/2018/06/12/launch-safefood-ai-worlds-first-ai-driven-food-safety-intelligence-service/

UNDP (1994): *Human Development Report*. New York – Oxford: Oxford University Press.

Werthes, S., Heaven, C. and Vollnhals S. (2011). *Assessing Human Insecurity Worldwide:The Way to A Human (In)Security Index*, INEF Report 102/2011, Institute for Development and Peace, Universität Duisburg – Essen.

UDK 343.344:17
https://doi.org/10.18485/fb_ic4hs.2018.4

NON-LETHAL WEAPONS IN DOMESTIC LAW ENFORCEMENT: SOME LEGAL AND ETHICAL ASPECTS

Adelina TUMBARSKA*

Abstract: The main principle embodied in the concept of non-lethality is the intention of avoiding fatalities and permanent injuries to people and damage to material objects and the environment. Accordingly, non-lethal weapons (NLWs) are designed to produce short-lasting and reversible effects, unlike conventional weapons intended to cause large-scale death and destruction.

International law (IL) is a key instrument for NLWs development and use. However, there are significant gaps and ambiguities in IL regulating the use of weapons and international standards with respect to the legitimate use of NLWs in law enforcement (LE), which cast doubt on the use of NLWs. According to international standards, firearms should be used only exceptionally in LE and governments are therefore encouraged to develop and equip LE officials with NLWs. At the same time, existing laws and policies do not sufficiently stimulate the utilization of NLWs' potential as an alternative to deadly weapons.

Despite significant progress in the development and improvement of NLWs, they are not perfect –the potential for undesirable consequences always exists, since their effects depend on many factors i.e. zero lethality is a goal, not a guarantee. However, problems lie predominantly in the way NLWs are used rather than in the technology itself. The use of NLWs is sometimes untimely, unnecessary or improper, giving grounds for considerable public disapproval.

NLWs have been used in LE all over the world since the 1960s. The interest in their military applications, declared in the early 1990s, initiated extensive debates involving scientists and experts from various fields, politicians, human rights activists, and citizens. These debates are ongoing and concern all aspects of NLWs – conceptual, political, ethical, legal, medical, technological, strategic, operational, tactical, etc.

This paper represents an effort to briefly address the most important legal and ethical problems and discussions arising from the use of non-lethal weapons in domestic law enforcement, as far as this is possible in 12,000 characters including spaces.

* Assistant-Professor, PhD, Institute of Metal Science, Equipment and Technologies, Bulgarian Academy of Sciences (IMSETHAC-BAS), y.toumbarski@ims.bas

Key words: non-lethal weapons (NLWs), law enforcement

1. INTRODUCTION

Under International law (IL), each State has obligations to respect, protect, ensure and fulfil human rights (ICRC, 2015), including to ensure that its law enforcement (LE) agencies and officials respect and protect the right to life (Geneva Academy of IHL, 2016). According to international standards, "[e]very effort should be made to exclude the use of firearms." (UN, 1997, Art.3) Governments are encouraged to develop and equip LE officials with weapons "that would allow for a differentiated use of force and firearms", including non-lethal weapons (NLWs). (UN, 1990, Art.2) However, the standards with respect to use of NLWs in LE [and IL regulating the use of weapons as a whole] are outdated or ambiguous in a number of key areas. (Dymond-Bass & Corney, 2014).

Law enforcement comprises not only domestic peacetime policing but also a number of other functions, such as counter-terrorism, counter-narcotics, border protection, etc. In any situation LE officers must perform their duties in accordance with applicable national and international law, complying with rigorous ethical and professional requirements. The need to manage individuals or groups, when a show of force or voice commands are not sufficient and deadly force is not authorized or preferred, is a difficult aspect of the civil LE. To meet this need, LE institutions are widely applying non-lethal technologies in the continuing efforts to protect lives, including of those attempting to harm LE officers or other citizens.

Non-lethal alternatives to conventional weapons are welcomed by LE officers, as they provide means to control various situations with reduced risk for all persons involved and prevent the escalation of force. However their use is not acceptable to everyone. "Criticism has come from suspects, politicians, activists, and citizens. Arguments include the legitimate concerns for human rights and the potential for abuse" (Penn State University, 2010, p.6-3), even claims that NLWs are unhuman, especially created for torture. These critics are part of a large debate on all aspects of NLWs, initiated by the interest in NLWs military applications declared in the early 1990s.

2. NON-LETHAL (LESS-LETHAL) WEAPONS CONCEPT

Intention embodied in the concept of non-lethality is avoiding fatalities and injuries on people and damage to material objects and the environment. Accordingly, non-lethal weapons are designed to produce short-lasting and reversible effects. Since the effect of a NLW depends on many factors (weapon characteristics, user skills, context, targeted object characteristics, etc.), potential for undesirable consequences always exist. Principles underlying the NLWs concept give reason to believe that these weapons are more human and ethically superior than conventional, but ultimately conclusion whether NLWs are more ethical depends on the way they are used.

The concept of NLWs in very complex, therefore finding correct term and formulating correct definition is a difficult task. Much of confusions and controversies surrounding NLWs come from the lack of universally accepted term and definition (Barron, 2008). Yet

all existing definitions include the compulsory requirement of avoiding death or injuries and no one - assurance of the full absence of lethal effects. 'Non-lethal weapons' is a term introduced in the 1960s. Though even then it was noted that to avoid misconceptions or false expectations in must be borne in mind that 'nonlethal' is relative, not absolute term (Coates, 1970, p.2), this term is still criticized and defined from 'incorrect' to 'intentionally misleading'. Although far from perfect, it clearly expresses the intention of user not to cause damage and is established as the most used one amongst dozens of proposed terms ('less-lethal' is term preferred by LE community in some countries). In the context of civil LE, less-lethal weapons (LLWs) are those "primarily designed to temporarily disable or stop suspects without killing, thereby providing an alternative to lethal force where appropriate. These weapons are 'less lethal' in a literal sense because none can be guaranteed to avoid serious injury or death". (National Security Research, 2003, p.10)

3. SOME LEGAL AND ETHICAL ASPECTS OF THE NLWS' USE IN DOMESTIC LAW ENFORCEMENT

NLWs have been used by police over the world since the 1960s as an alternative or addition to police batons and firearms in controlling aggressive crowd behavior. (Davison, 2009) At present LE forces are equipped with a wide range of NLWs used in various operations ranging in character and intensity - from confrontations 'one to one' to large-scale organized disorder and violence. Despite the experience gained, the use of certain NLWs can result in unintended outcomes under certain conditions. Research has shown that problems are rather in tactics, procedures, policies, training and use of NLW than in technology itself (Penn University, 2010) - large part of accidents, including amongst users, are due to improper handling. Thereby the Human Rights Council, encouraging states to make NLWs available to their LE officials, also encourages international efforts to regulate and establish protocols for training and use of NLWs. (Geneva Academy, 2016)

Combining the maintenance of public order at meetings with the right to freedom of speech, freedom of dissent and the right to assembly is a serious challenge. (Casey-Maslen, 2014) NLWs with worst reputation in such situations are the kinetic non-lethal munitions and the chemical riot control agents (RCAs), particularly tear gas. Although modern impact munitions has been significantly refined, compared to plastic and rubber bullets that have led to a number of deaths in the past, they still can cause injuries if directed to some parts of the human body or shot at too close distance. RCAs are widely debated, as their use as "method of warfare" is prohibited unlike the use in "law enforcement including domestic riot control purposes". (Chemical Weapons Convention, 1993, Art.II,9,d). In other words, chemical RCAs „are lethal enough to fall under the CWC of 1993, but in domestic affairs during times of peace, when human rights law is the applicable legal regime, these same riot control agents are accepted as a riot suppressant against often innocent civilians". (Knoechelmann, 2012, p.1) There are views that partial or radical changes in IL are needed to allow for use of RCAs in armed conflicts (Fidler, 2001), and vice versa - that RCAs should be totally prohibited. The last indicates "lack an

understanding of the benefits and necessity of RCAs as a tool of protecting public order". (Knoechelmann, 2012, p.34)

Other distaste with NLWs comes from their use on suspects, detainees and prisoners. There are claims that NLWs are used untimely or unnecessarily, "in situations that would have previously been resolved with the use of less force, or even without the use of any force at all". (Coleman, 2012, p.198) Evidences exist that many US police agencies are routinely deploying 'Tasers' to subdue individuals who do not pose a serious danger to themselves or others. (Amnesty International, 2002) Most claims in the US judicial system connected with NLWs are based on the use of 'excessive force' resulting from choice of incorrect weapon/ammunition or its use outside the established guidelines. (Penn University, 2010) Though, "[w]hen used responsibly by well-trained and fully accountable law enforcement officials, LLWs can prevent and minimize deaths and injuries to assailants, suspects and detainees, as well as protect the police and prison officers themselves". (Amnesty, 2015)

Abuses of NLWs by repressive governments are regularly documented by several organizations. Reports expose terrible practices of torture or extraction of information from suspected criminals and dealing with political opponents or non-tolerated religious and social groups applied in some countries. (Bureau of Democracy, 2017) Apart from barbarian methods and tools, torturers rely on more advanced technologies - examples of abuse of 'Tasers', rubber bullets and tear gas are highlighted in a number of Amnesty International and Omega Foundation reports. These institutions call for banning NLWs export to countries where they are used for human rights violations to "back moral responsibility with legal liability". (Wright, 2001, p.223)

Counter-terrorist operations pose great challenges as terrorists are often mixed with citizens, whether hostages or passers-by. Although certain NLWs significantly increase the probability for saving hostages and capturing terrorists alive, their use is perceived in contradictory ways. An emblematic case in this regard is the hostage rescue action in Moscow in 2002. After 2-day siege of the theater, where 40-50 heavy armed Chechen terrorists put bombs and held 916 hostages, Russian spec-forces introduced an anesthetic agent into the ventilation system and then stormed the building. As a result 129 hostages lost their lives (many due to inadequate evacuation and medical care) and all the terrorists were shot. This operation is widely criticized, however although it may seem excessive that 16% of the hostages died from or after the gas exposure, 84% survived; "The use of an 'incapacitant' in this setting was a novel courageous attempt at saving the most lives". (Reimann, 2007, p.3a-7). This case provoked discussions on incapacitating chemical agents (ICAs) in general, and on the legality of their use in LE. The right conclusion seems to be that use of ICAs "in contexts where neither individual dosage nor the exposure conditions can be controlled is legitimate only in extreme situations". (Fidler, 2005) Killing the incapacitated terrorists, instead of being arrested and handed to justice, brings to the fore a very important problem – about the use of NLWs for facilitating the use of deadly force.

Many official documents state that NLWs are developed to provide LE with an alternative to lethal force, however policy and practice cast doubt on these allegations – the

authorities who control the police use of NLWs are often too cautious to use them as a substitute for lethal weapons. (Davison, 2009) Other documents clearly show the intention that NLWs "should never be considered a replacement for the legal use of lethal force" rather LE officers should use them "as an instrument of force continuum between show of force or verbal commands and deadly force". (National Security Research, 2003, p. 10) Indeed, although LE officers are required to employ only 'reasonable' or 'proportionate' levels of force, there is no legal obligation of using NLWs first before resorting to lethal weapons. Some suppose that "the law may well develop in the direction of requiring them to proceed with the less deadly means first". (Koplow, 2005, p.796) However, given the resistance of some states to the adoption of international treaties restricting the use of lethal weapons, this is unlikely to happen.

4. CONCLUSION

While NLWs conception gives reasons to believe that they are more human and ethical than conventional weapons, examples of their use (from involuntary mistakes to deliberate abuse) are constantly emerging and raising doubts about such an assertion. Improving the use of NLWs in LE can be achieved through developing appropriate policies and procedures for use, review and supervision, and creating laws and policies stimulating utilization of the NLWs' potential as an alternative to deadly weapons. Although not perfect, NLWs provide domestic LE authorities with capabilities to apply low levels of force in maintaining law and order and controlling violent situations. Undoubtedly, public debates are necessary to ensure that NLWs are developed and used in accordance with law and ethics. An unbiased and informed discussion would be even more constructive, focusing not only on negatives accumulated over the years but also recognizing the benefits of implementing NLWs.

5. REFERENCES

Amnesty International. (2002). Excessive and Lethal Force? Amnesty International's Concerns about Deaths and Ill-Treatment Involving Police Use of Tasers. Amnesty International, Retrieved from https://www.amnestyusa.org/reports/usa-excessive-and-lethal-force-amnesty-internationals-concerns-...

Amnesty International. (2015, April 13). 'Less-lethal' weapons can kill and police misuse them for torture. Retrieved from https://www.amnesty.nl/actueel/less-lethal-weapons-can-kill-and-police-misuse-them-for-torture

Barron, B. (Ed.). (2008). Non-Lethal Weapons International Study. Pennsylvania, USA: Penn State Fayette, Retrieved form http://fieldcommand.org/wp-content/uploads/2013/05/ Penn-State-Intl-NLW-study.pdf

Bureau of Democracy, Human Rights and Labor. (2017). Country Reports on Human Rights Practices. U.S. Department of State. Retrieved from https://www.state.gov/documents/organization/277207.pdf

Casey-Maslen, S. (2014). Crowd management, crowd control, and riot control. In S. Casey-Maslen (ed.). Weapons under International Human Rights Law. Cambridge, UK: Cambridge University Press.

Coates, J. (1970). Non-Lethal and Non-destructive Combat in Cities Overseas. Alexandria, USA: Institute for Defense Analyses. Retrieved form http://www.dtic.mil/dtic/tr/fulltext/u2/745773.pdf

Coleman, S. (2015). Possible Ethical Problems with Military Use of Non-Lethal Weapons. Case Western Reserve Journal of International Law. 47 (1), Issue 1, 185-199.

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction. (1993). Geneva, CH. Retrieved form https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVI-3&chapter =26&lang=en

Davison, N. (2009). Non-Lethal Weapons. London, UK: Palgrave Macmillan. Retrieved form https://link.springer.com/chapter/10.1057/9780230233980_2

Dymond-Bass, A. & Corney, N. (2014). The use of 'less-lethal' weapons in law enforcement. In S. Casey-Maslen (ed.). Weapons under International Human Rights Law, Cambridge, UK: Cambridge University Press.

Fidler, D. (2001). 'Non‐lethal' weapons and international law: Three perspectives on the future. Medicine, Conflict and Survival. 17(3). 194-206. DOI: 10.1080/13623690108409579.

Fidler, D. (2005) The meaning of Moscow: 'Non-lethal' weapons and international law in the early 21st century. International Review of the Red Cross, 87(859). 525-552. Retrieved from https://www.icrc.org/eng/assets/files/other/irrc_859_fidler.pdf

Geneva Academy of International Humanitarian Law and Human Rights. (2016). Use of Force in Law Enforcement and the Right to Life: The Role of the Human Rights Council. Academy In-Brief, No 6. Geneva, CH: The Academy. Retrieved from https://www.geneva-academy.ch/joomlatools-files/docman-files/in-brief6_WEB.pdf

International Committee of the Red Cross. (2015). The use of force in law enforcement operations. Geneva, CH: ICRC. Retrieved from https://www.icrc.org/.../the-use-of-force-in-law-enforcement-ic...

Knoechelmann, K. (2012). The Legal Paradox of International Chemical Riot Control Regulations. Association for the Promotion of International Humanitarian Law. Retrieved form http://www.alma-ihl.org/opeds/knoechelmann-riotcontrolagents102012

National Security Research. (2003). A Research Guide for Civil Law Enforcement and Corrections, USA: Department of Justice. Retrieved form https://www.ncjrs.gov/pdffiles1/nij/grants/200516.pdf

Penn State University. (2010). Guidebook for Less-Lethal Devices: Planning for, Selecting, and Implementing Technology Solutions. Pennsylvania, USA: WPSTC.

Reimann, K. (2007). Non-Lethal Technology (NLT) Approaches to Hostage Situations. NATO Research and Technology Organization Report NATO RTO-EN-HFM-145. Retrieved from https://www.sto.nato.int/publications/pages/results.aspx?sq=1&k=non-lethal%20weapons&s=Search%20All%20STO%20Reports

United Nations. (1979). Code of Conduct for Law Enforcement Officials. Adopted by United Nations General Assembly resolution 34/169 of 17 December 1979, Retrieved from https://www.ohchr.org/Documents/ProfessionalInterest/codeofconduct.pdf

United Nations. (1990). Basic Principles on the Use of Force and Firearms by Law Enforcement Officials. Adopted by the 8th UN Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 Aug. to 7 Sept. 1990. Retrieved from https://www.ohchr.org/en/professionalinterest/pages/useofforceandfirearms.aspx

Wright, S. (2001). The role of sub‐lethal weapons in human rights abuse. Medicine, Conflict and Survival, 17(3). 221-233. DOI: 10.1080/13623690108409581.

UDK 623.454.8(497.1)
https://doi.org/10.18485/fb_ic4hs.2018.5

OPEN DATA AND AVAILABLE RESEARCH ON DEPLETED URANIUM WEAPONS – REASONS FOR CONTROVERSY (YUGOSLAVIA 1999 - CASE STUDY)

Nada SEKULIĆ*

Abstract: The paper addresses the question: How is public opinion built in the absence of reliable data? The theoretical background in this approach is based on the theories of public opinion which assume that "individuals do not turn to media primary for truth or information, they turn to the media to help themselves define social reality" (Moy & Bosch, 2013). This means that public opinion, and particularly public opinion on controversial issues which are not presented in a transparent and objective way, is built on stereotypes framed by political assumptions and affinities, without making a clear distinction between facts and preferences.

The paper presents the results of an online survey conducted on a sample of 534 Serbian citizens, in which we tried to use the approach mentioned above as a hypothesis and to operationalize and prove it by covering the issue of the usage of depleted uranium (DU) weapons in the 1999 NATO bombing of the FRY. The results show that the attitude about the harmful effects of DU munitions depends strongly on the political affinities of the respondents towards the East or the West and on their views on how the crises in Kosovo should be resolved. It also correlates strongly with their positive/negative identification with the Serbian national identity.

Keywords: depleted uranium, military operation "Noble Anvil", public opinion on the NATO bombing of the FRY

1. INTRODUCTION

On May 18, 2018, nearly twenty years after the NATO military intervention against the FRY, the government of Serbia established a special commission with the task of estimating the effects of the usage of depleted uranium (DU) during the military intervention "Noble Anvil". During these two decades, the chances to thoroughly and continually monitor the citizens and areas which had been exposed to DU was lost, in spite

* Full Professor, PhD, University of Belgrade Faculty of Philosophy, wu.wei@orion.rs

of the fact that the bombing of the FRY was the first case in which NATO was forced to publicly confirm the usage of DU munitions.

In the absence of a clear strategy and action plan by the state, which would provide information about the facts, various controversial pieces of information have emerged in the media estimating the scope of the ecological disaster produced by DU weapons. The issues of DU's carcinogenic activity and whether there has been a disproportionate increase in malignancies in Serbia over the past two decades have been particularly controversial. Experts and laymen – politicians, celebrities, doctors, NGO activists, lobbyists, lawyers, public figures – all gave statements to the media, which were often brought into the spotlight in sensational talk shows. They provided little explanatory information about cognitive, military-political or ethical concerns. Dramatic images of public battles and unpleasant situations among the guests of these shows increased the ratings of these programs, but did not contribute to the development of objective and impartial journalism.

In such context, the public has not had enough sources and open social space to develop a rational and cognitive approach to the issue.

1. THE ONLINE SURVEY "IMPACT OF PUBLIC POLITICAL PREFERENCES ON ATTITUDES ABOUT DETRIMENTAL EFFECT OF DEPLETED URANIUM (DU) WEAPONS"

An online pilot survey was conducted on a sample of 534 respondents. The survey was publicly distributed on the Facebook social network during the summer of 2018 and was available until it was filled in by around 500 respondents. The only requirement for the respondents was that they were citizens of Serbia (including those with dual nationality, who encompassed 3.8% of the sample). The data were not used for generalizations, but with the preliminary purpose of examining the structure of responses and the interdependence between four groups of questions/topics: 1) attitudes of the respondents about the detrimental effects of depleted uranium, 2) the political preferences of the respondents regarding the status of Kosovo, 3) political preferences towards Western or Eastern countries/political blocks, 4) affirmative/negative attitudes toward the Serbian identity and Serbian self-identification.

The main aim of this research was to examine if and how much the public opinion relating to DU was influenced by the broader public's political opinions and preferences.

The research uncovered "deep play" (Geertz, 2005) between opposing political groups/subjects, in which a cognitive issue (the detrimental effects of DU) becomes the stake in their public gaming/betting for social approval and support. This political battle has the "all-or-nothing" form, since audience cannot bet on both sides/parties and have to choose only one political side/party. Just as in the case of the Balinese cocks in Geertz's story of the Balinese, here we have "deep play", which transfers the debate and raw fight between political groups to the "pseudo-cognitive" debate on DU. This debate also takes

the form of an "all-or-nothing" discourse aiming at persuasion between "right" and "wrong", which is a form of political betting.

Since most of the respondents (83%) declared themselves as Serbian (9.9% did not answer the question, 2.2% are Yugoslav and all other options are below 1%), we could also interpret the data referring to the Serbian identity as positive or negative ethnic self-identification.

2. DESCRIPTIVE ANALYSES

2.1. ATTITUDES ABOUT THE DETRIMENTAL EFFECTS OF DEPLETED URANIUM (ADU)

This group of questions included six statements, which were used as a composite variable defining the attitude of the respondents towards the detrimental effects of depleted uranium, with an emphasis on its carcinogenic effects. The list of responses offered in the online questionnaire was longer, but these six items satisfied the requirements of consistency, homogeneity and normal distribution.

Table 1. Items of the composite variable: Attitudes about the detrimental effects of depleted uranium (with an emphasis on its carcinogenic effects), and the correlation matrix between them

1=strongly disagree, 2= partially disagree, 3= neither, 4= partially agree, 5= strongly agree

R= responses that required reverse scoring

	%	*1*	*2*	*3*	*4*	*5*
1	(I believe that) bombs with depleted uranium cause cancer.	8.4	5	17	20.8	49
2	A lot of research and data confirm the devastating effects of depleted uranium, but their publication is being obstructed.	11.6	8	32.4	20.6	27.4
3	In Serbia there has been an extraordinary increase in the number of cancer diseases due to the depleted uranium bombing.	9.2	6.7	23.7	23.5	37
4	It was high time for the Serbian government to form a commission to investigate the consequences of the 1999 NATO bombing.	10.9	4.2	16	18.3	50.6
5	**R** It has been scientifically proven that depleted uranium bombing does not cause cancer.	46.1	9.9	31	5.1	7.8
6	**R** It is irresponsible to confuse people with questions about depleted uranium twenty years after the bombing.	43.8	17	11.3	13	14.9

Correlation matrix (Pearson's):

	1	2	3	4	5	6
1	1.00	.684	.793	.610	.686	.558
2	.684	1.00	.672	.528	.566	.423
3	.793	.672	1.00	.615	.630	.537
4	.610	.528	.615	1.00	.500	.535
5	.686	.566	.630	.500	1.00	.504
6	.558	.423	.537	.535	.504	1.00

Cronbach's alpha=0.893; Mean: .589; Min..423, Max..793; Kaiser-Meyer-Olkin Measure=.897; Bartlett's test of Sphericity (Sig.)=.000

The responses show that majority of the respondents believe that DU bombs (i.e. munitions) have carcinogenic effects. According to their responses, this has also been the main cause of the increase in carcinogenic diseases in Serbia since the 2000s. Most of them take the health issue caused by the 1999 bombing very seriously and think that the Serbian government still has a duty to investigate the case. The majority of them do not agree with the statement that it has been scientifically proven what exactly is the effect of DU bombing and believe that the publication of the data that question NATO's reports have been obstructed. In addition, only 6.7% trust the reports of NATO (NATO's reports do not confirm the carcinogenic influence of DU munitions). (Due to the lack of normal distribution, the last statement was unsuitable to be included in the composite variable and was analyzed as independent variable – almost 80% /78.9%/ of the respondents do not trust NATO's research and public data on nuclear weapon.)

2.2. THE POLITICAL PREFERENCES OF THE RESPONDENTS REGARDING THE STATUS OF KOSOVO (AK)

The composite variable was made of eight statements which related to the respondents' understanding of the political crises in Kosovo and their vision for the solution of the problem. These eight statements proved to be consistent and suitable in all aspects for parametric analyses. The table below shows the respondents' choices and the correlation matrix between these eight statements.

Table 2. The political preferences of the respondents regarding the status of Kosovo and the correlation matrix between them

1=strongly disagree, 2= partially disagree, 3= neither, 4= partially agree, 5= strongly agree

R= responses that required reverse scoring

	%	1	2	3	4	5
1	Instead of being put behind bars for organizing the bombing of the FRY, Madeleine Albright and Wesley Clark are buying mines and businesses in Kosovo.	5.2	3.4	22.5	19.7	49.2
2	Kosovo is Serbia.	16.8	8.2	14.3	11.9	48.8
3	The attitude of Albanians towards the monuments of Serbian medieval Orthodox culture in Kosovo is in itself a sufficient reason for Serbia not to recognize Kosovo.	10.9	11.1	16.3	14.9	46.7
4	Kosovo – the heart of Serbia.	25.1	10.2	17.8	12.3	34.7
5	Concerning Serbian culture in Kosovo, Albanians are the same as the Taliban.	8.2	7.3	18	16.1	50.5
6	**R** Whether someone likes it or not, the fact is that Serbia has lost Kosovo.	24.7	12.2	14.9	20.1	28.1
7	**R** Serbian property in Kosovo is lost. It's best not to discuss it again.	45.6	17.2	10.9	15.1	11.3
8	**R** Serbian generals who hide their responsibility for killing Albanian civilians in Kosovo do not have the legitimacy to speak about the harmful consequences of the FRY bombing.	23.2	9	21.5	20.3	26.1

Correlation matrix (Pearson's):

	1	2	3	4	5	6	7	8
1	1.00	.484	.459	.478	.421	.411	.329	.320
2	.484	1.00	.704	.775	.458	.654	.618	.469
3	.459	.704	1.00	.650	.422	.523	.498	.385
4	.478	.775	.650	1.00	.394	.620	.549	.507
5	.421	.458	.422	.394	1.00	.328	.289	.318
6	.411	.654	.523	.620	.328	1.00	.657	.468
7	.329	.618	.498	.549	.289	.657	1.00	.398
8	.320	.469	.385	.507	.318	.468	.398	1.00

Cronbach's alpha: .883; Mean: .485, Min. 289, Max.775; Kaiser-Meyer-Olkin Measure=.902; Bartlett's test of Sphericity (Sig.)=.000

The list of the offered responses related to Kosovo was longer, but not all of them could be included in the composite variable. Some of these responses show that the majority of the respondents have an almost identical opinion regarding certain issues – 81.7% of the respondents do not agree with the attitude that Serbs got what they deserved in Kosovo, 79.4% think that Albanians conducted preplanned cultural genocide against Serbs in Kosovo, and 65.2% are against the recognition of Kosovo.

The indicators included in the common variable cover the issue of Serbian war crimes in Kosovo, the issue of Serbian property in Kosovo, Albanian destruction of Orthodox heritage and Serbian culture in Kosovo and attitudes about the independence of Kosovo.

2.3. POLITICAL PREFERENCES TOWARDS EASTERN/WESTERN POLITICAL ALLIES (AEW)

We combined eight indicators into a single variable measuring the respondents' political preferences towards the East or West. Conceptually and statistically, this variable proved to be consistent and suitable for further analyses as well. It encompassed a range of statements related to Serbia's potential membership in the EU, military cooperation with Russia, positive or negative attitudes towards the German/Russian people, and the affinity towards public figures such as Russian president Vladimir Putin. All statements were designed to measure solidarity, affinity, the political assessment of the East or West and the ideas about what kind of military alliances would be best for the future of Serbia.

Table 3. The political preferences regarding Eastern/Western countries and the correlation matrix between them

1=strongly disagree, 2= partially disagree, 3= neither, 4= partially agree, 5= strongly agree

R= responses that required reverse scoring

	%	*1*	*2*	*3*	*4*	*5*
1	The construction of a Russian military base near Niš should be allowed.	29	10.3	21.4	12.6	26.7
2	Russians are our brothers.	24.9	12.6	21.8	18.4	22.2
3	EU leaders do not want a strong Serbia.	11.7	9.8	20.3	16.5	41.8
4	Putin is a tsar.	30.6	10.1	20.5	14.3	24.5
5	Germans have always been our enemies.	21.2	19.7	23.9	15.7	19.5
6	If Serbia needs a military ally, then it should be Russia.	23.4	9.8	20.9	18.4	27.4
7	It's better for Serbia to cooperate more with the East than with the West.	18.4	12.8	34.5	16.5	17.8
8	**R** Serbia should join the EU.	33.6	14.8	13.4	16.5	21.7

Correlation matrix (Pearson's):

	1	2	3	4	5	6	7	8
1	1.00	.697	.435	.705	.451	.686	.628	.400
2	.697	1.00	.475	.775	.491	.747	.638	.406
3	.435	.475	1.00	.451	.406	.496	.430	.457
4	.705	.775	.451	1.00	.446	.736	.650	.431
5	.451	.491	.406	.446	1.00	.538	.446	388
6	.686	.747	.496	.736	.538	1.00	.770	.524
7	.628	.638	.430	.650	.446	.770	1.00	.516
7	.400	.406	.457	.431	.388	.524	.516	1.00

Cronbach's alpha: .905; Mean: .543, Min..388, Max.775; Kaiser-Meyer-Olkin Measure=.911; Bartlett's test of Sphericity (Sig.)=.000

2.4. SERBIAN IDENTITY – POSITIVE/NEGATIVE IDENTIFICATION

In addition, the questionnaire included one battery of statements referring to the positive/negative orientation towards the Serbian identity and the main symbols of Serbian identity. Since the responses for these statements do not have a normal distribution, we used only several of them as independent variables and analyzed them using a nonparametric HI- test.

Table 4. Positive/negative attitudes towards the Serbian identity
1=strongly disagree, 2= partially disagree, 3= neither, 4= partially agree, 5= strongly agree

	%	*1*	*2*	*3*	*4*	*5*
1	The Cyrillic alphabet is obsolete.	75.1	9.6	6.9	4.2	4.2
2	Sometimes I'm ashamed of being from Serbia.	58.4	10.2	6.1	13.2	12.1
3	People in Serbia are primitive and it will take a long time for us to get closer to the European level of culture.	36.3	14.9	13.6	20.7	14.5
4	When I'm abroad I don't like people to know I'm from Serbia.	79.3	8.4	5.2	3.4	3.4

Parametric analyses and χ^2 test

The aim of this part of the analysis was to show how much the attitudes concerning DU (composite variable ADU) were determined by the political orientations/preferences of the respondents (composite variable AEW, AK) and if the attitude on DU was related to the positive/negative Serbian ethnic self-identification.

Multiple regression was applied on three composite variables – ADU (attitudes about the detrimental effects of depleted uranium) as a dependent variable and AEW (the political preferences regarding Eastern/Western countries and the correlation matrix between them) and AK (the political preferences of the respondents regarding the status of Kosovo) as predictors.

Analyses show strong correlations between these three variables:

Table 5. Correlations between composite variables ADU, AK and AEW

		1 ADU	2 AK	3 AEW
1.	ADU (Attitudes about DU)	1.00	.673	.623
2.	AK (Attitudes about Kosovo)	.673	1.00	.768
3.	AEW (Attitudes about Eastern/Western Allies)	.623	.768	1.00

Parson's corr. Sig. 000

Since the correlations between AK and AEW were too high (above 0.700), which implies that these two composite variables measured almost the same thing, they were merged into one variable. The new composite variable (AK/AEW) correlates strongly with the dependent variable AK (0.690). The assumption of normality, multicollinearity and homogeneity of variance was not violated. The regression model explains 47.6% of the variance (R^2=.476; Sig.000), which means that the analyses confirmed a strong influence of the respondents' political preferences on their attitudes about the detrimental effects of DU. This means that we can predict public attitudes on DU by knowing the political preferences concerning the political solution for Kosovo's crises or the preferences for certain political alliances. The fact that somebody strongly supports Kosovo's independence or argues in favor of NATO allies can be interpreted as a predictor of their attitudes about the toxicological and radiological effects of DU.

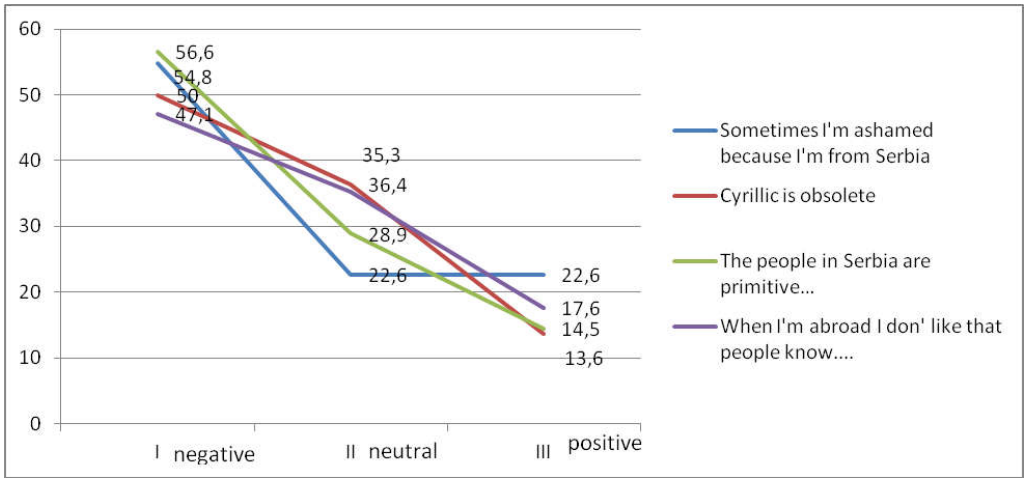
In addition, the interconnection between ADU (attitudes about the detrimental effects of DU) and positive/negative Serbian self-identification was measured using HI-square analyses. The analyses confirm a significant connection ($p < 0.05$). The increase in negative attitudes toward Serbian self-identification is accompanied by a decrease in negative attitudes towards the detrimental effects of DU. The respondents who have negative Serbian self-identification are exactly those who share the attitude that DU is not related to cancer and that its detrimental effects are low. This pattern was confirmed in the comparison of all the measured statements (table 6).

Table 6. Interconnection (Hi-square measurement) between positive/negative attitudes toward the Serbian identity (self-identification) and ADU (attitudes about the detrimental effects of DU)

- = negative

+ = positive

N= neutral



%	-	N	+	χ^2
The Cyrillic alphabet is obsolete.	50	36.4	16.3	χ2=54.99, Sig.000 Cramer's V=.230
Sometimes I'm ashamed because I'm from Serbia.	54.8	22.6	22.6	χ2=45.23, Sig.000 Cramer's V=.209
When I'm abroad I don't like people to know I'm from Serbia.	47.1	35.3	17.6	χ2=24.57 24.57, Sig.002, Cramer's V=.154
People in Serbia are primitive and it will take a long time for us to get closer to the European level of culture.	56.6	28.9	14.5	χ2=47.07, Sig.000, Cramer's V= .213

3. CONCLUSION

In this paper, we have tried to examine some aspects of the public opinion dynamics in the debate on DU weapons. The analyses show a strong influence of the need for social grouping regarding public attitudes about the detrimental effects of DU, which is basically a cognitive issue.

The conclusion of the paper is that the public atmosphere related to the debate on this issue favors the social dynamics of "a psychological crowd", which is a signal of mass culture and society, but not of a democratic, attentive and cognitive media audience, stirring conflicts and increasing "the public fog" in which it will not be possible to present the objective scope of damage and develop beneficial and responsible political strategies.

4. REFERENCES:

Bennet T. (1982). "Theories of Media, Theories of Society". in Gurevitch M.(ed.): Culture, Society and the Media, London: Methuen

Bon Le G.(2005): Psihologija gomile, Beograd: Algoritam

Capstone Deleted Uranium Aerosols. (2004). Report. Pacific Northwest National Laboratory

"Depleted uranium and Canadian Veterans"(2013). Scientific Advisory Committee on Veterans' Health

"Depleted Uranium in Serbia and Monte Negro. Post-conflict Environmental Assessment in the FRY". (2002), Switzerland, UNEP (Unated Nations Environment Programme)

Evert P., Isernia P. (eds.) (2001). Public Opinion and the International Use of Force. London, New York: Routledge

Geertz C. (2005): "Deep Play: Notes on the Balinese Cockfight". Daedalus, Fall 134:4. (pp 56-86)

Ginneken van J. (2003). Collective Behaviour and Public Opinion, Mahwah, New Jersey, London: Lawrence Erlbaum Associates Publ.

Institute of Medicine. (2008). Gulf War and Health. Committee of Gulf War And Health, Washington: The National Academy Press

Laswell H.D. , Blumenstok D. (2006): World Revolutionary Propaganda, San Francisco: Alfred A. Knopf

Liolios Th.E. (1999). "Assessing the risk of the DU used in the operation Allied Forces", Science & Global Security, Volume 8:2, (pp 163-181)

Lippmann W (1922). The Public Opinion, New York: Harcout

Lippmann W.(1993/1925). The Phantom Public, New Brunswick, London: Transaction Publishers

Malignant Effects: Depleted uranium as genotoxin and carcinogen. (2012). ICBUW (International Coalition to Ban Uranium Weapons), Manchester: ICBUW

Moy P., Bosch B. (2013). "Theories of Public Opinion" Sociology Department. Faculty Publications. 244, University of Nebraska- Lincoln

Orlic M. (2000). "Osiromaseni uranijum kao produkt nuklearne tehnologije", XLIV konferencija za ETRAN, Sokobanja 26-29. jun.

Pavlovic R, Pavlovic S., Sipka D., Todorovic D., Paligoric D., Radenkovic M., Djuric J. (2001): "Osiromaseni uranijum u agresiji NATO na FRJ", rad saopsten na seminaru: "Osiromaseni uranijum – istine i zablude", jun, Beograd, Hem.ind. 55:7-8, pp.309-317

Petkovic S., Zaric M., Devic Z. (2001). "Upotreba municije sa osiromasenim uranijumom u agresiji NATO na FRJ". Rad saopsten na seminaru: "Osiromaseni uranijum – istine i zablude", jun, Beograd Hem.ind. 55:7-8, (pp.318-324)

Review of Toxicologic and Radiologic Risks to Military Personnel from Exposure to DU During and After Combat. (2008) National Research Council, http://www.nap.edu/catalog/11979.html , Retrieved on 9/8/2018.

Visser M. (1998). Five Theories of Voting Actions, Twente University Press

Facts on Depleted Uranuim (2001). papers submitted to the conference. Prague. https://inis.iaea.org/collection/NCLCollectionStore/_Public/34/083/34083234.pdf Retrieved on: 9/8/2018

UDK 351.817
https://doi.org/10.18485/fb_ic4hs.2018.6

MASS SURVEILLANCE THROUGH RETAINED METADATA: AN OVERVIEW

Bojan PERKOV[*], Danilo KRIVOKAPIĆ[**], Andrej PETROVSKI[***]

Abstract: Data retention, i.e. collecting bulk data and analysing patterns and anomalies for the entire population under the pretext of national security and fighting crime has been in place for a while in most countries in the world, including Serbia. The research focuses on the mechanisms and practices of accessing retained data by police and government agencies, which brings some transparency and can help understand different aspects and implications of surveillance. Mass surveillance through metadata is one of the most severe threats to privacy. This paper revolves around the issue of accessing retained data through mechanisms that are based on a law, but also on the practices that are in place that do not have a legal basis, i.e. do not include a court order, which is a requirement according to Serbian law. The research methodology has two aspects. The first aspect is the infrastructure, and focuses on the architecture of the ICT network in Serbia. The second aspect is the analytical aspect; it includes an analysis of data regarding the statistics and mechanisms of access to retained data. Data from previous years have shown that state agencies access retained data over 200,000 times every year directly on the servers of one ICT company. Additionally, the difference between the number of requests for retained data that include a court order and independent accesses without one is extremely big. Even though a legal framework exists and the rules of accessing retained data are quite clear, some practices are not in line with the law. Some countries in Europe have set a trend in abolishing data retention altogether as it has proven to be an ineffective manner of fighting crime. This is a positive development and something that should be looked into in the future.

Keywords: data retention, surveillance, privacy, personal data, metadata

[*] MA, SHARE Foundation, Policy Researcher, bojanperkov@sharedefense.org
[**] LL.B., SHARE Foundation, Director, danilo@sharedefense.org
[***] MSc, SHARE Foundation, Director of Tech, a.petrovski@sharedefense.org

1. DATA RETENTION - "COLLECT IT ALL NOW, ACCESS LATER"

In the past 20 years, many aspects of law enforcement have been shifting towards data collection and analysis, not just because of the rise of cybercrime, but also because data are a reliable proof in investigations for all types of criminal activity. Increasing challenges for national security, such as international terrorism, have influenced the introduction of measures such as the mass collection and retention of data on electronic communications of citizens – their emails, phone calls, instant messages, text messages and so on. This so-called "metadata", i.e. data describing communication data, includes information such as the date and time when the communication took place, the duration of this communication, data on the sender, data on the recipient, location data, IP addresses, phone numbers, email addresses and other personal data. In the digital era, you do not need the content of communication to investigate a person's activities, map their daily movement and routines or their social circles and connections. When collected, processed and analysed on a mass scale, these data sets represent a treasure for anyone aiming for uncontrolled mass surveillance of the population. Having all this in mind, "the future-orientation increasingly severs surveillance from history and memory and the quest for pattern-discovery is used to justify unprecedented access to data" (Lyon, 2014: 1).

The first decade of the 21st century was marked by terrorist acts which shook the foundations of Western democracies and instigated governments to rethink their approach to surveillance and communications interception. The United States of America, targeted in September 2001, passed the USA PATRIOT Act ("Patriot Act") soon after the attacks on the World Trade Center in New York City. It gave government agencies and law enforcement unprecedented surveillance powers which significantly reduced the U.S. citizens' right to privacy. Even after the sweeping surveillance revelations by former National Security Agency (NSA) contractor Edward Snowden in 2013, USA FREEDOM Act reforms and many other controversies over the years (Tummarello, 2016), the Patriot Act still stands strong and will almost certainly reach "adulthood" in 2019.

The European Union (EU) took a similar path as the U.S., and after terrorist attacks in Madrid and London in 2004 and 2005 respectively, the EU Data Retention Directive 2006/24/EC was adopted. As early as 2006, the Directive imposed a mandatory communications data retention regime for operators of electronic communications, such as internet service providers or telecommunication services providers, with the duration for keeping the data between six months and two years, depending on how a Member State implemented the Directive. However, in 2014, the Court of Justice of the European Union (CJEU) ruled that the Data Retention Directive was invalid since it seriously undermined the right to privacy and the right to personal data protection of EU citizens in its landmark judgement in joined cases *Digital Rights Ireland* and *Seitlinger and Others* (Back to the Drawing Board: Data Retention Directive Declared Invalid, SHARE Foundation, 2014). This was an important first step towards better protection of citizens' privacy in the EU, but more challenges for the complete abolishment of data retention remained.

After the ruling, it was not exactly clear what this invalidation meant from a legal perspective, or how it would be implemented on the Member State level and what the next steps regarding data retention in the EU were. The CJEU therefore had to issue another,

more detailed judgement in late 2016. The joined cases were *Tele2 Sverige AB v. Swedish Post and Telecom Authority* and *Secretary of State for the Home Department v. Tom Watson and Others,* and the Court's opinion was that EU Member States cannot impose a general regime of communications data retention on providers of electronic communications services (The Member States may not impose a general obligation to retain data on providers of electronic communications services, Court of Justice of the European Union, 2016). The CJEU reasoning was that the "legislation prescribing general and indiscriminate retention of data does not require there to be any relationship between the data which must be retained and a threat to public security" (The Member States may not impose a general obligation to retain data on providers of electronic communications services, Court of Justice of the European Union, 2016: 2) and it "therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society" (The Member States may not impose a general obligation to retain data on providers of electronic communications services, Court of Justice of the European Union, 2016: 2).

However, even in spite of the second landmark CJEU judgement on practically the same matter, data retention still haunts EU citizens. In June 2018, a group of more than sixty NGOs, community networks, academics and activists sent an open letter to the European Commission, explaining that blanket data retention, still in practice in 17 EU Member States, is not in accordance with EU law and asking for change (Massive claims against unlawful data retention, Stop Data Retention, 2018). Since the EU has adopted a new set of data protection rules, i.e. the General Data Protection Regulation (GDPR) and the Law Enforcement Directive, they are expected to bring important changes to the way EU citizens enjoy their rights to privacy and personal data protection and how their data are used for law enforcement purposes.

2. CURRENT STATE OF DATA RETENTION IN SERBIA

In 2017, 68 per cent of households in Serbia had an internet connection (Usage of Information and Communication Technologies in the Republic of Serbia in 2017, Statistical Office of the Republic of Serbia, 2017: 14), whereas 53 per cent of households had access to the Internet via mobile phones or tablets using the 3G network – a large increase from 18 per cent in 2015 (Usage of Information and Communication Technologies in the Republic of Serbia in 2017, Statistical Office of the Republic of Serbia, 2017: 17). Also, it is estimated that almost five million people in Serbia use a mobile phone (Usage of Information and Communication Technologies in the Republic of Serbia in 2017, Statistical Office of the Republic of Serbia, 2017: 22). Tablets, smartphones and other devices that keep us constantly connected have become an essential part of our everyday lives, but have also caused us to produce more data about ourselves and our habits than ever before.

In the Republic of Serbia, mandatory data retention for all electronic communications for the duration of 12 months from the date of communication is prescribed in the Law on Electronic Communications, which was adopted in 2010 and most recently amended in 2014. However, the legal framework was not harmonized, since laws on security services

had loopholes which enabled access to citizens' data and communications without a court order. In 2012, provisions of the law regulating the work of Serbia's military agencies, which granted the Military Security Agency (MSA) (Vojnobezbednosna agencija, VBA) powers to access citizens' data from telecom operators, were declared unconstitutional. A year later, three provisions of the Law on Security Information Agency (SIA) (Bezbednosno-informativna agencija, BIA), the Serbian secret service focused on civilian matters, were also struck down by the Constitutional Court of Serbia (Ustavni sud RS). Finally, in June 2013, provisions of the Law on Electronic Communications which ignored the constitutional guarantees of communications secrecy by enabling access to retained data without a court order were deemed unconstitutional, forcing the adoption of amendments to the Law (Communications Data Retention in Serbia: How much are we being surveilled? (2014-2016), SHARE Foundation, 2017).

As a mechanism of transparency and control of access to citizens' retained communications data, Article 130a of the Law on Electronic Communications prescribes that all operators of electronic communications in Serbia and state bodies authorised to access retained data submit annual *records on access to retained data* to the Commissioner for Information of Public Importance and Personal Data Protection of the Republic of Serbia (Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti RS) (Law on Electronic Communications, 2014). These records are a foundation for researching the data retention practices of operators and access to the data by state authorities. SHARE Foundation, an expert think-tank from Serbia focused on advocacy and research at the intersection of human rights, technology and law, obtained these records using a freedom of information request for four consecutive years, from 2014 to 2017, and will continue with this yearly practice.

It is important to note that these records only contain statistical data (number of received requests for access to data, number of granted requests, dates, authority which submitted the request etc.), the publication of which cannot endanger the national security of Serbia or criminal investigations. Also, publishing these statistics is important for the public oversight, transparency and accountability of state authorities carrying out surveillance and is therefore in the public interest. The European Court of Human Rights (ECtHR) affirmed the public's right to know when it comes to statistical data on surveillance, i.e. the number of people in Serbia placed under electronic surveillance by the Security Information Agency during one year (Youth Initiative for Human Rights v. Serbia, European Court of Human Rights, 2013).

On a practical level, state authorities access retained communications data in two ways: through submitting requests to the operators (by email, fax, phone or in person) and by directly accessing the operators' information systems through dedicated applications. While the first way has a legal basis and offers more protection to citizens' rights to privacy and protection of their personal data, independent (direct) access is a highly controversial measure of very dubious legality, which makes arbitrary access to citizens' data possible.

Analysis of mobile network data surveillance by SHARE Foundation (Invisible Infrastructures: Surveillance Architecture, SHARE Foundation, 2015), based on the

documents obtained from the Commissioner for Information of Public Importance and Personal Data Protection, has shown that between March 2011 and March 2012, i.e. during one year, the Ministry of Interior, VBA[1] and BIA[2] independently accessed Telenor's database more than 270,000 times (Proceedings of oversight of implementation of the Law on Personal Data Protection by Telenor, Commissioner for Information of Public Importance and Personal Data Protection, 2012: 16). Data on Telenor from more recent years show that this practice has continued, showing that retained data were accessed independently slightly more than 200,000 times, almost exclusively by the Ministry of Interior. In 2015 and 2016, the numbers were even higher – around 300,000 for each year. Telenor, the second largest mobile operator in Serbia, is the only one which registers instances of direct access to retained data made by the competent authorities in addition to the requests received through the regular procedure – or is the only one reporting the statistics on direct access. Given the scope of direct access, it seems logical to assume that the practice of direct access by competent authorities exists with other operators, but that they either do not record these approaches or do not want to report them to the Commissioner. We confirmed this conclusion in the report of the Military Security Agency, which states that "access to retained electronic communications data is obtained through VIP, Telenor, MTS and Telekom's access applications" (Communications Data Retention in Serbia: How much are we being surveilled? (2014-2016), SHARE Foundation, 2017). According to data obtained from the Commissioner for 2017, Telenor remains the only operator which provides information about independent access in their report, recording 381,758 instances of direct access to retained communications data.

When we take into account the market share of mobile operators in Serbia for the second quarter of 2018, Telekom Serbia as the largest operator covered 45.4% of users, Telenor 31.3%, VIP 23.2% and virtual mobile operators had 0.1% of the market share (An overview of the electronic communications market in the Republic of Serbia - the second quarter of 2018, Regulatory Agency for Electronic Communications and Postal Services, 2018: 8). If we make a realistic assumption that there was a similar number of direct access instances in the cases of Telekom Serbia and VIP to those of Telenor, the total number of direct access instances in Serbia could be estimated at one million.

3. FUTURE OF DATA RETENTION IN SERBIA

For some time now, there are intentions to adopt a new Law on Electronic Communications and in late 2016 the Ministry of Trade, Tourism and Telecommunications presented a draft of the new law. The draft practically confirmed that the provisions of the current Law on Electronic Communications related to the secrecy of electronic communications, legal interception of communications and retention of metadata will continue to apply even after the adoption of a new law until there is a separate law regulating these issues. This means that the lawmakers have decided not to change the legal framework at this time, but a completely new law opens the possibility

[1] Military Security Agency

[2] Security Information Agency

for better adjustment to EU standards on the one hand, and carries the risk of further reducing citizens' right to privacy on the other. The draft law envisaged the mandatory registration of electronic communications subscribers, which is a highly controversial measure as it could also include user registration of prepaid SIM cards, which the current law does not prescribe (Communications Data Retention in Serbia: How much are we being surveilled? (2014-2016), SHARE Foundation, 2017).

As the new Law on Electronic Communications is expected, data retention in its current form needs to be considered, especially in the wake of new developments in the EU, where some Member States are still quite reluctant to completely give up on their data retention policies. The "collect and store all data by default" approach to data retention will certainly need to be changed, since it is a very intrusive measure for the privacy and secrecy of citizens' communications, employed without adequate transparency and safeguards.

4. REFERENCES

Commissioner for Information of Public Importance and Personal Data Protection. (2012). Proceedings of oversight of implementation of the Law on Personal Data Protection by Telenor. Retrieved July 2, 2018, from https://labs.rs/Documents/ZapisnikTelenor.pdf

Court of Justice of the European Union. (2016). The Member States may not impose a general obligation to retain data on providers of electronic communications services. Retrieved June 25, 2018, from https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf

European Court of Human Rights. (2013). Youth Initiative for Human Rights v. Serbia, App. no. 48135/06. Retrieved June 28, 2018, from http://hudoc.echr.coe.int/eng?i=001-120955

Law on Electronic Communications. (2014). Official Gazzette of the Republic of Serbia, 44/2010, 60/2013 - Constitutional Court judgement and 62/2014. Retrieved June 28, 2018, from https://www.paragraf.rs/propisi/zakon_o_elektronskim_komunikacijama.html

Lyon, D., (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big

Data & Society, 1(2), 1-13. https://doi.org/10.1177/2053951714541861

Regulatory Agency for Electronic Communications and Postal Services. (2018). An overview of the electronic communications market in the Republic of Serbia - the second quarter of 2018. Retrieved September 21, 2018, from https://www.ratel.rs/uploads/documents/empire_plugin/Q2%202018%20ENG.pdf

SHARE Foundation. (2017). Communications Data Retention in Serbia: How much are we being surveilled? (2014-2016). Retrieved June 28, 2018, from https://labs.rs/sr/zadrzavanje-podataka-o-komunikaciji-u-srbiji/

SHARE Foundation. (2015). Invisible Infrastructures: Surveillance Architecture. Retrieved July 2, 2018, from https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/

SHARE Foundation. (2014). Back to the Drawing Board: Data Retention Directive declared invalid. Retrieved June 25, 2018, from http://www.shareconference.net/sh/defense/back-drawing-board-direktiva-o-zadrzavanju-podataka-nevazeca

Statistical Office of the Republic of Serbia. (2017). Usage of Information and Communication Technologies in Republic of Serbia in 2017. Retrieved September 20, 2018, from http://publikacije.stat.gov.rs/G2017/PdfE/G20176006.pdf

Stop Data Retention. (2018). Massive claims against unlawful data retention. Retrieved June 27, 2018, from http://stopdataretention.eu/

Tummarello, K., (2016). Debunking the Patriot Act as It Turns 15. Retrieved June 25, 2018, from https://www.eff.org/deeplinks/2016/10/debunking-patriot-act-it-turns-15

UDK 351.817:343.1
https://doi.org/10.18485/fb_ic4hs.2018.7

INTERCEPTION OF ENCRYPTED TELECOMMUNICATION AND THE SO-CALLED ONLINE SEARCH OF IT SYSTEMS FOR THE PURPOSE OF CRIMINAL PROSECUTION

Jan Dirk ROGGENKAMP*

Abstract: In 2008, Germany's Federal Constitutional Court ("FCC") rejected North Rhine-Westphalia's Constitutional Protection Act, which allowed the so-called online search of computers and other IT systems and the interception of encrypted telecommunication at the source[1]. The FCC stated that the society has a legitimate interest in the confidentiality and integrity of the IT systems protected by the constitution. In their view, the general right of personality encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems. However, with regard to preventive measures, the FCC deemed the measures acceptable within strictly defined limits. The secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read is – according to the FCC – constitutionally only permissible if factual indications exist of a concrete danger to a predominantly important legal interest[2]. Whether or not the disputed measures may be permissible for the purpose of criminal prosecution, has been discussed ever since. In August 2017, an amendment to the German Code of Criminal Procedure was adopted. This allows the law enforcement authorities to secretly monitor encrypted telecommunications and to conduct so-called online searches of information technology systems (e.g. personal computers, smartphones, etc.). This extension of state powers raises strong constitutional concerns both with regard to human dignity and the so-called right to integrity and confidentiality of information technology systems. In addition to that, the new measures pose a threat to national (and international) IT security.

Keywords: online search, lawful interception, interception of encrypted telecommunication, criminal prosecution

---

* Professor, PhD, Berlin School of Economics and Law, jan.roggenkamp@hwr-berlin.de

[1] Also called ″source telecommunication surveillance″ as opposed to general telecommunications surveillance, because it allows to access data at the source prior to encryption via a special software which has to be secretly installed on the target computer or smartphone.

[2] Predominantly important are the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence.

1. BASELINE INFORMATION

In Germany it has been discussed for several years whether or not, and if so, and under which preconditions law enforcement agencies should be able to conduct a so-called online search of information technology systems and / or conduct a so-called source telecommunications surveillance (Jahn and Kudlich, 2007; Roggenkamp and Braun, 2011; Roggan, 2017). Both measures are to accommodate the difficulties in criminal investigations emerging if the targeted individuals use information technology, especially encryption techniques.

1.1. "ONLINE SEARCH"

In order to secretly (!) retrieve information stored on an information technology system (e.g. a computer, a smartphone, a tablet - hereafter "**Information Technology System**" or "**Target System**") the investigating law enforcement agency has to gain access to the system without the user (the target) noticing (Buermeyer, 2007:160). This is usually done by infiltrating into the Target System by taking advantage of its security loopholes (also called software vulnerabilities) and installing a spy program (so-called *"***Trojan Software***"*) (Buermeyer 2007: 163; Soiné, 2018:501; Pohlmann and Riedel, 2018:37). Using such Trojan Software makes it possible to monitor the use of the Target System, in order to view the data on the storage media and extract it, and/or to control the Information Technology System remotely (Freiling, Safferling and Rückert, 2018:16). This measure is called *"Online-Durchsuchung"* in Germany, which literally translates as "**Online Search**" (and is not to be confused with a mere search for information on the Internet via search engines and the like).

1.2. SOURCE TELECOMMUNICATION SURVEILLANCE

The so-called source telecommunication surveillance ("**STS**") is a special method of telecommunications surveillance, which is used to access and extract telecommunications data (e.g. speech, messages) at the source of communication (e.g. a smartphone or laptop). It is thus deemed necessary to intercept potentially encrypted telecommunication e.g. via messenger apps such as WhatsApp or Telegram before it is being encrypted, or after it has been decrypted (Roggenkamp and Braun, 2011:681). As with Online Searches, it is necessary to infiltrate into the Target System and implement Trojan Software that (clandestinely) extracts the relevant telecommunications data and submits it to the law enforcement agency (Buermeyer and Bäcker, 2009:434).

1.3. THE "ONLINE SEARCH JUDGEMENT" BY THE GERMAN FEDERAL CONSTITUTIONAL COURT

In 2008, Germany's Federal Constitutional Court (*"***FCC***"*) rejected North Rhine-Westphalia's Constitutional Protection Act (North Rhine-Westphalia Constitutional Protection Act, 2006), which empowered the constitution protection authority of the federal state of North Rhine-Westphalia to conduct Online Searches and STS for preventive purposes (FCC 2008).

The FCC stated that the society has a legitimate interest in the confidentiality and integrity of the Information Technology Systems protected by the German constitution (i.e. the *Grundgesetz* – "**German Basic Law**"). In their view the general right of personality encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems (FCC 2008: Headnote 1).

However, the FCC deemed such measures, if conducted with a preventive objective, acceptable within strictly defined limits. The secret infiltration of an Information Technology System by means of which the use of the system can be monitored and its storage media can be read is – according to the FCC – constitutionally (only) permissible if factual indications exist of a concrete danger to a *"predominantly important legal interest*". Predominantly important legal interests are defined as *"the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence"*.

Furthermore, the FCC held that insofar as empowerment of the investigating authority is restricted to a state measure by means of which the contents and circumstances of on-going telecommunication are collected in the computer network, or the data related thereto is evaluated, the encroachment is to be measured against the right to privacy of telecommunications (German Basic Law: Article 10.1) alone.

1.4. PERMISSIBILITY FOR PURPOSE OF CRIMINAL PROSECUTION

Whether or not these measures may be permissible for the purpose of criminal prosecution has been discussed ever since. In August 2017, an amendment of the German Criminal Code of Procedure (*"***CCP***"*) entered into force expanding the powers of law enforcement agencies to conduct Online Searches and intercept encrypted telecommunication via STS. In August 2018, a constitutional complaint against the aforementioned amendment has been filed with the FCC deeming it unconstitutional (Martin, 2018).[3]

2. INFRINGEMENT OF HUMAN DIGNITY?

2.1. INTRUSION OF PRIVACY

Both measures, Online Searches and STS, enable law enforcement agencies to secretly intrude into the privacy of a person and collect all-encompassing intimate information about this person. The amount of private information, which may be gathered, is unparalleled in comparison to other measures such as house searches (Roggan, 2017).

Smartphones in particular, but also other Information Technology Systems, have become constant and personal companions to their users (Proner, 2015). They "know" every location the user visits or has visited, they *"*know*"* the users likes and dislikes. Information Technology Systems are used to share and discuss political, religious or social topics – sometimes highly personal. Users "confer" with search engines before a new car is bought, but also in case of illness or relationship problems. The search for a life partner is assisted by so-called apps, as is the search for the current cinema or theatre programme. Holiday

[3] Disclosure: the author of this article is one of the legal representatives of the plaintiffs.

pictures, pictures of kids or erotic "selfies" are shared via messenger services. If a smartphone, which is connected to the Internet, is being surveilled, it is actually a surveillance of the inner world of ideas, emotions and common behaviour (Roggan, 2017:817). It is possible to generate a personality profile, which could not be more detailed.

2.2. HUMAN DIGNITY

The inviolable fundamental right to human dignity is not only the foundation of the right to privacy (Floridi, 2016:307), but directly protects the so-called core area of private life of every human being (pro omnibus Papier, 2017:3028).

According to the FCC, secret surveillance measures carried out by state agencies must absolutely respect this inviolable area. Even overriding interests of the public cannot justify encroachment on it. The FCC states that the development of the personality in the core area of private life includes the possibility to express inner events such as perceptions and feelings, as well as considerations, views and experiences of a highly personal nature, without fear that state agencies may have access to them (FCC 2008: Para 271).

With regard to the aforementioned (B. 1.) use of smartphones etc., it is the view expressed here that the secret surveillance of a personal Information Technology System is a disrespect for the inviolable core area of private life and, thus, unconstitutional. The secret investigation of a person's world of thought that goes hand in hand with the measures discussed here is, in the view held here, an unjustifiable violation of human dignity.

3. INFRINGEMENT OF RIGHT TO CONFIDENTIALITY AND INTEGRITY OF INFORMATION TECHNOLOGY SYSTEMS?

However, the FCC held in 2008 that an Online Search is "only" to be seen as an encroachment on *"the general right of personality in its particular manifestation as a fundamental right to the guarantee of the confidentiality and integrity of information technology systems"* (FCC, 2008: Para 166).

3.1. PREDOMINANTLY IMPORTANT LEGAL INTERESTS

The FCC stated that such an encroachment may (only) be provided for *"if the empowerment to encroach makes it contingent on the existence of factual indications of a concrete danger to a predominantly important legal interest"*.

With regard to measures, which serve the purpose of criminal prosecution, it is unclear if and how this requirement can be transposed. Criminal investigations and prosecutions do not aim at averting *"concrete dangers to predominantly important legal interest"* but serve mainly to enforce the State's right to inflict punishment if a crime has been committed. Whether this is a *"predominantly important legal interest"* in itself is to be doubted. A constructive approach asks whether the crime, which is investigated, is actually a realisation of a danger to the aforementioned *"predominantly important legal interest"* and if an Online Search may have been conducted in order to prevent the realisation, had the danger been known in time. Hence, the investigation of a murder or a hostage taking may be carried out via online search but not crimes such as corruption, theft, receiving and handling, drug dealing, etc.

The new regulation of the CCP from 2017 (see A. 4.) does not comply with these requirements. Online Searches are only to be permitted in cases where there is a "particularly serious crime". However, offences such as money laundering, commercial receiving of stolen goods or bribery are also considered to be "particularly serious" under the new provisions of the CCP (see Sect. 100b Para 2 CCP), which is too broad to meet the aforementioned requirements. Moreover, the new CCP merely requires that "certain facts give rise to suspicion" that the target person is the perpetrator or participant in a "particularly serious crime". In order to do justice to the seriousness of the encroachment, however, higher demands must be made than just a simple initial suspicion.

3.2. SUITABLE STATUTORY PRECAUTIONS

Furthermore, according to the FCC (FCC, 2008: Para 257), the empowerment to effect secret access to Information Technology Systems *"must be linked with suitable statutory precautions in order to secure the interests of the person concerned under procedural law. If a norm provides for secret investigation activities on the part of the state which – as here – affect particularly protected zones of privacy or demonstrate a particularly high intensity of encroachment, the weight of the encroachment on fundamental rights is to be accounted for by suitable procedural precautions"*.

a. Reservation of judicial order

With regard to this, the FCC holds that secret access to an Information Technology System is in principle (the exception being imminent danger) to be placed under the reservation of a judicial order in order to protect the concerned individual from unlawful use of the measure.

The new CCP (Sect. 100e Para 2 CCP) fulfils this requirement by demanding not only a judicial order by a single judge, but by a chamber of the district court (*Landgericht*).

b. Protection of core area of private life

In addition to that, adequate statutory precautions to avoid encroachments on the absolutely protected core area of private life have to be provided (FCC, 2008, Para 270).

The FCC acknowledges, *"In the context of secret access to an information technology system, the danger exists that the state agency might collect personal data which is to be attributed to the core area. For instance, the person concerned may use the system to establish and store files with highly personal contents, such as diary-like records or private film or sound documents. Such files can enjoy absolute protection, as can for instance written embodiments of highly personal experiences [...]. Secondly, insofar as it is used for telecommunication purposes, the system can be used to transmit contents, which can equally fall within the core area. This applies not only to speech telephony, but for instance also to telecommunication using e-mails or other Internet communication services [...]. The absolutely protected data can be collected with different types of access, such as with the inspection of storage media, just as with the surveillance of on-going Internet communication or indeed with full surveillance of the use of the target system."* (FCC, 2008: Para 272)

However, although the FCC does not hold that such secret access to highly personal contents is a violation of human dignity in itself, it deems that it is necessary to provide statutory precautions to protect the core area of private life. These precautions have to be provided on two levels, these being (1) the collection of information and (2) the evaluation of information collected. The FCC holds that a statutory empowerment must ensure *"as far as possible"* that no data is collected which relates to the core area (FCC, 2008: Para 277).

At first glance at the new CCP, the legislator seems to fulfil this requirement by stating that the law enforcement agency conducting an Online Search has to apply technical means to ensure ″as far as possible″ that information relating to the core area of private life is not being collected (cf. Sect. 100e Para 3 CCP). A closer look shows, however, that the provision is inadequate as there are no technical means (at least not yet) to comply with this statutory ″precaution″. In order to avoid the collection of information, which is of a highly personal nature, the only viable approach is a ″risk evaluation″ with regard to the Target System. Such a risk evaluation is undertaken under German law in cases where a house or a flat is monitored acoustically (Sect. 100c CCP). In these cases the law enforcement agency has to – by law – evaluate whether it is to be expected that discussions/events in the particular room will be of a highly personal nature. If this is the case (e.g. bedroom of a couple), the monitoring of this room is not allowed (cf. Sect. 100e Para 4 CCP). A similar approach is – according to the view expressed here – possible (and necessary) with regard to Information Technology Systems. It has to be evaluated whether it is to be expected that the Target System will be used for highly personal purpose (e.g. personal smartphone). If this is the case, the law enforcement agency must refrain from conducting a (secret) Online Search.

3.3. PROTECTION OF DATA AND IT SECURITY

In order to guarantee sufficient protection for the integrity of the Target System, it is the view expressed here that it must be stipulated by law that the Trojan Software used is examined by at least one independent body (e.g. the Federal Data Protection Authority) for compatibility with data protection law before use. This is the only way to avoid third parties also having access to the mobile phones and laptops of the monitored users through unknown back doors or – in the worst case – a data breach (Roggenkamp, 2018:610).

In addition, it must be stipulated by law that the state may not exploit unknown security gaps (so-called zero day exploits) in order to install the software. In the view of the complainants of four constitutional complaints currently pending[4], this must be prohibited – as must the procurement and "storage" of such "exploits" – in order to guarantee national (and international) IT security (Pohlmann and Riedel 2018:37). Incidents such as the "WannaCry" infection of millions of computers all over the world, allegedly caused by an "exploit" lost by the NSA (Patrizio, 2017), must not be repeated.

With regard to both Online Searches and STS, the new regulation of the CCP is incompatible with data and IT security.

[4] Only one of the complaints has been published so far: https://freiheitsrechte.org/home/wp-content/uploads/2018/08/GFF_Verfassungsbeschwerde_Staatstrojaner_anonym.pdf.

4. CONCLUSION

According to the view expressed here, it is preferable to regard online searches and STS as unconstitutional and unjustifiable encroachments on human dignity and to refrain from corresponding measures. If one sees this differently, as does the FCC, then, however, sophisticated legal precautions must be taken to protect the personal rights of the persons concerned and general IT security. The regulations in the new German CCP do not meet these requirements.[5]

5. BIBLIOGRAPHY

Buermeyer, U. (2007). Die "Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme [The "online search". Technical background of covert sovereign access to computer systems]. *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht* [Online journal for highest court rulings on criminal law] (HRRS), [online] 2007(4), pp.154 - 166. Available at: https://www.hrr-strafrecht.de/ .

Buermeyer, U. and Bäcker, M. (2009). Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO [On the illegality of source telecommunications surveillance on the basis of Sect. 100a CCP]. *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht* [Online journal for highest court rulings on criminal law](HRRS), [online] 2009(10), pp. 433 - 441. Available at: https://www.hrr-strafrecht.de/.

Federal Constitutional Court of Germany (2008). Judgment of the First Senate of 27 February 2008 - Ref. 1 BvR 370/07. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html.

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy and Technology*, 29(4), pp. 307 - 312.

Freiling, F., Safferling, C. and Rückert, C. (2018). Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen [Source telecommunication surveillance and online search as new measures for law enforcement: Legal and technical challenges]. *Juristische Rundschau* [Legal review] (JR), 2018(1), pp. 9 - 23.

Gesetz über den Verfassungsschutz in Nordrhein-Westfalen [North Rhine-Westphalia Constitution Protection Act (2006)] in the version of the Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen [Act Amending the Act on the Protection of the Constitution in North Rhine-Westphalia] of 20.12.2006. *Law and Ordinance Gazette of North Rhine-Westphalia* (GVBl NW) 2006, p. 620).

Grundgesetz für die Bundesrepublik Deutschland (GG) [Basic Law for the Federal Republic of Germany (1949) - (German Basic Law)], 23.5.1949, with subsequent

[5] Four constitutional complaints were lodged with the FCC against the new regulation. However, a decision is not expected for a few years.

amendments. Available at https://www.gesetze-im-internet.de/englisch_gg/index.html.

Jahn, M. and Kudlich, H. (2007). Die strafprozessuale Zulässigkeit der Online-Durchsuchung [The admissibility of online searches in criminal procedural law]. *Juristische Rundschau* [Legal review] (JR), 2007(2), pp. 57-61.

Martin, D. (2018). Germany's government hackers face Constitutional Court. *Deutsche Welle News* (07.08.2018). Available at https://www.dw.com/en/germanys-government-hackers-face-constitutional-court/a-44988326.

Papier, H. (2017). Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft [Rule of law and protection of fundamental rights in the digital society]. *Neue Juristische Wochenschrift* [New Legal Weekly] (NJW), *70*, 42, 3025 - 3031.

Patrizio, A. (2017). Microsoft to NSA: WannaCry is your fault. [online] *Network World*. Available at: https://www.networkworld.com/article/3196222/security/microsoft-to-nsa-wannacry-is-your-fault.html.

Pohlmann, N. and Riedel, R. (2018). Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen [Criminal prosecution must not compromise IT security on the Internet]. *Datenschutz und Datensicherheit* [Data Protection and Data Security] (DuD), 42(1), pp.37 - 44.

Proner, P. (2015). The Extended Self – Die Bedeutung von Smartphones für Nutzer und Konsumenten [The Importance of Smartphones for Users and Consumers]. [online] *Think with Google*. Available at: https://www.thinkwithgoogle.com/intl/de-de/insights/kundeneinblicke/the-extended-self-die-bedeutung-von-smartphones-fur-nutzer-und-konsumenten/.

Roggan, F. (2017). Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit [The criminal procedural source telecommunication surveillance and online search: Electronic surveillance measures with risks for accused persons and the general public]. *Strafverteidiger* [Defence Counsel] (StV), 37(12), p. 821.

Roggenkamp, J. and Braun, F. (2011). Ozapftis - (Un)Zulässigkeit von "Staatstrojanern" [Ozapftis - (In)permissibility of "State Trojans"] *Kommunikation und Recht* [Communcation and Law] (K&R), 2011(11), pp.681-686.

Roggenkamp, J. (2018). *Handbuch europäisches und deutsches Datenschutzrecht* - § 21 - Datenschutz und präventive Tätigkeit der Polizei [European and German data protection law handbook - § 21 - Data protection and preventive police work]. Munich: C.H. Beck / Specht, L. and Mantz, R. (Editors), pp.599 - 622.

Soiné, M. (2018). Die strafprozessuale Online-Durchsuchung [The criminal procedural online-search]. *Neue Zeitschrift für Strafrecht* [New Journal for Criminal Law] (NStZ), 38(9), pp.497 - 504.

Strafprozessordnung (StPO) [Criminal Code of Procedure - (CCP)], 1.2.1877 in the version published on 7 April 1987. *Bundesgesetzblatt* [Federal Law Gazette] Part I p. 1074, 1319), with subsequent amendments. Available at: https://www.gesetze-im-internet.de/stpo/.

UDK 004.056(497.11)
https://doi.org/10.18485/fb_ic4hs.2018.8

IMPACT ANALYSIS OF THE APPLICATION OF THE GDPR REGULATION ON THE FUNCTIONING OF THE INFORMATION AND COMMUNICATION SYSTEM OF THE MOI OF THE REPUBLIC OF SERBIA

Milan GLIGORIJEVIĆ[*], Radosav POPOVIĆ[**], Aleksandar MAKSIMOVIĆ[***]

Abstract: The development of new information and communication technologies brings undoubted benefits to society, as their use allows for a significant reduction in costs, business processes are automated, facilitated and accelerated, various types and amounts of information become available, and communication opportunities are expanding considerably. Simultaneously with the development of new technologies, threats to their security are growing globally, and hence great attention is paid to their adequate protection. The Republic of Serbia has also realized the importance and seriousness of this issue, and has been working very hard to create a sustainable information society in recent times. Coordination needs to be improved, not only at the national, but also at the international level, bearing in mind that many incidents in ICT systems have a cross-border character. Except in certain areas where there are special regulations (protection of classified information, personal data, electronic communications, etc.), there is no obligation to determine the measures that are necessary to take in order to protect the ICT system. Public authorities, persons dealing with particularly sensitive personal data and legal persons performing activities of general interest must increase their resistance to compromising information security, since the tasks that are of great importance and their smooth functioning are increasingly dependent on new technologies. Infringement of information security could cause major disruptions in vital functions and cause significant damage to the state and its citizens. One such system is also the information and communication system of the Ministry of Interior of the Republic of Serbia, which has recently faced a great challenge: How to implement the obligations and responsibilities prescribed by the new GDPR regulations, and on the other hand to provide the same or higher level of protection of the system itself?

[*] Assistant Professor, PhD, Academy of Criminalistic and Police Studies, Belgrade, milan.gligorijevic@mup.gov.rs

[**] MoI of the Republic of Serbia, Deputy Head of the Sector for Analytics, Telecommunications and Information Technologies, Belgrade, radosav.popovic@mup.gov.rs

[***] MoI of the Republic of Serbia, Head Specialist, Legal expert for network and information security, CERT Centre, Belgrade, aleksandar.maksimovic@mup.gov.rs

Keywords: information security, information and communication system, GDPR regulation, protection of classified information, personal data protection

1. INTRODUCTION

In the modern era the right to privacy is increasingly enshrined in constitutional and human rights instruments, and, in some cases, a specific right to the protection of personal data is also included. At the same time, privacy and personal data protection are often challenged in the digital era, due in particular to the worldwide proliferation of internet-based communications that are notoriously difficult to police; the rise of data-hungry applications like search engines, targeted advertising platforms or social networks; and the use of various methods of online surveillance by both private and governmental entities. (Lehavi, Larouche, Accetto, Purtova & Yemer, 2016) The alleged borderless nature of digital technology leads to a complicated set of normative and policy questions. These queries relate not only to the adequate scope of substantive balancing between the individual interest in privacy and the potential interest of other private users, commercial entities, and governments in data disclosure, but also to questions of jurisdiction and governance. The dilemma is thus not only one of *how* (or *how far*) privacy and personal data should be protected, but also one of *who* should be in charge of establishing and enforcing the governing legal norms.

In order to meet all these requirements, the European Union drafted GDPR regulation act in 2016. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). (Blackmer, 2016) New EU data protection regime extends the scope of the European Union data protection laws to all foreign companies processing EU citizens' data. This Regulation provides for the harmonization of data protection rules across the EU, which defines that non-European companies, if they have any personal data on EU citizens in any way, must comply with these regulations.

2. THE MOST IMPORTANT CHANGES INTRODUCED BY THE GDPR REGULATION

The GDPR regulations came into force on 25 May 2018, with the aim of replacing the 1995 Data Protection Directive (Directive 95/46/EC). While Directive 95/46 was in force, EU members adopted local regulations and therefore the laws on the protection of personal data across the EU were not harmonized. By adopting the GDPR, a single legal instrument with direct application has been created in all 28 Member States, and wider, replacing all the different ways in which the previous Directive was implemented. In addition, GDPR also takes into account new technologies that are not covered by the Directive, such as Big Data, mobile applications, social networks, etc. (Babel, 2017)

GDPR introduces new and more comprehensive rules regarding the use and protection of personal data, and the mere fact that penalties for non-compliance with these regulations

reach up to €20 million, or 4% of annual turnover, speaks about the necessity for timely harmonization of business operations with the new regulations.

Figure 1. Important points of GDPR regulation

Some of the key novelties that the GDPR regulation introduces are:

• Citizens' rights

One of the basic ideas for guiding the adoption of GDPR was that citizens can resume control over their data. Thus, companies in possession of personal data, are obliged to inform their users about the ways in which their data is used, to enable them to inspect data, provide copies, or modify incorrect data. One of the novelties is the so-called 'right to be forgotten' (Mantelero, 2013) which means that the existing right to delete data adapts to the reality on the Internet in which our data is constantly published and shared. It is similar to the right to data transferability, which implies that companies dealing with analytics of personal data will have to provide their users, on their request, with all the information about them in machine-readable format, so that this data can be used for others services.

• Records of the processing of personal data

Keeping records of personal data processing, but also formally registering such records with the Commissioner for the Protection of Personal Data is an obligation that is prescribed by the current Law in Serbia. GDPR imposes somewhat fewer obligations, and prescribes only the obligation to keep such records, with the exception of smaller operators

and those that do not collect sensitive data. But here we should wait and see what the new law solutions will be pertaining to these records.

• Privacy by design and Privacy by default (Privacy by design & Privacy by default)

The concepts Privacy by Design and Privacy by Default (Cavoukian, 2011) as a rule will be discussed in detail in future because the implementation of information solutions based on these principles will be an imperative for large systems that handle personal data, but also a business opportunity for software development companies and similar technical solutions.

GDPR prescribes that it is necessary to design data processing and information systems from the very beginning to effectively implement the data protection principles and protect the rights of the persons to whom the data relate to, and that appropriate measures need to be implemented in order to process only data on the personality that are necessary for the specific purpose of processing i.e., to collect minimum data from citizens.

• Reporting security incidents

Despite the fact that investment in infra-red security has increased considerably, we can read almost every day that multi-million personal databases have been often compromised. Accordingly, the GDPR prescribes that in the case of incidents or data compromise (data breach) there is an obligation to notify the competent bodies for personal data protection within 72 hours with the submission of a detailed case report. And not only that, companies that have found themselves in this situation have to inform all persons whose data are compromised.

3. OBLIGATIONS OF THE REPUBLIC OF SERBIA IN ACCORDANCE WITH THE GDPR REGULATIONS

Formal reasons why Serbia must comply with GDPR regulation are the obligations that Serbia has towards the European Union and the obligations that Serbia has imposed on itself. As an EU membership candidate, Serbia is obliged to harmonize its legislation with the EU acquis. According to the Article 81 of the Law on the Confirmation of the Stabilization and Association Agreement between the European Communities and their Member States of the one part and the Republic of Serbia of the other part (SAA, 2013), the Republic of Serbia has committed itself to harmonizing its legislation on the protection of personal data with communitarian legislation and other European and international privacy regulations.

Harmonization with the Regulation implies that not only the applicable Personal Data Protection Act will be changed, but other laws governing the processing of personal data will be amended or adopted. It is also necessary to adopt by-laws. The method of harmonization will also depend on the constitutional order, because the Constitution of the Republic of Serbia determines that the processing of data must be regulated by law.

4. GDPR IMPACT ON THE FUNCTIONING OF THE INFORMATION AND COMMUNICATION SYSTEM OF THE MOI OF THE REPUBLIC OF SERBIA

In the previous period, the Ministry of Interior of the Republic of Serbia has received several complaints from the Commissioner for Information of Public Importance and Personal Data Protection regarding the unauthorized processing of personal data through a video surveillance system and a system for recording radio-communication of police officers (recording of participants in traffic using the so-called 'Interceptor, audio and video surveillance of the conduct of police officers during the performance of duties and tasks within their competences, etc.). (Gligorijević, Jokić & Maksimović, 2016) Consequently, the definition of legal frameworks and drafting of legal norms within the framework of the Law on Records and Processing of Data in the Ministry of Interior of the Republic of Serbia in this area has begun. In this way, for the first time, in a clear, precise and transparent manner, the sphere of personal data processing in the MoI, as well as the data set on the person being processed, and of course the purpose of the processing itself, has been regulated. By adopting the aforementioned Law, which is fully in line with the GDPR regulations and new Law on Police, the area of personal data processing in the Ministry of Interior has been shaped in accordance with current legal requirements.

Since information security means the protection of systems, data and infrastructure in order to preserve the confidentiality, integrity and availability of information, the application of the law affects all citizens, public authorities and businesses that use information and communication technologies. Namely, legal solutions build user trust in the safe functioning of ICT systems, citizens' trust in the protection of personal data in ICT systems, awareness raising about the necessity of implementing information security measures, data protection, protection of ICT systems, security of electronic transactions, efficient mechanisms of protection and realization of rights in the processes of electronic business, electronic data interchange and e-government services.

The Ministry of Interior owns its own information and communication system, which, beside various databases, containing information obtained by the operational work of the MoI members, has also unique national databases with data on citizens of Serbia. (Popović & Maksimović, 2017) These data are crucial in determining the identity of an individual, and any problem, whether it is an inability to access data, unauthorized access, loss or damage to data, can lead not only to the problems for the individual, but also to the moral and material consequences for the MoI, in the sense of losing citizens' confidence in the ability of this ministry to fulfil its competencies, as well as potential damage that might arise from the blocking of certain services provided by the MoI information and communication system. Therefore, the Ministry of Interior already applies comprehensive protection measures in ICT systems and information in general, and thus we have avoided any incidents that could endanger data or degrade the characteristics of the system. Each segment of the system is defended against external influences, and databases are located on a special, internal computer network of the Ministry that has no contact with other networks. In cases when it is necessary to provide access to data to another state

institution, a separate server is formed, separated from the internal network of the Ministry, with a replicated database. (Nedeljković & Forca, 2015)

5. CONCLUSION

The EU General Data Protection Regulation (GDPR) which replaced the Data Protection Directive from 1995, was drafted and designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, to unify personal data processing and to reshape the way organizations across the region approach data privacy. Both organizations that process the EU citizens' data, and those who are not in the European Union, will have to comply with new rules on personal data protection. This practically means that this regulation also applies to the Republic of Serbia, although it is not a member of the EU yet. Accordingly, the Ministry of Interior of the Republic of Serbia has made appropriate changes in its regulations in order to comply with the GDPR regulations. Such an approach encompasses full compatibility in cooperation and exchanging information with all relevant EU institutions.

6. REFERENCES

Babel, C.: *The High Costs of GDPR Compliance,* InformationWeek, UBM Technology Group, 2017.

Blackmer, W.S.: *GDPR: Getting Ready for the New EU General Data Protection Regulation*, Information Law Group, InfoLawGroup LLP, 2016.

Cavoukian, A.: Privacy by Design in Law, Policy and Practice, A White Paper for Regulators, Decision-makers and Policy-makers, Information and Privacy Commissioner, Canada, 2011.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, 1995.

Gligorijević, M., Jokić, N., Maksimović, A.: Forensic and legal aspects concerning the use of the video surveillance system in proving crimes and offences, Tematski zbornik radova, Dani Arčibalda Rajsa, Tom III, Kriminalističko-policijska akademija, 2016.

Lehavi, A., Larouche, P., Accetto, M., Purtova, N., Yemer, L.: *The Human Right to Privacy and Personal Data Protection: Local-to-Global Governance in the Digital Era*, Research Project Human Rights Working Group, Law Schools Global League, 2016.

Mantelero, A., The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten', Computer Law & Security Review, 2013.

Nedeljković, S., Forca, B.: Evropska strategija bezbednosti i sajber pretnje – značaj za Srbiju, Vojno delo, Ministarstvo odbrane Republike Srbije, 2015.

Popović, R., Maksimović, A.: Institucionalni i pravni okviri upravljanja policijskom organizacijom u sprečavanju i suzbijanju pretnji bezbednosti informaciono-komunikacionog sistema Ministarstva unutrašnjih poslova, Upravljanje

policijskom organizacijom u sprečavanju i suzbijanju pretnji bezbednosti u Republici Srbiji, Tematski zbornik radova, Kriminalističko-policijska akademija, 2017.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Brussels, 2016.

Stabilisation and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Serbia, of the other part, Brussels, 2013.

UDK 355.40
https://doi.org/10.18485/fb_ic4hs.2018.9

INTERNATIONAL INTELLIGENCE SHARING: KEY PRECONDITIONS FOR AN EFFECTIVE OVERSIGHT

Luka GLUŠAC*

Abstract: International intelligence sharing has increased in the last twenty years or so, particularly after the terrorist attacks of 11 September 2001. Already established intelligence cooperation agreements, bilateral and multilateral, have entered into a new phase, resulting in a vast amount of intelligence shared, including the information on their own citizens communicated by national agencies both among themselves, and with their foreign counterparts. Some of those intelligence cooperation agreements are formal, constituting legal instruments, but an important number of them are actually informal, based upon the common understanding between heads of the national intelligence services or other state officials. When intelligence exchange is based on informal international cooperation, rooted only in a scarce and usually outdated national legislation, then there are no legal safeguards for the citizens, who are essentially the targets of such an exchange. In other words, these practices have had many human rights implications. While there is a considerable body of literature on intelligence sharing per se, its human rights aspects remain largely neglected. Hence, our aim is to map the preconditions for an effective oversight of international intelligence sharing, concentrating on the external oversight that should be designed to guarantee a legally sound exchange of intelligence with foreign partners.

Keywords: security, oversight, privacy, intelligence sharing, intelligence cooperation

1. INTRODUCTION

Globalisation has created a relatively borderless world in which states move clumsily but wherein their illicit opponents move elegantly (Aldrich, 2008). National governments have placed intelligence in the front line against a range of transnational opponents, coupled with an increased understanding of the importance of international intelligence cooperation. However, at the same time, such a cooperation has been a great challenge, since it is not a natural instinct of intelligence services (ibid). Intelligence services are in

* The author is a PhD Candidate at the University of Belgrade - Faculty of Political Sciences, and Independent Adviser in the Secretariat of the Protector of Citizens (Ombudsman) of the Republic of Serbia, lukaglusac@gmail.com. The views expressed in this article are his own and do not necessarily reflect the positions of the Ombudsman. lukaglusac@gmail.com

constant fear that with intelligence sharing they actually risk not only the disclosure of secret information obtained from secret sources, but a potential exposure of their methods, thus hindering their ability to collect intelligence in the future.

After 9/11, the United States made full use of its foreign intelligence cooperation (liaison) relationships, for both defensive and offensive purposes (Joint Intelligence Committee, 2002). At the same time, inquiries into 9/11 have shown that cooperation between the different services even within one country is often poor (Aldrich, 2010: 21). In the decade since 9/11, many national governments have worked to overcome legal and organisational barriers to information sharing, both on domestic and international levels. The director of Spain's intelligence service publicly confirmed the enhanced level of cooperation among intelligence agencies since 9/11 (Lefebvre, 2003). As a result, the new zeal for information sharing has extended well beyond counterterrorism to a wide array of law enforcement responsibilities including border security, immigration, smuggling, and espionage (Roach, 2012: 131).

There is a considerable body of literature on intelligence sharing, including those on the costs and benefits to each country of engaging in intelligence sharing (see Walsh, 2007; Sims, 2004; Richelson, 1990). When intelligence exchange is based on informal international cooperation, rooted only in a scarce and usually outdated national legislation, then there are no legal safeguards for the citizens, who are essentially the targets of such exchange. However, these human rights aspects of intelligence sharing remain largely neglected in the literature. Hence, our aim is to map the preconditions for an effective oversight of international intelligence sharing that should be designed to guarantee a legally sound exchange of intelligence with foreign partners.

2. WHAT IS INTERNATIONAL INTELLIGENCE SHARING

Intelligence sharing occurs when one state – the sender – communicates intelligence in its possession to another state – the recipient (Walsh, 2007: 154). Some of those intelligence cooperation agreements are formal, constituting legal instruments, but an important number of them have actually been informal, based upon the common understanding between the heads of national intelligence services or other state officials. Such intensified intelligence exchange has not been followed by appropriate legislation, either on national or international level.

Allies routinely exchange intelligence through various bilateral and multilateral means, but the depth and breadth of these exchanges depend very much on their sharing of a common perception of a threat or sets of interests (Taillon, 2002: 174-175). Bilateral cooperation (or so-called liaison) arrangements are a defining characteristic of the intelligence world. Set up formally (i.e. with the signing of a Memorandum of Understanding) or informally (on the basis of an unwritten, gentlemanly agreement), they pay particular attention to the participants' protection of their intelligence (Lefebvre, 2003: 533). They usually cover a wide range of issues, including the sharing of assessments, raw data, or training facilities and the conduct of joint operations, some of which could lay dormant at any given time (ibid: 533).

Multilateral intelligence sharing arrangements also cover an array of potential activity between governments including, *inter alia*, information sharing, operational cooperation, facilities and equipment hosting, training and capacity building, and technical and financial support. One of the most known arrangements is the Five Eyes alliance – a secretive, global surveillance arrangement comprised of the relevant intelligence agencies of United States, United Kingdom, Canada, Australia and New Zealand, recently referred to as "the most comprehensive and closest intelligence sharing and co-operation arrangement" (Cullen & Reddy, 2016: 46). Although it is a long-lasting alliance with over 70 years of history, little is known about it and about the agreement(s) that governs it. Even less is known about the other surveillance partnerships that have grown from the Five Eyes, such as the 9-Eyes, the 14-Eyes, and the 43-Eyes (see: Privacy International, 2017).[1]

3. HUMAN RIGHTS ASPECTS OF INTERNATIONAL INTELLIGENCE SHARING

Although there is a wide agreement that international intelligence sharing is necessary for countering contemporary threats, its recent expansion has raised a number of potential problems that require vigilant oversight. Individuals are at greater risk of having their rights, especially their right to privacy, infringed. As noted by Roach, individuals will rarely have the opportunity to challenge the accuracy of shared information because they will often be unaware that information about them has been shared and will not have access to the shared information (Roach 2012: 131).

Probably the most obvious human right at risk in this case is the right not to be subject to torture or other forms of cruel, inhuman, or degrading treatment. For instance, information sent to a foreign agency may be used by that agency in support of extrajudicial detention, torture, and even killings. Conversely, information received from a foreign agency may have been obtained through torture or be otherwise tainted (Roach, 2012: 134). Thus, a special care should be taken when sending questions to foreign agencies, not only because they may invite the use of harsh interrogation tactics, but also because foreign agencies may use such questions in a way that is even less amenable to control by caveat (Arar Commission, 2006). In principle, information should never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture (ibid: 345). The UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism recommended that "before handing over information, intelligence services [should] make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and, will not be used for purposes that violate human rights" (UN Human Rights Council, 2010: 46). While this recommendation may seem idealistic, it indeed grasps the very *credo* of human rights-sensitive international intelligence sharing.

[1] For other multilateral intelligence agreements see, for instance: Lefebvre, 2003.

4. MAPPING THE PRECONDITIONS FOR AN EFFECTIVE OVERSIGHT

The sharing of information with foreign agencies generally presents the greatest challenge to oversight bodies and one of the permanent risks to human rights. It is, thus, vitally important that oversight bodies have access to the information being shared by the agencies they oversee — whether or not that information is subject to the claims of secrecy. The above-mentioned UN Special Rapporteur stated that "it is good practice for national law to explicitly require intelligence services to report intelligence-sharing to an independent oversight institution" (UN Human Rights Council, 2010: 49). To facilitate that, intelligence sharing should, preferably, be developed through written agreements, specifying the obligations of both sending and receiving parties with regard to human rights. They should also include standard clauses that permit received information to be shared with the service's principal oversight body and, when possible, with related oversight bodies that agree to the same confidentiality protocols. In other words, intelligence sharing with foreign partners should always be well documented because of the risks involved, and also facilitate review and oversight (Roach, 2012: 137).

While every state chooses its own institutional setup for the oversight, it is widely acknowledged that there has to be a complex oversight system, designed through various forms: internal and external; political and expert; judicial and quasi-judicial; *ex ante* and *ex post* (Glušac, 2018). Given that the oversight powers of particular institutions differ in nature, scope and reach, a high level of cooperation and coordination between them is necessary, both in normative and operational terms (ibid: 19). For instance, in some countries, such as Germany and Serbia, competent parliamentary oversight committees are not granted access to shared information because they are considered to be the so-called third parties.[2] However, in case of Serbia, shared information can be accessed by the Ombudsman, as an independent oversight mechanism.[3]

A totality of individual mandates of oversight bodies should ensure that such oversight system is able to scrutinize at least the following aspects of international intelligence cooperation: (1) effectiveness of cooperation with foreign entities; (2) the legal and (operational) policy framework for international intelligence cooperation; (3) high-risk relationships; (4) risk assessment processes; (5) personal data exchanges and their human rights implications; (6) caveats and assurances relating to information sent to foreign services; (7) reporting and records keeping; (8) joint operations; (9) provision of training and equipment to foreign services; (10) services' training of their own staff; (11) financial transactions relating to international intelligence cooperation; and (12) the role of the executive in international intelligence cooperation (Born, Leigh, & Wills, 2015: 134-143).

Scholars have identified different methods used by overseers to scrutinize international intelligence cooperation, including hearings, documentary analysis, interviews, sampling, and direct access to databases (ibid: 143-150). External overseers may use different types of investigations, such as case-specific, thematic, comprehensive and/or periodic.

---

[2] More on third parties in: Born, Leigh, & Wills, 2015: 152-154.

[3] For more on the Ombudsman's role in oversight of the security services see: Glušac, 2018.

Oversight bodies should understand that intelligence services sometimes use intelligence sharing as a means of avoiding national (domestic) restrictions on their activities. Hence, intelligence services should be "explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities" (UN Human Rights Council, 2010: 49-50).

5. CONCLUSION

To sum up, in order to create an effective oversight system of international intelligence sharing, some basic principles have to be followed. Intelligence services need to be subject to oversight that is complete, i.e. it should encompass all stages of the intelligence cycle. Oversight should be both *ex ante* and *ex post*, but also internal and external. External elements of the oversight should include judicial and expert specialised bodies. Such bodies should be independent, and able to provide for redress. Redress should be provided through, *inter alia*, own-initiative investigations and individual complaint-handling procedures, when applicable. Ombudsman or similar specialised (external) body can act as quasi-judicial mechanism, complementing the work of judiciary. Irrespective of the institutional design, such mechanism should have broad mandate and sufficient resources to perform effective oversight. Those bodies should also serve to provide layered transparency, which is of critical importance in a democratic society.

As argued in this paper, international intelligence sharing should be regulated by written agreements, whenever possible. It is expected that, in most circumstance, making such an agreement in writing would not have negative consequences on its implementation, but would enable oversight that is more robust.

Finally, as national intelligence agencies share information in order to be able to fulfil their mandates, national oversight bodies should do the same. A step in the right direction is a recent initiative of independent oversight bodies in five countries which agreed to establish the Five Eyes Intelligence Oversight and Review Council "to facilitate the sharing of experiences and best practice in oversight and review" (Australian Inspector-General of Intelligence and Security, 2017: v).

6. BIBLIOGRAPHY

Aldrich, R. J. (2008). Setting Priorities in a World of Changing Threats. In S. Tsang, *Intelligence and Human Rights in the Era of Global Terrorism* (pp. 158-171). Stanford: Stanford University Press.

Aldrich, R. J. (2010). International Intelligence Cooperation in Practice. In H. Born, I. Leigh, & A. Wills, *International Intelligence Cooperation and Accountability* (pp. 18-41). New York: Routledge.

Australian Inspector-General of Intelligence and Security. (2017). *Annual Report 2016-17.* Barton: IGIS.

Born, H., Leigh, I., & Wills, A. (2015). *Making International Intelligence Cooperation Accountable.* Geneva: DCAF.

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. (2006). *Report of the Events Relating to Maher Arar: Analysis and Recommendations.* Ottawa: Privy Council.

Cullen, M., & Reddy, D. P. (2016). *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand.*

Eskens, S., van Daalen, O., & van Eijk, N. (2015). *Ten Standards for Oversight and Transparency of National Intelligence Services.* Amsterdam: University of Amsterdam - Institute for Information Law.

Glušac, L. (2018). National Human Rights Institutions and Oversight of the Security Services. *Journal of Human Rights Practice, 10*(1), 58–82.

Joint Intelligence Committee of the US Senate and US House of Representatives. (2002). *Investigating the Events Leading to the Attacks of September 11, 2001*. Washington, DC.

Lefebvre, S. (2003). The Difficulties and Dilemmas of International. *International Journal of Intelligence and, 16*(4), 527-542.

Privacy International. (2017). *Human Rights Implications of Intelligence Sharing.* London: Privacy International.

Richelson, J. (1990). The Calculus of Intelligence Cooperation. *International Journal of Intelligence and Counterintelligence, 4*(3), 307-323.

Roach, K. (2012). Overseeing Information Sharing. In H. Born, & A. Wills, *Overseeing Intelligence Services: A Toolkit* (pp. 129-150). Geneva: DCAF.

Sims, J. (2004). Foreign Intelligence Liaison: Devils, Deals, and Details. *International Journal of Intelligence and CounterIntelligence, 19*(2), 195-217.

Taillon, P. (2002). Hijacking and Hostages: Government Responses to Terrorism. Westport: Praeger.

UN Human Rights Council. (2010). Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

Walsh, J. I. (2007). Defection and Hierarchy in International Intelligence Sharing. Journal of Public Policy, 27(2), 151-181.

UDK 343:004.056(437.6)
https://doi.org/10.18485/fb_ic4hs.2018.10

TECHNOLOGIES AND DEVELOPMENT IN VIEW OF TAX CRIMINAL OFFENCES[1][2]

Tomáš STRÉMY[*], Natália HANGÁČOVÁ [**]

Abstract: Nowadays, technologies are developing rapidly and legal systems are not able to react to changes in the society and economy as fast as the perpetrators of individual criminal offences. This fact is particularly notable in the area of economic criminality. Due to the European Union's evolution, European Union's internal market, the digitalisation of economy and the development of new technologies, it is necessary to adapt the legal systems of states to new challenges, in order for them to be able to react to changes in society in an appropriate manner.

Tax criminal offences are committed across a number of states, making cooperation among states necessary as well. Cooperation and mutual assistance should be strengthened, in order to prevent states from losing revenues from taxes, which will be used to finance public services.

These days many companies use clouds as a medium to store data, e.g. data concerning companies' bookkeeping records. In the legislation of the Slovak Republic, there is a special procedural institute for securing data stored in clouds. This is why the data stored in clouds are secured in a different way for the purpose of criminal proceedings than other data/evidence saved or downloaded on personal computers. Using clouds as a place for storing accounting records is a new trend. However, the Slovak Republic has legislation enabling the state to secure data stored in clouds. On the other hand, many problems arise in practice.

It is clear that legislation has to be in compliance with the development of new technologies. Therefore, the following question arises: *"Are technologies a tool of empowerment or vulnerability?"*

---

[1] Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-15 0740.

[2] This paper was supported by the Agency for Research and Development under contract no. APVV-15-0740.

[*] Prof. JUDr., PhD, Faculty of Law, Comenius University in Bratislava, tomasstremy@gmail.com

[**] JUDr, Faculty of Law, Comenius University in Bratislava, natalia.hangacova@flaw.uniba.sk

Keywords: tax criminal offences, mutual assistance in criminal matters, clouds, evidence in criminal law

1. INTRODUCTION

Technologies are our future. In recent years, the European Union has launched several exchange programs (for the exchange of information among the Member States) which use technologies with the aim of preventing tax criminal offences. Council Directive 2008/117/EC also emphasises the fact that the exchange of information between the Member States needs to be strengthened. The basic framework for exchange of information is Council Directive 2006/112/EC. Council Directive 2008/117/EC amends Council Directive 2006/112/EC. The latter was introduced due to the losses that the Member States were suffering as a consequence of value added tax frauds (hereinafter referred to as "VAT frauds"). VAT frauds distort competition in the single market: Member States are losing tax revenues and goods are placed on the market at abnormally low prices as a consequence of companies' fraudulent behaviour.

Technologies themselves are helping in the exchange of information between the Member States of the European Union to facilitate a quick response to required information. Eurojust has its coordination centres and Europol deploys a mobile office which enables real-time information exchange on e.g. VAT frauds.[3] A close cooperation between Eurojust and Europol helps to reveal VAT frauds.

The use of technologies is also helping in the area of situation prevention, where camera systems are installed and used in public places and private premises to protect property against criminality. Property criminality is the most common type of criminality committed in the Slovak Republic.

On the other hand, modernisation and technologies help to facilitate money laundering, where money moves quickly through a number of bank accounts in order to cover its real origin. Money usually comes from illegal activities such as drug trafficking or illicit arms trafficking. Technologies promote a rapid flow of money; however, when businesses use bank transfers, these transactions can be traced. The problem with tracing the transactions arises due to bank secrecy, alternatively known as bank-client confidentiality or financial privacy. Money is moved across a number of Member States or third countries. At this stage, exchange of information is crucial.

Technologies, the Internet and modernisation are lending a hand to cybercrimes as well e.g. hacking, phishing and other forms of frauds committed in cyberspace. This is why technologies should be used to support the fight against tax criminality. In the article, the authors focus on the issues of securing evidence for criminal proceedings stored in clouds and on the videotaking of evidence in criminal proceedings. In the course of securing evidence, a search warrant has to be issued, yet its execution interferes with human rights.

---

[3] A major Europe-wide VAT fraud network busted with the support of Eurojust and Europol. (2018, July 16). Retrieved from http://www.eurojust.europa.eu/press/PressReleases/Pages/2015/2015-03-03.aspx, 15.8.2018.

2. SECURING EVIDENCE IN CLOUDS

In the Slovak Republic, there is a difference between securing evidence downloaded and/or saved on personal computers and evidence which is located in mailboxes or in clouds. This is relevant mainly in connection with tax criminal offences. The issues of cloud storage are not applicable in connection with e.g. the criminal offence of abuse of competition, because cartel agreements are usually not made in writing and non-existent agreements can therefore not be stored in clouds.

Cloud storage is a new phenomenon for businesses. It is a place where companies store data. By virtue of digitalization, companies are increasingly using information technologies for their business activities. Companies claim that they are going green (because e.g. purchase orders, invoices, and bookkeeping records are not kept at the seat of the company physically but are stored electronically in clouds). Cloud storage means that data are stored in an immaterial cloud. Cloud storage providers provide a service and they make the stored data available to their "owners" anytime and anywhere. The owner simply needs to have Internet access. The documents located in mailboxes or in the cloud are accessible on the Internet.

For most people, it seems that clouds are a new phenomenon. However, the first clouds were invented in the 1960s and the first widely used cloud was Amazon's cloud, which was introduced in 2006.

Purchase orders, invoices and bookkeeping records are crucial evidence in criminal proceedings related to tax criminal offences, because they refer to business which was made. However, in carousel frauds the transactions are made only "on paper" most of the time. It is therefore important to confront the transactions declared with witness statements.

When law enforcement agencies need to secure evidence stored in the cloud in criminal proceedings related to tax criminal offences, they need an Order according to § 115 (Interception and recording of telecommunication operation) or § 116 (Notification of telecommunication data) of the Criminal Procedure Act of the Slovak Republic. However, cloud providers cannot grant them access to the content saved in the cloud; under the Order, they are obliged/allowed to give only log-in data such as name/e-mail and password to law enforcement authorities.[4] This is justified by the fact that cloud or e-mail providers are not allowed to store the content of e-mails or content of cloud data.

According to § 130 subparagraph 2 of the Criminal Code Act of the Slovak Republic, *the thing* for the purpose of criminal proceedings is also immaterial information and data from computing technology. Immaterial information and data from computing technology can be secured for the purpose of criminal proceedings using the institute of house search, personal search or search of other premises and land set in § 99 and following the Criminal Procedure Act of the Slovak Republic. The institute of house search is applicable only in cases when the information which will be secured as evidence in criminal proceedings has been saved or downloaded on a computer which was found on the inspected premises. The

[4] Article 116 subparagraph 2 of the Criminal Procedure Act of the Slovak Republic.

institute of house search is not applicable for securing data stored in clouds or in e-mails. In accordance with § 100 subparagraph 1 of the Slovak Criminal Procedure Act, a search warrant is required. The requirement of the search warrant rests on the fact that its execution interferes with human rights such as the right to home liberty as well as the right to privacy. A house search may be executed if there is reasonable suspicion that there is a thing of importance for criminal proceedings (i) in a flat or (ii) on other premises used for housing or (iii) on the premises belonging to them as well as (iv) premises not used for housing and (v) land which is not publicly accessible.[5] Data which are saved on a computer are considered to be a *thing* in terms of § 130 subparagraph 2 of the Criminal Code Act of the Slovak Republic and may be secured and analysed legally if they were secured during a house search when a search warrant was issued.

On the other hand, e-mail communication as well as information in clouds has the character of a telecommunication operation. This information is accessible on the Internet and the Internet is not a *thing* in accordance with the definition enshrined in § 130 of the Criminal Code Act.

The institute of notification of telecommunication data enshrined in § 116 of the Slovak Criminal Procedure Act is applicable in situations where e-mail communication (any communication available on the Internet) needs to be secured for the purpose of criminal proceedings. The notification of telecommunication data refers to electronic communication that has already taken place (not communication running in real time, e.g. having WhatsApp communication where § 115 of the Slovak Criminal Procedure Act is applicable). Communication and information accessible on the Internet (not saved or downloaded on a computer) cannot be secured using the institute of house search.

The conditions for issuing an Order for the notification of telecommunication data are set in § 116 subparagraph 1 and 6 of the Slovak Criminal Procedure Act. Provision § 116 subparagraph 6 refers to the fact that paragraphs 1 to 5 of § 116 also apply to data transmitted via a computer system, i.e. data stored in clouds. An Order for the notification of telecommunication data may be issued in relation to an exhaustive number of criminal offences, but only if the intended purpose cannot be achieved otherwise, if achieving the intended purpose would otherwise be substantially more difficult and if the information is necessary to clarify facts important for criminal proceedings.[6]

In practice, problems arise when the cloud provider has its seat in another Member State or in a third country or when the provider is unknown. In the worst-case scenario, law enforcement agencies will not be granted log-in data and they are prevented from inspecting documents e.g. bookkeeping records stored in the cloud. From this point of view, it seems that technologies may facilitate the commitment of criminal offences, predominantly tax criminal offences, where documentary evidence is crucial.

5 Article 99 subparagraph 1 and 2 of the Criminal Procedure Act of the Slovak Republic.

6 The restrictions for issue of Order for notification of telecommunication data are imposed in order to protect telecommunication secrecy and personal data of individuals.

3. VIDEOTAKING OF EVIDENCE

Another modern type of evidence in criminal law apart from evidence stored in clouds is evidence obtained by videotaking. In the second part of the article, we focus on the issue of videotaking of evidence.

The classification of evidence defines the differences between various types of evidence and determines their relevance for the evidentiary process during criminal proceedings.

Evidence in criminal proceedings is classified according to the subject matter of the accusation, according to the relationship between the evidence and the source of information, according to the relationship between the evidence and the facts to be proven, according to the source of evidence and according to the possibility of its use in criminal proceedings.

According to the possibility of their use in criminal proceedings, two types of evidence are distinguished:

- absolutely void evidence – evidence obtained illegally, which may not be used in the evidentiary process, e.g. a coerced confession of the accused,
- relatively void evidence – evidence with lesser defects that can be used in the criminal proceedings provided that the defects are eliminated, e.g. if the accused signs the pages of the minutes that he did not sign during his examination,
- absolutely valid evidence – evidence obtained legally, by using the means of evidence in accordance with the Criminal Procedure Act.

According to § 119 subparagraph 2 of the Criminal Procedure Act of the Slovak Republic, evidence can be not only what is mentioned as the evidence in this article but everything that can contribute to the clarification of the case and that has been obtained from evidences according to the Criminal Procedure Act of the Slovak Republic or another act. In conclusion, we believe that we could add videotaking of evidence to absolutely valid evidence.

Videoconferencing is a useful tool, which has great potential not only at the national level but also in cross-border situations involving different Member States and even third countries. In cross-border cases, smooth communication between the judicial authorities of the Member States is crucial. Videoconferencing is a possible way of simplifying and encouraging such communication. The advantages of videoconferencing are acknowledged by Union Law, which encourages its use, inter alia, in cross-border taking of evidence, in civil and commercial matters, in the European Small Claims Procedure, or in regulated procedures for its use in criminal proceedings.[7]

It is essential to understand the main purposes of Regulation 1206[8] in order to improve and facilitate judicial cooperation between the Member States. The central theme of Regulation 1206 is that the taking of evidence needs to be efficient and swift. Courts are

[7] Torres M. (2018). Cross-border litigation: Videotaking of Evidence within EU Member States. Dispute Resolution International, 12(1), 71.

[8] Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

expected to execute a request from other Member States expeditiously.[9] Regulation 1206 provides a certain number of forms to allow reliable communication among courts in the interest of swiftness and limits the cases in which cooperation requests may be refused. Finally, Regulation 1206 tries to minimise the issue of costs as an obstacle to the execution of requests. The EU promulgated the Strategy on European e-Justice (2014–2018), adopted by the Council (Justice and Home Affairs) on 6 December 2013. An e-Justice Action Plan 2014–2018 (the "Action Plan") was also adopted by the Council. This was followed by guidelines on the implementation of the Multiannual European e-Justice Action Plan (2014–2018), which were endorsed by the Council (Justice and Home Affairs) on 4 December 2014, and set out concrete steps to implement the Action Plan by the Working Party on e-Law (e-Justice).[10]

According to Council Act (2000/C 197/01) article 10 paragraph 1, if a person is in one Member State's territory and has to be heard as a witness or expert by the judicial authorities of another Member State, the latter may, where it is not desirable or possible for the person to be heard to appear in its territory in person, request that the hearing take place by videoconference, as provided for in paragraphs 2 to 8 of article 10.

The requested Member State must agree to the hearing by videoconference provided that the use of the videoconference is not contrary to the fundamental principles of its law and on condition that it has the technical means to carry out the hearing. If the requested Member State has no access to the technical means for videoconferencing, such means may be made available to it by the requesting Member State by mutual agreement (article 10 paragraph 2 of 2000/C 197/01).

The paragraph 8 of article 10 of 2000/C 197/01 states that each Member State shall take the necessary measures to ensure that, where witnesses or experts are being heard within its territory in accordance with this Article and refuse to testify when under an obligation to testify or do not testify according to the truth, its national law applies in the same way as if the hearing took place in a national procedure.[11]

If we ask ourselves under what conditions a witness can be heard via videoconferencing or other technical means, the answer would be that before examining the witnesses the court must establish their identity and their relationships to the parties. Furthermore, witnesses must be informed of the significance of the testimony, their rights and obligations, the criminal consequences of giving false testimony, and of their entitlement to witness fees. The court invites the witnesses to describe, in a coherent manner, everything that they know about the subject matter of the examination. The court then asks the witnesses questions that are necessary for supplementing and clarifying their testimony. Witnesses

[9] Recital 10 of the Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

[10] Torres M. (2018). Cross-border litigation: Videotaking of Evidence within EU Member States. Dispute Resolution International, 12(1), 72-73.

[11] Council Act (2000/C 197/01) establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

may not be asked tendentious or leading questions. If the parties to the proceedings or expert witnesses are asked any such questions or any questions relating to the legal assessment of the case, the presiding judge will deem the questions inadmissible. The presiding judge decides on the inadmissibility of the questions in an order that is not served and against which no appeal may be lodged. The order only forms part of the transcript of the hearing. Subject to the consent of the parties to the proceedings, the court can organise an oral hearing via videoconferencing or other communication technology facilities.[12]

4. CONCLUSION

The article has dealt with technology as a tool of empowerment or vulnerability. The authors have highlighted the securing of evidence in clouds because cloud storage is a new phenomenon for businesses – it is a place where companies store data. Cloud computing has been one of the most important topics in the field of Information Technology in recent years, and its popularity is rising very fast. According to Forbes contributor Louis Columbus, a key point from an IBM study was that "Cloud computing has rapidly accelerated from 30% of Chief Information Officers (CIOs) mentioning it as a crucial technology for customer engagement in 2009 to 64% in 2014". Every day, many organizations and companies are migrating their services over the cloud, and a great number of companies are considering adopting this technology. But companies' primary obstacle to moving their systems to the cloud concerns security and the constantly increasing number of digital crimes occurring in cloud environments. The authors have also dealt with the videotaking of evidence because the possibility of taking evidence by videoconference has been enthusiastically promoted by the European Union Member States, and it is now legally permissible not only for civil and commercial matters but also for criminal matters. Subject to the consent of the parties to the proceedings, the court can organise an oral hearing via videoconferencing or other communication technology facilities.

5. REFERENCES:

Act no. 301/2005 Coll. Criminal Procedure Act of the Slovak Republic.

Act no. 300/2005 Coll. Criminal Code Act of the Slovak Republic.

BLAŽEK R. (2018) *Trestnoprávne aspekty držania strelných zbraní v Slovenskej republiky*. Bratislava, Slovak Republic: Heureka.

ČENTÉŠ J. a kol. (2017) *Trestný poriadok Veľký komentár.* Bratislava: Bratislava, Slovak Republic: Eurokódex.

Council Act (2000/C 197/01) establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

[12] Taking of evidence – Slovakia. (2018, July 16). Retrieved from https://e-justice.europa.eu/content_taking_of_evidence-76-sk-en.do?member=1#toc_2_12, 15.8.2018.

Council Directive 2008/117/EC of 16 December 2008 amending Directive 2006/112/EC on the common system of value added tax to combat tax evasion connected with intra-Community transactions.

Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC.

Major Europe-wide VAT fraud network busted with the support of Eurojust and Europol. (2018, July 16). Retrieved from http://www.eurojust.europa.eu/press/PressReleases/Pages/2015/2015-03-03.aspx. 15.8.2018.

STRÉMY T., HANGÁČOVÁ N. (2017) *Value Added Tax Frauds (Carousel Frauds)*. Praha, Czech Republic: Leges.

ŠAMKO P. (2017) *Poznámky k aplikačným problémom pri zaisťovaní počítačových údajov v trestnom konaní*. Zo súdnej praxe, 6, 248-252.

Taking of evidence – Slovakia. (2018, July 16). Retrieved from https://e-justice.europa.eu/content_taking_of_evidence-76-sk-en.do?member=1#toc_2_12

Torres M. (2018). *Cross-border litigation: Videotaking of Evidence within EU Member States*. Dispute Resolution International, 12(1), 71-95.

UDK 323.284—053.6
https://doi.org/10.18485/fb_ic4hs.2018.11

JUVENILES INSIDE THE TERRORIST GROUPS

Božidar BANOVIĆ[*], Višnja RANĐELOVIĆ[**]

Abstract: One of the main features of contemporary terrorist groups is an increasing number of juveniles in their ranks. Juveniles are easy and cheap recruits, and make it easier for terrorist groups to attack. The main reasons why terrorists recruit juveniles are that they are cheap recruits, who also bring some tactical and strategic advantages to their operations. For example, a juvenile in the role of a suicide bomber spreads fear wider, which is the main consequence that terrorist groups intend to produce. Furthermore, there are many reasons why juveniles join terrorist groups, for example, religious motivations, economic and financial motivations, and social motivations. There are many different ways in which terrorist groups recruit and attract juveniles. Institutions that juveniles interact with, like schools, can play a significant role. A modern way of recruiting juveniles by terrorist groups is via the Internet and social networks, which is now recognised as an increasing problem. In the papers, the authors analyse reasons why terrorist groups recruit juveniles, as well as why juveniles join terrorist groups, the role that juveniles have inside the terrorist groups, and the ways they are recruited, especially via the Internet and social networks, as a modern way of recruitment.

Keywords: terrorist groups, recruitment of juveniles, juveniles' roles, social networks

1. INTRODUCTION

Terrorism, as a dominant security challenge worldwide in recent years, has multiple impacts on juveniles and therefore presents an increasing problem for the protection and safety of juveniles. Not only that the recruitment of juveniles by terrorist groups jeopardizes the security and safety of juveniles, but it also presents an increased threat to civilians and causes greater fear among them. So, juveniles are drown into terrorism as victims and as participants, perpetrators of terrorist acts.

Nowadays, many different reasons for recruiting juveniles by terrorist groups can be recognised, and they include both forced recruitment and joining on a voluntary basis.

[*] Full Professor, PhD, University of Belgrade Faculty of Security Studies,banovicb@fb.bg.ac.rs
[**] Teaching Assistant, Faculty of Law, University of Kragujevac, vmilekic@jura.kg.ac.rs

Aetiology of these two ways of recruitment is different, but we can find the same environmental and circumstantial factors that lead to the engagement of juveniles in terrorist activities. Understanding the aetiology and phenomenology of the problem presents a useful step in the combat against terrorism.

But, the practice has shown that terrorists always find some new ways to act. Nowadays, with the global use of the Internet and social networks, it is obvious that they can be used not only for entertainment and business, but they can also be misused. Terrorists have realised the benefits of the Internet and social networks and started using them for recruitment of new members and for publishing recordings of their activities.

2. TERRORISM

Terrorist activities mostly have international implications, but at the beginning of the fight against terrorism, sovereign states had the dominant role. Eventually it was realised that any sovereign state by itself could not effectively fight against terrorism, but instead a comprehensive international cooperation was required. Consequently, intensive international and regional legal activity followed in order to establish a unique legal frame with the aim to fight against terrorism more effectively (Banović, 2007, p. 145.).

After many attempts to define terrorism properly, in 2000 the UN General Assembly adopted the International Convention for the Suppression of the Financing of Terrorism (UN General Assembly, 2000), which included the definition of terrorism that was later determined as a definition that encompassed the essence of terrorism. According to this Convention, terrorism includes: *first*, an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex (for example, taking of hostages, terrorist bombings etc.), and *second*, any other act intended to cause death or a serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when a purpose of such act, by its nature and context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act (article 2. (1) (a) (b)).

One of the main characteristics of terrorism is the depersonalisation of the victim, because the perpetrator of a terrorist act doesn`t attack any particular victim, but he attacks the victim on a random basis. Furthermore, terrorism can manifest in many different shapes, as we could see from the definition which is not determined on the *numerus clausus* basis. That is why people say that terrorism has a ‘chameleon nature’ (Kaseze, 2005, p. 144.).

However, during all the efforts to enact and apply counter-terrorism legislation, there were only few considerations that juveniles could be some of these terrorists and that some aspects of this problem should be taken into account (Brett, 2002, p. 33.).

3. RECRUITMENT OF JUVENILES BY TERRORIST GROUPS

Recruitment of juvenile by terrorist groups has become a well-known practice in many countries around the world, and it is a recent phenomenon that has been developing through the last decade. The reasons why terrorist groups recruit juveniles are multiple and

complex, also depending on the concrete situation, but the fact is that some terrorist groups, when recruiting, target particularly juveniles (UNODC, 2017, p. 10.).

There are many reasons why terrorist groups recruit juveniles and there are many researches on the aetiology of this phenomenon. We will point out to some of them. One research (UNODC, 2017, p. 10-11.) has shown that some terrorist groups, like Boko Haram and ISIL, recruit juveniles in order to *boost their visibility*, as means of propaganda, and to shock the public and to show the power and ruthlessness of the group. Although, there are demographic reasons, since in some countries there are more juveniles than adults, making juveniles more available for recruitment and abduction. There are also economic reasons, since juvenile recruits are usually less paid and need less food to survive. With the proliferation of small arms and light weapons, juveniles are increasingly likely to act as effectively as adults, and that is also why terrorist groups recruit them. Furthermore, juveniles' mental and physical capacities make them easier to intimidate and easier to control, and, what is particularly important they show higher degree of loyalty to authority figures. Also, recruitment of juveniles brings some tactical advantages to terrorist groups. Namely, juveniles have less understanding of the risk they are facing and they are more obedient than adults, which is why they are used as spies, porters, to carry materials and undertake suicide attacks.

According to other research, terrorist groups recruit juveniles because it is a low-cost way to build their forces, bringing tactical and strategic advantages. Additionally, there is one psychological moment: the use of suicide bombers spread fear wider than conventional terrorism, and putting juveniles in this role heightens the hysteria terrorists strive to cause (Singer, 2006, p. 118-119.).

Some terrorist groups often target orphans, the fatherless and refugees, offering them a 'the new family' and, consequently, using them for suicide bombing (Meillahn, 2008, p. 7.).

But the recruitment of juveniles by terrorist groups presents only one side of the problem, because there is much evidence around the world showing juveniles who voluntarily join terrorist groups. Aetiology of this side of the problem is also multiple and complex and presents a combination of youth's susceptibility to powerful influences and the cruel environment which shape them (Singer, 2006, pp. 119-120.). So, the first reason why juveniles join terrorist groups can be found in religious motivations. For example, in Islam there is a tendency to promote the concept of martyrdom, dying for one's faith. There are sometimes economic motivations, because juveniles from poor families and environments join terrorist groups in order to get food, clothes and shelter. Some of these groups promise to pay juvenile's family or to take care of them, if the juvenile joins the group. Schools and other institutions of importance for juveniles can also play a significant role by indoctrination, ideological education and other means of imposing attitudes and beliefs. Social environment can also influence juveniles' decisions to join, which is particularly peculiar for *shame societies*, where acquisition of honour and avoidance of shame present the key factor of behaviour. In some societies this can be even more pronounced, like in Sri Lanka and Pakistan, where terrorist groups give families of young suicide bombers special recognition and honours in the community. There are some personal reasons for joining terrorist groups, for example, loss of family member or close friend, other forms of

direct suffering from violence, jailing or brutalisation from local security forces etc. (Singer, 2006, pp. 120-124.). Some of these circumstances, or their combination, can act as a push factor in relation to juvenile's decision to join terrorist groups.

Some of the other reasons or motivations that lead to their engagement within terrorist groups are: moral outrage, ideology, revenge, patriotism, financial incentives, religious incentives, prestige, as well as sense of purpose, meaning and identity. Beside these reasons, there are some particularly characteristic for female juveniles, like a response to the cultural importance placed on the male child, loss of a family member, lack of material or financial support, rape, divorce, marriage to someone the family disapproves of, rejection by society, sense of cultural humiliation etc. (Meillahn, 2008, p. 11.).

Some juveniles are born and live in an environment that is likely to make them become terrorists. For example, in Lebanon and Palestinian territories, where the cults of martyrdom exist, many juveniles, even very young children, are willing to make the ultimate sacrifice of martyrdom. Many of them have passed through the 'education' that presents psychosocial manipulation and indoctrination. Terrorists have used juveniles for different purposes, for propaganda, for fighting and even hacking off the heads of hostages (Meillahn, 2008, p. 6-7.).

According to Israeli Security Agency (sources, 2003), terrorist groups recruit children because their innocent appearance does not arouse suspicion and can easily blend in with the crowd. They are easily influenced and thus make them more convenient recruits for suicide bombing missions. Children are taken from their homes and families and schools and indoctrinated in order to carry out terrorist act, very often by convincing them that they will be granted paradise if they do so. Children are indoctrinated with extreme Islamic ideas, in schools, youth camps and via the Internet. Childhood is used in many ways by terrorists. Not only children are used to conduct terrorist activities, but also children toys are used for camouflaging their activities. Furthermore, terrorists try to camouflage their activities by acting near schools and kindergartens.

When trying to explain the aetiology and the phenomenology of the recruitment of juveniles by terrorist groups, many authors take the example of Palestinian juveniles. One of the main characteristics of the war between the Palestinians and Israelis is a large number of terrorist acts, especially suicide bombings, carried out by Palestinian juveniles. Juveniles participated in the war from its beginning, however from September 2000 the involvement of juveniles got a dark twist, because a lot of them joined different terrorist organisations and expressed a strong will to commit acts of terrorism and suicide (Rosen, 2005, p. 92.). The Palestinians constantly attribute the terrorist acts, especially suicide bombings, to the horrific situation of the Palestinians under Israeli occupation. In that way, the responsibility for these acts is transferred to Israel. So, suicide bombers are 'double victims', first victims of Israeli occupation, and then victims of their own acts of self-annihilation in response to Israeli occupation. It is obvious that revenge is the main motive for terrorist activities (Rosen, 2005, pp. 123-124.).

4. THE ROLE OF THE INTERNET AND SOCIAL NETWORKS

One of the main characteristics of the Internet and social networks is the massiveness of users. Logically, this advantage of the Internet and social networks has not been recognised only by those who use the Internet and social networks for work, fun and pleasure, but also by those who are prone to criminal activities, and among them – by terrorist groups. And this is the dark side of the fact that 'almost whole world is on the Internet'. So, the Internet by itself is not harmful, but the way it is used by some individuals or groups (Milekić, 2013, p. 177.), in this case by terrorist groups.

Cyber terrorism is a problem of the modern age. In order to find and recruit new members, terrorists use all the Internet resources and services, as well as different forums and social networks. The Internet and social networks are, as well, often used for propagation of terrorist activities and for taking responsibilities for conducted terrorist acts (Miladinović & Petričević, 2012, p. 7.). Considering aetiological aspects, the main reasons for conducting criminal activities on the Internet and social networks are massiveness of users, informatics illiteracy, lack of awareness of security risks, difficulties in identifying criminals (in this case terrorists) etc. (Miladinović & Petričević, 2012, pp. 2-3.). Of course, these reasons become even more pronounced in relation to juveniles. Namely, great number of users are juveniles, and juveniles are those informatics illiterates who lack awareness of security risks. The consequence is that this represents a fertile soil for terrorist groups to recruit juveniles, with little or almost no chance to be discovered and identified.

Namely, terrorist groups also use the Internet and social networks for multiple reasons. We are all familiar with videos published on the Internet with recorded activities of terrorist groups, killing or torturing someone, or with recorded messages for the international society in order to cause a fear. Terrorists have also realised that the development of many different social networks could be used as a source of new recruits, especially among juveniles who are the main users of these networks.

Some researches reveal that the use of the Internet has rapidly increased during the last decade. In 1998 there were twelve active terrorists websites, by 2003 this number increased to 2600, and in 2009 it is estimated that there were nearly 7000 active terrorists websites (Weimann, 2009).

5. INSIDE TERRORIST GROUPS

Bearing in mind the nature of terrorist activities and the scope of their consequences, it is obvious that not every juvenile can conduct these activities. Also, juveniles have to pass a kind of training and preparations in order to conduct terrorist acts by themselves. Close relations inside terrorist groups increase intimacy and create the atmosphere of obedience and respect for the leader.

In accordance with the aim of a concrete terrorist act, terrorists choose juveniles very carefully. So, the selection of juveniles is the first step, and in addition to juveniles' intelligence and enthusiasm, it is very important that they can blend in with the crowd (Singer, 2006, p. 127.). After the process of selection, juveniles are subjected to training, both physical and mental. The mental training is the most important, especially when the

juveniles' mission is to carry out a suicide attack. This training includes intense mental preparation, indoctrination, studying the texts that glorify sacrifice and ease the fear of death. Hours before the attack are spent in prayer and in recording wills and farewell messages on video or audiotapes. These videos are later used for new generations of recruits and as insurance that the bomber will carry out the attack; otherwise, he would be humiliated (Singer, 2006, pp. 127-129.).

6. STATISTICS

Security Council Secretary-General and Special Representative of the Secretary-General for Children and Armed Conflict submit annual reports on the issue of armed conflicts and their impact on juveniles. The impact of terrorism on juveniles around the world is analysed in some of these reports, with a special focus on different aspects of this increasing problem. As these reports are evidence-based and proved by field investigations, we consider them reliable and for that reason we will present the data contained in these reports.

According to the Annual Report of the Special Representative from 2009 (Special Representative of the Secretary-General, 2009, par. 41-43.), terrorist acts committed during conflicts in Iraq, Afghanistan and in the occupied Palestinian territory caused a lot of damage to juveniles. Terrorist attacks are directed against civil population and civil objects, and children and schools within them, constituting grave breaches of human rights in that way. But, children are also used all the time to perpetrate these attacks, because they can be more easily forces to act and they are less noticeable. Also, children are recruited and trained as suicide bombers, and used as human shields, decoys in suicide car bombings, or to transport improvised explosive devices. The other side of the problem is the impact of counter-terrorism on children. Namely, counter-terrorism measures also target juveniles, for example, through arrest and detention of juveniles because of their alleged participation in terrorist activities or associations with terrorist groups. Many of these children are detained without respect for their procedural rights according to international standards of juvenile justice.

In its Report from 2015 (Special Representative of the Secretary-General, 2015, p. 4.), in the section on emerging issues and challenges, Special Representative points to the fact that terrorist groups have benefited from advantages in technology, which have facilitated their rapid growth and led to the expansion of their territorial control, very often across national borders. The response to this development, embodied in counter-terrorism operations, has caused many children to be killed, maimed, and their homes and schools destroyed. Furthermore, terrorist groups regularly recruit juveniles from around the world using propaganda on the Internet and social media. The attention should be given to the recruitment networks of terrorist groups, with the aim of preventing them. Education of juveniles on this topic could be a very useful means of prevention.

This problem is also addressed in the next Report from 2016 (Special Representative of the Secretary-General, 2016), stating that juveniles continue to be severely affected by extremist violence and are often the direct targets of acts intended to cause maximum civilian casualties and terrorise communities. The recruitment of juveniles presents the

prevalent concern. Social media also continues to be used for purposes of propaganda and to encourage recruitment of children.

The Final Report on Recruitment and Radicalisation of School-Aged Youth by International Terrorist Groups, prepared for the U.S. Department of Education, Office of Safe and Drug-Free Schools (Homeland Security Institute, 2009), includes the analysis of the recruitment of juveniles by the following terrorist groups: Hamas and Hizballah, Al-Qaeda in the Islamic Maghreb (AQIM), Al-Qaeda and Affiliated Groups, Euskadi Ta Askatasuna (ETA) and Jemaah Islamiyah (JI).

Hamas and Hizballah strive to recruit and radicalise juveniles through active campaigns in schools, youth camps and mass media, including TV, the Internet and radio, where their activities are extreme. Juveniles are used to fill the ranks of these terrorist organisations, and carry out suicide attacks and conduct other terrorist activities. Also, they are used as human shields because these terrorist organisations know that Israeli soldiers are prohibited to shoot at children. By recruiting and radicalising juveniles as young generations, Hamas and Hizballah are establishing societal support for future operations. These terrorist groups start with recruitment at an early age, even when children are in kindergarten, and strive to gain their support and prepare recruits for future membership. They control the whole educational system, and follow their recruits all the way to college. Schools provide education that is in accordance with terrorist groups' ideologies and beliefs and also provide physical training in order to prepare juveniles for future groups' activities. Both groups sponsor summer-camps and other extra-curricular activities for juveniles. Mass media is also used for ideological purposes, where juveniles can watch cartoons and play video games that promote violence against the West. These groups have their own TV and radio stations that are used for ideological purposes and in order to recruit as more members as possible.

Jemaah Islamiyah uses Islamic schools and universities as a recruiting pool, and strives to radicalise recruited juveniles. Some of the members of this terrorist group are former students and/or instructor of these schools and universities. This terrorist group is well known for its strong familiar relations which means that juveniles often follow their relatives and join the group, and in that way the group maintains a strong and unified support in community.

Al-Qaeda and Affiliated Groups use a broad range of tactics and messages to recruit and radicalise juveniles. These groups conduct their activities all around the world, but mostly in Afghanistan, Pakistan, Iraq and the UK. Among European countries, the UK has encountered the problem of juveniles recruited by terrorist groups, because these groups methodically and intentionally target juveniles across the UK. For example, Al Qaeda recruited juveniles as young as 15 and used them for a deliberate campaign of terror in the UK, and for carrying out acts of terrorism. The reason why Al-Qaeda is looking for young recruits from Western countries is obvious – their familiarity with the language, culture and appearance. The juveniles who would not arouse any suspicion when standing beside ordinary people, are necessary for Al-Qaeda to conduct its terrorist activities against the West. The research shows that UK universities are of a particular importance, because nearly 30 terrorist groups have been identified at different campuses. In conflict zones in

Afghanistan, Pakistan and Iraq, Al-Qaeda has cleverly used situational factors, such as personal grievances and poverty, to recruit and indoctrinate juveniles. The most used method of recruitment is by kidnapping or other means of force. Juveniles are often used to carry out suicide bombings. In these countries juveniles are seen as new generation of Mujahidins, and there is a lot of evidence showing juveniles taking part in terrorist activities.

Al-Qaeda in the Islamic Maghreb is an active terrorist organisation not only in Maghreb region, but in Europe as well. Here, schools do not play significant roles in recruitment and radicalisation of juveniles; instead, mosques and the Internet are used for these purposes.

Euskadi Ta Askatasuna has traditionally been a youth organisation and it is now recruiting even younger members. These members participate in protests, riots and street violence.

Among European countries, beside the UK, the Netherlands also has a problem with recruitment and radicalisation of juveniles. This is the case within immigrant population, with young second and third-generation of Muslims from Morocco. Radical mosques, some Islamic schools and the Internet are being used as recruiting base.

7. CONCLUSION

It is this characteristic of terrorism – its 'chameleon nature' – that can be correlated with the global trend of recruiting juveniles to conduct acts of terrorism. Increased international cooperation in the fight against terrorism has forced terrorists to find new ways of acting. The solution has been found in the recruitment of juveniles and their use for terrorist activities. The reason is clear and obvious – juveniles could easily blend into the crowd and they arouse less suspicion than adults. There is, however, the other side of the problem – juveniles joining terrorist groups and their engagement in terrorist activities, both on a voluntary basis.

In order to address the problem of juveniles recruited by terrorist groups and used to conduct terrorist activities, it is essential to understand aetiology and phenomenology of the problem, as well as psychophysical characteristics and maturity of juveniles. The comprehensive analysis and understanding of the phenomenon is required. This means that it should be clear why terrorists recruit juveniles, why juveniles join terrorist groups on a voluntary basis, for what purposes and tasks terrorists use juveniles, and what the role of juveniles' psychophysical characteristics and maturity is.

Research has shown that terrorists recruit juveniles for many different reasons, e.g. to *boost their visibility*, as means of propaganda, to shock the public, to show the power and the ruthlessness of the group, because in some countries there are more juveniles than adults, for economic reasons, since they are easier to intimidate and control due to their juvenile mental and physical capacities, because it brings some tactical advantages to terrorist groups etc.

There are also many reasons why juveniles join terrorist groups on a voluntary basis, like: religious motivations, economic motivations, because of indoctrination, ideological education and other means of imposing attitudes and beliefs, all through schools and other

forms of formal education, social environment like violence in everyday life, personal reasons like a loss of a family member or a close friend, moral outrage, ideology, revenge, patriotism, financial incentives, religious incentives, prestige, as well as a sense of purpose, meaning and identity.

Once recruited, the juveniles receive intensive physical and mental trainings, after which they are ready to conduct a terrorist act. The researches have also shown that they are mostly used to carry out an act of suicide bombing.

One new characteristic of a terrorist method of recruitment is finding new juvenile recruits online. Earlier, terrorists used meetings and personal approaches and connections in order to find, recruit and indoctrinate juveniles, but now, with the advance and development of the Internet and social networks, they can achieve the same goals online, by acting faster, easier, from a remote distance and anonymously. Furthermore, these goals can be achieved in a wider context and with far-reaching consequences, because nowadays almost every juvenile uses the Internet or some social network. So, it can be said that the Internet and social networks make the terrorists` assignments more easily to accomplish – they can operate by sitting in the chair.

8. REFERENCES

Assembly, U. G. (2000). International Convention for the Suppression of the Financing the Terrorism.

Brett, R. (2002). Juvenile justice, counter-terrorism and children. Children and Security, 29-36.

Institute, H. S. (2009). Recruitment and Radicalization of School-Aged Youth by International Terrorist Groups. Arlington: Homeland Security Institute.

Kaseze, A. (2005). Međunarodno krivično pravo. Beograd: Beogradski centar za ljudska prava.

Meillahn, M. (2008). The Strategic Landscape: Avoiding Future Generations of Violent Extremists. Strategic Insight, 1-22.

Miladinović, A., & Petričević, V. (2012). Kriminogeni aspekt društvenih mreža. Retrieved from Academia: http://www.academia.edu/10138697/Kriminogeni_aspekt_drustvenih_mreza

Rosen, D. (2005). Armies of the Young: Child Soldiers in War and Terrorism. New Brunswick/New Jersey/London: Rutgers University Press.

Secretary-General, S. R. (2009). Annual Report on Children and Armed Conflict. United Nations.

Secretary-General, S. R. (2015). Annual Report on Children and Armed Conflict. United Nations.

Secretary-General, S. R. (2016). Annual Report on Children and Armed Conflict. United Nations.

Singer, P. (2006). Children at War. Berkeley/Los Angeles: University of California Press.

sources, I. s. (2003, January 14). The exploitation of children for terrorist purposes. Retrieved from Likoed Nederland: https://likud.nl/2003/01/the-exploitation-of-children-for-terrorist-purposes/

UNODC. (2017). Handbook of Children Recruited and Exploited by Terrorists and Violent Extremist Groups: The Role of the Justice System. Vienna: United Nations.

Weimann, G. (2009). The Internet as a Terrorist Tool to Recruit Youth. Youth Recruitment & Radicalization Roundtable. Arlington.

Бановић, Б. (2007). Тероризам у праву Европске Уније. Правни систем Србије и стандарди ЕУ и Савета Европе, pp. 145-160.

Милекић, В. (2013). Фејсбук, приватност и криминалитет: међусобна повезаност, условљеност и друштвена реакција. Социјална мисао, 167-180.

UDK 351.78
https://doi.org/10.18485/fb_ic4hs.2018.12

PERSONALISED SECURITY: A STEP TOWARDS APPLIED HUMAN SECURITY

Savvas E. CHRYSOULIDIS [*], Phaedon KYRIAKIDIS [**]

Abstract: 'Human security' as a term was first introduced in the United Nations Human Development Report in 1994[1]. The after-effect of the report was the ascertainment that the state's security did not at the same time achieve individual empowerment and security of people residing in its territory. Adjunct to the introduction of the term Human Security was the decisive shift of the centre of gravity in the field of security, from the state (state-centric) to the human (people-centric)[2]. As a result, the subject of human security is the individual people, not the state.

A first important step in this direction is the redetermination of the threats (new and old ones) that contemporary man is facing and managing, both those which emanate from the physical but evenly the human environment.

The purpose of the article is to highlight the use of new technologies to further strengthen human security as they now provide the toolbox to achieve the idealisation and deepening of the human-centred orientation of human security into the personalised security.

Personalised human security refers to the safety that assesses the geospatial characteristics of each person and applies accordingly to these. Each person has a unique geospatial profile (identity) that is spatio-temporal and formed both by the natural environment in which a person operates and interacts, and by the culture that the person advocates taking into account its continuously-changing nature.

From the above, the necessity arises to define the individual elements that compose this geospatial profile. Lastly, people who safeguard security are redefined, including individuals who are given the opportunity to contribute to their security, with a non-passive stance as it has been so far but active and in cooperation with other players that

[*] Ph.D. Candidate, Department of Civil Engineering and Geomatics, Cyprus University of Technology (CUT), chrysoulidis@hotmail.com

[**] Proffesor, PhD, Department of Civil Engineering and Geomatics, Cyprus University of Technology (CUT) , phaedon.kyriakidis@cut.ac.cy

[1] (United Nations Development Programme, 1994).

[2] ("Human Security in Theory and Practice: An Overview of the Human Security Concept and the United Nations Trust Fund for Human Security," 2009)

play a role. In addition, it is reported that during a threat the management focuses on the person / persons exposed to it and not only the threat.

Keywords: Human Security, geospatial profile, applied human security, personalized security, human security threats

1. INTRODUCTION

Humans, similar to animals, are born with inherent instincts, the most important of which is a survival instinct. The definition of the survival instinct is contained in the ability to know what to do to stay alive (2018, Merriam-Webster Dictionary). Contemporary humans belong to organised societies, where roles and responsibilities for human-related issues pertaining to survival and well-being are assigned to a specific group of people. This group of people has strict roles and responsibilities and constitutes the authorities of a state. Of utmost concern is the security of the citizens from all potential threats against humans, an issue that is commonly the state's responsibility around the world. This notion of security is called Human Security (HS) (Kofi Annan, 2001), and is considered as the ultimate form of all kinds of security concerns, as the other forms such as national – military security, have the success of HS as their final objective (Lincoln Chen, 1995).

This paper aims to contribute to the enhancement of HS by proposing a framework of increased human security awareness at the individual level, as contemporary humans typically forego their responsibility to protect themselves and hand over this role to state authorities. As state stakeholders do not often use new technologies and their capabilities to customize their services to individual needs and thus often operate inefficiently, this paper advocates the use of modern technologies by state authorities in order to achieve enhanced HS.

This modern approach to HS can only succeed via the exploitation of new technologies, as they produce a multiplier effect on the enhancement of human capabilities and on the mitigation of their vulnerabilities, so that individuals can be protected from critical (severe) and pervasive (widespread) threats and situations (Commission on Human Security, 2003). In this direction, a new term 'geospatial profile' should be introduced for the identification of customised security needs of individuals, which is expected to change the current state of mind in HS in two directions. First, by making individuals aware of threats and how to mitigate their impact on their lives, and second, by providing state authorities with new tools and data in order to offer personalised HS by saving resources and lives. In the long term, the geospatial profile will offer another crucial and essential factor for HS to succeed; namely, the active participation of every individual who can be influenced by a threatening situation, or who can influence this situation by his/her actions. The individual's passive behaviour dramatically reduces the possibilities to act/respond in the most efficient way during a threatening situation and deal with it. As a result, individuals should be repositioned as the main actors to safeguard HS, and their synergy should be counted upon along with all other stakeholders. Moreover, the introduction of a new approach aiming to understand individual behaviour in space and time, to personalise and specify weaknesses and capacities in order to provide the basis to evaluate and manage their participation in different ongoing situations, is considered an

imperative necessity. The introduction of a notion of geospatial profile is a prerequisite towards clarifying stakeholder relation to human security, as well as the type of securities connecting human security and corresponding threats. In addition, the undermentioned in paragraph 4, the introduction of the new term 'geospatial profile' offered in this paper, furnishes a tool (via the use of modern technologies) for the individuals to make it possible to change their role, to become more actively involved and finally to obtain security mentality.

2. HUMAN SECURITY STAKEHOLDERS

Numerous stakeholder theories and definitions (Economie & Bedrijfskunde, 2008) describe in a holistic way the term HS, as opposed to other terms, such as an actor (actors are always stakeholders but stakeholders are not always actors) or a role player. Primarily the term stakeholder was devised and introduced for organisations management and general business environments, but later was used in other realms, such as security. Edward R. Freeman, who is considered the "father of the stakeholder concept" (Fontaine, 2006) published many definitions, one of which is "Any group of individuals who is affected by or can affect the achievement of an organisation's objectives" [Freeman & McVea, 2001 (Freeman, 1984, pg. 5)]. This definition could be modified within a HS perspective, to become "any individual, group (made up of people who share a common interest) or organisation which can be influenced by a project or can influence this project", where the term *project* could pertain to any kind of issue or state.

Within the context of the most widely known theories about stakeholders (Donaldson & Preston, 2018), it is critical to understand how each stakeholder behaves and to understand his/her actions, roles and responsibilities, as well the ethical principles within the objectives of the organisation the stakeholder belongs to.

Stakeholder mapping

States around the globe have many differences due to different historical transitions in political, social, environmental, economic, military and cultural systems they operate in. For this reason it is impossible to identify similar (in terms of a name or role) stakeholders for different states. However, an overarching link is the common threats that human citizens of different states must deal with, and on this basis a different approach to emergencies and other security issues should be established using all the existing theoretical backgrounds, to identify the proper stakeholders involved in each different situation, irrespective of the differences between states. This different approach focuses on the security of human life, by monitoring the position of each individual, independently of the kind, of the threatening situation or its evolution. All relevant stakeholders are properly mapped according to how the lives of the individuals are possibly affected due to their position with relation to the threat. For instance, in a fire emergency situation, where one is monitoring the threat (fire), the proper stakeholders are the firefighters, and their role is clearly to extinguish the fire. The case of this fire causing an electricity failure, however, could put traffic lights out of order and thus cause several car accidents, possibly causing deaths that the fire itself would not have caused directly. According to this new approach,

which calls for monitoring individuals and not the fire (threat) itself, the relevant stakeholders (traffic police, electricity company employees) will be more efficiently involved, focusing on the synergistic monitoring of the position of individuals in connection to the threat, instead of monitoring the threat alone.

Stakeholder mapping can be addressed into two contexts, national and international. In most states, national stakeholders are civilian government agencies (health, transportation, education, and many other agencies), security sector (military, police, firefighters, intelligence services, justice and rule of law institutions), non-state armed groups, business sector, civil society (local religious institutions, local universities, and community-based organisations), media and non-governmental organisations (NGOs). International stakeholders could be international organisations (the UN, the World Bank, the International Monetary Fund), intervening states, contractors[3], humanitarian organisations (UN humanitarian agencies, the Red Cross/Red Crescent Movement, humanitarian non-governmental organization), international non-governmental organizations (NGOs) and transnational non-state armed groups (Schirch, Lisa, 2016). The common point for all stakeholder, regardless of states and roles, is the fact that their cornerstone is the human being itself.

Stakeholder roles and responsibilities

Governments retain the primary role and responsibility for their citizens (United Nations General Assembly, 2012). Stakeholder roles and responsibilities are involved in response to various pressures and influences according to stakeholder behaviours and cultures, as a result of facing multifarious threats caused by a continuously changing complex environment. This implies that stakeholder roles and responsibilities are not static or immutable. New or old threats (with new different impact) demand that we reconsider the roles and responsibilities, such as the involvement of the armed forces to manage additional threats beyond national defence (Krupanski, 2002). The most efficient way to identify primary and secondary stakeholders, in order to organise and share roles (first responders, coordinators) and responsibilities, is to follow a top-to-bottom approach. Threats are placed on the top of the pyramid and stakeholders are placed at the bottom. Secondly, the impact of each stakeholder should be identified in this pyramid, according to their power and capabilities (Mayers, 2005) in each specific moment and situation. Moreover, impact should be classified as positive, negative or neutral. Stakeholder behaviour can be delineated investigating past actions, studying similar situations in order to analyse their actual behaviour and find potential cooperation (Fontaine, 2006). Beside this, a constructive and logical explanation can report on why specific stakeholders act in a particular way. Key stakeholders remain the individuals, as they constitute the core of HS and the cell of each organisation. It is critical to know how they act in emergencies and in other incidents related to their security, by understanding their responsibilities in fulfilling their roles. The empowerment of HS is only possible via the change of individuals'

[3] Contractors, also known as private military corporations (PMC), private military firms (PMF), or private military or security companies.

mentality[4] (Javaid, 2013). In a fire incident, for example, the main difference between firefighters and the individuals who are in danger is the different way of thought (mentality), as firefighters are well trained and prepared, given their role and responsibility, to save people. A person, on the other hand, with no security mentality, acts passively, performing the role of a victim, without feeling any responsibility for the outcome of the ongoing situation, even if this affects his/her own life.

3. TYPES OF HUMAN SECURITY – THREATS

The term *security* was first introduced by Cicero and Lucretius referring to a philosophical and psychological state of mind, or the subjective feeling of freedom from sorrow (UNU-EHS, 2005). Nowadays, the term *security* is more often used in connection with the phenomenon of globalisation (Fukuda-Parr, 2003). Apart from academic research, policymaking stakeholders and organisations related to the security domain also focus on the global dimension of security. This paper aims to make a step forward for human security, by moving away from people-centred HS to personalised HS, and from the global focus to the personal focus, beyond the community or local level. However, the main concept remains the same. The ultimate purpose of human security is the protection and empowerment of individuals from all threats that are beyond their control[5].

Types/Dimensions of Human Security

The Human Development Report (HDR) of 1994[6] introduced seven main types/dimensions of security within which threats can be categorized; these are economic, food, health, environmental, personal, community, and political security. However, the question of 'security' was once just a political and social one, but today it is becoming more cultural (Watanabe, 2018). Of course, the concept of culture is not new, but human cultural insecurities[7] are recently taken into consideration for causing tensions, hostilities and general threats to human beings. Therefore, another type of security should be introduced in order to succeed in integrated management of HS. This type is Cultural Security (Alkire, 2003), the eighth type/dimension of HS. Strong approval of the importance of the cultural dimension of human security is corroborated by the establishment of UNESCO (UNESCO, 1995) and the number of states which recognise and participate in this international organisation under the United Nations.

Human Security threats

Four security dangers can be distinguished, and these are: threats, challenges, vulnerabilities and risks (Brauch, 2011). Risks are considered as the lowest level of dangers, while threats are the highest. Challenges are the escalation level between threats

[4] The term *security* introduced by Cicero and Lucretius refers to a philosophical and psychological state of mind, this is the security mentality I referred to, the state of mind.

[5] Ibid. p. 7

[6] Ibid. pp. 24-25

[7] Ibid. pp. 17-32

and risks, and vulnerabilities are the weaknesses that expose an organisation to risks. Threats are the last level of security dangers that affect directly human beings' livelihood and empowerment[8]. A list that includes all the threats against human security is almost impossible to be compiled and might be needless. New threats are being continuously recorded as the technological evolution is ongoing. New threats, like cyberattacks, data fraud or theft, climate change and fake news are only some of those[9]. The categorisation of the most widespread and severe threats under the eight types of security mentioned above could be a starting point in order to record the main threats and collect data, and find how individuals can protect and empower themselves. Some of the main threats that can be classified in eight types of security are: **economic security** (persistent poverty, unemployment), **food security** (hunger, famine, spoiled food), **health security** (deadly infectious diseases, unsafe food, malnutrition, lack of access to basic health care), **environmental security** (climate change, environmental degradation, resource depletion, natural disasters, pollution, water crisis), **personal security** (physical violence, crime, terrorism, domestic violence, child labour, fake news), **community security** (inter-ethnic violence, vandalism against public property, civil war), **political security** (political repression, human rights abuses, corruption incidents, war), **cultural security** (monuments – heritage disaster, art crimes, racism crimes, violation of cultural rights, religious and other culture-based tensions, genocide based on discriminations). The recording and categorisation of threats in the eight above mentioned types of security can be accomplished via the use of new technologies which are necessary for the implementation of the geospatial profile, details of which will be introduced in the next paragraph. The geospatial profile could provide individuals with the ability to increase their awareness of all potential threats, which, in conjunction with proper awareness of vulnerabilities and strengths, could help protect themselves more effectively and efficiently. The global point of view focuses on transnational threats (Patrick, 2006), such as military conflicts, terrorism and other (Report, 2018). Minor security issues that individuals might have to deal with every day are secondary in importance for governmental authorities, but can have a huge negative impact on the lives of individuals.

4. GEOSPATIAL PROFILE

The main difference introduced in this new approach towards HS is the consideration of individuals separately, ensuring a customised (personalised) security, adapted to the personal, unique and dynamic needs of each individual. Until now, stakeholders in the security domain have treated individuals as a common, unified and indivisible whole, often called *a society* or *community*. This approach has a negative impact on how people 'perceive' their roles and responsibilities from minor to large-scale security incidents. Moreover, when planning the crisis response and risk management, individuals have a neutral or negative participation, because they are considered, from a policy-making standpoint, more as victims than as equally capable and critical stakeholders. If one takes

[8] Ibid. p. 7

[9] Ibid, Figure IV

into consideration that in the majority of incidents (from civil wars and hostilities to a wildfire or car accidents) individuals are by far the greatest part of the people involved, then it can be easily understood how they impact (by their neutral or negative contribution) the evolvement of the incident. Nowadays, new technologies such as Geoinformatics, Spatial Analysis, Geographic Information Systems, Data Science and Analytics provide the required toolbox to identify and analyse/model the characteristics of each individual in order to personalise his/her security. This policy change in the long term will redefine the role of individuals, responsibilities and their security attitude. The final purpose remains their protection and empowerment[10]. In what follows, we will introduce the Geospatial Profile (spatial identity), which refers to the characteristics/elements of each person, based on two pillars comprising the physical (natural) and human environment.

Geospatial profile characteristics/elements

The elements of the geospatial profile pertaining to the physical environment originate from studies on the vulnerability (Lukacs & Bhadra, 2012) and capacities (Hansford, Faleiro, Hughes, Marshall, & Wiggins, 2011) of individuals towards natural hazards (Papathoma-Köhle, Neuhäuser, Ratzinger, Wenzel, & Dominey-Howes, 2007), other physically-based emergencies and issues relevant to HS. Examples of such physical elements, which influence the way a person or group of people is affected by reducing or increasing the individual's capacities and vulnerabilities are: the precise position of a person – Coordinates, Elevation, Slope, Hydrology of the area, Weather, Land Cover – Land Use. Human environment elements arise mainly from the answer to the question: which factors affect the individual's decision-making process, and focus on the behaviour of one person or group of people mainly during crisis situations (Arru, Negre, 2017) and other threatening socio-economic phenomena. Examples of such human environment elements are: Socio-Economic Status (SES) [Age, Sex, Nationality, Religion, Residence Place, Level of Education, Civil Status (married with children, divorced etc.), Income (wealthy, car owner) and Occupation], Health Condition, Government Role (Civilian/Civil Protection/Local or Federal Enforcement/Armed Forces)[11]. The Geospatial Profile is dynamic, because its constituent elements change continuously over time (short and long-term ones). In addition, the Geospatial Profile is person-specific, since its constituent elements are unique for each person; in other words, the geospatial profile is considered as the spatio-temporal 'identity' of each human being. Moreover, under some parameterisation of the constituent elements, the geospatial profile could be used in an aggregate or mean sense to characterise groups of people, organisations, communities, regions and generally defined structures with spatial characteristics. Providing the capability/opportunity to an individual to be aware of his/her geospatial profile (specify vulnerabilities and capabilities), while at the same time becoming responsible for potential dangers (before they become threats), can be considered as a starting point for a person to acquire security mentality. For instance, one could visualise how an individual will act in

[10] Ibid, p.7

[11] Ibid, p.48-54

case of a flood, if one knows from his geospatial profile the hydrographic network, land cover, slope in relation to his/her position. On the other hand, this profile is expected to be of significant value to security authorities when they plan and execute their duties, along with elements like individual health condition, age, existence of car or not, or recorded history of similar incidents. Finally, with the implementation of the geospatial profile, the necessary data mentioned above (elements of physical and human environment) are collected from the source (from individuals who are influenced by a threatening situation) and for the first time the data will correspond to each person who has specific and recorded characteristics, solving the lack of observable and structural input data (Douglas, 2007). The timely and accurate data directly acquired from the source are expected to promote the analysis of a threatening situation in an efficient way, providing lessons learned for future exploitation and finally the involvement of all proper stakeholders and the mitigation of the final situation. Moreover, real-time recording of data could provide a useful database for further research on HS.

5. CONCLUSIONS

This article proposes ways in which new technologies can provide a framework to make the necessary transition from people-centred to personalised Human Security. It also advocates new roles and responsibilities for individuals in order to implement a new state of individual's mind, as the current state of individuals not acting responsibly (and not knowing what type of action to take) for their own security, is the main reason of the failures in HS, where every failure counts in terms of human lives. Novel approaches are needed to deal with new threats; otherwise, the repetition of previous failures is inevitable. A wide variation of HS definitions and approaches creates a question about whether the concept of human security can serve as a practical guide for academic research or governmental policy-making (Barnett et al., 2001). Applied HS can act as a bridge connecting the academic research with policy-making actors in the field. In this direction, as mentioned in the title of this paper, the geospatial profile provides the very first step towards personalised security and towards extending applied HS.

6. REFERENCES

Alkire, S. (2003). A Conceptual Framework for Human Security . *CRISE Working Paper* , *2*, 53.

Barnett, M., Beer, F., Brooks, S., Chan, S., Ciof, C., Drezner, D., Weiss, T. (2001). Human Security Roland Paris Paradigm Shift or Hot Air. *International Security*, *26*(2), 87–102. https://doi.org/10.1016/S0140-6736(11)61148-3

Brauch, H. G. (2011). Security Threat, Challenges, Vulnerability and Risks. *Coping with Global Environmental Change, Disasters and Security*, *5*, 61–106.

Commission on Human Security. (2003). *Human Security Now*. https://doi.org/0-9741108-0-9

Donaldson T. and Lee E. Preston. (Jan, 1995) The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications Source. Published by: Academy of

Management Stable URL: http://www.jstor.org/stable/258887 Accessed: 14-07-2018 15:31 UTC, Vol. 20, No. 1 (), pp. 65-91

Douglas, J. (2007). Physical vulnerability modelling in natural hazard risk assessment. *Natural Hazards and Earth System Sciences*, *7*(2), 283–288. https://doi.org/10.5194/nhess-7-283-2007

Economie, F., & Bedrijfskunde, E. N. (2008). Working Paper the Stakeholder Model Refined. *Journal of Business*, 1–46.

Fontaine, C. (2006). The Stakeholder Theory. *Management*, *1*(December), 37–44. https://doi.org/10.1057/9780230524224

Freeman, E., & McVea, J. (2001). A Stakeholder Approach to Strategic Management. *SSRN Electronic Journal*, *1*(01), 276. https://doi.org/10.2139/ssrn.263511

Fukuda-Parr, S. (2003). New Threats to Human Security in the Era of Globalization. *Journal of Human Development*, *4*(2), 167–179. https://doi.org/10.1080/1464988032000087523

Hans - Gunter B., UNU Institute for Environment and Human Security (UNU-EHS), Threats, Challenges, Vulnerabilities and Risks in Environmental and Human Security, (2005), p. 7.

Hansford, B., Faleiro, J., Hughes, D., Marshall, M., & Wiggins, M. (2011). Reducing risk of disaster in our community (Roots 9), 1–100.

Human Security in Theory and Practice: An Overview of the Human Security Concept and the United Nations Trust Fund for Human Security. (2009). *Un*, 1–45.

Javaid, M. A. (2013). The Psychology of Security. *SSRN Electronic Journal*, 50–79. https://doi.org/10.2139/ssrn.2342620

Kofi Annan. (2001). Definitions of Human Security - Millenium Report. *Global Development Research Centre* -, 1–10. Retrieved from http://www.gdrc.org/sustdev/husec/Definitions.pdf

Krupanski, A. S. ; M. (2002). Mapping Evolving Internal Roles of the Armed Forces Mapping Evolving Internal Roles of the. *The Geneva Centre for the Democratic Control of Armed Forces*, (ISBN 978‐92‐9222‐228‐4).

Lukacs, M., & Bhadra, D. (2012). Table of of contents. *Schriften Des Forschungszentrum Jlich Reihe Energietechnik*, *21*(November), 39. https://doi.org/10.1002/ejoc.201200111

Maude Arru, Elsa Negre. People behaviors in crisis situations : Three modeling propositions. 14th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2017), May 2017, Albi, France. Proceedings ISCRAM 2017 : Agility is coming ; 14th International Conference on Information Systems for Crisis Response And Management, pp.139-149, 2017. <hal- 01729057>

Mayers, J. (2005). Stakeholder power analysis. *Focus*, (March), 24. Retrieved from http://www.policy-powertools.org/Tools/Understanding/docs/stakeholder_power_tool_english.pdf

Papathoma-Köhle, M., Neuhäuser, B., Ratzinger, K., Wenzel, H., & Dominey-Howes, D. (2007). Elements at risk as a framework for assessing the vulnerability of communities to landslides. *Natural Hazards and Earth System Science*, *7*(6), 765–779. https://doi.org/10.5194/nhess-7-765-2007

Patrick, S. (2006). Weak States and Global Threats: Assessing Evidence of "Spillovers." *International Relations*, (73), 1–31. https://doi.org/10.1162/wash.2006.29.2.27

World Economic Forum Report 13th Edition. (2018). *Global Risk Report*. Retrieved from http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/the-global-risks-report-2018.pdf

Schirch, Lisa (editor). Handbook on Human Security: A Civil-Military-Police Curriculum. The Hague, The Netherlands: Alliance for Peacebuilding, GPPAC, Kroc Institute, March 2016.

UNESCO. (1995). Unesco 1945-1995: A Fact Sheet, 1–8. Retrieved from http://unesdoc.unesco.org/images/0010/001011/101118eo.pdf

United Nations Development Programme. (1994). Human Development Report 1994. *Human Development Report*, 226. https://doi.org/http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf

United Nations General Assembly. (2012). a/66/290, (October), 1–2.

Watanabe, Y. (Eds.). (2018). Handbook of Cultural Security. Cheltenham, UK: Edward Elgar Publishing. doi: https://doi.org/10.4337/9781786437747

UDK 351.753(430)
https://doi.org/10.18485/fb_ic4hs.2018.13

PERMISSION TO KILL? THE DISREGARD OF THE LEGAL REGULATIONS ON THE USE OF FIREARMS BY THE (BERLIN) POLICE AND THE ILLEGAL POLICE SHOOTING TRAINING

Oesten BALLER*

Abstract: Between 1990 and 2017, 276 persons died in Germany due to police shootings. In many cases, the victims were mentally ill; often they held a knife in their hands. Legitimisation of shooting via police law has become exceptional; the cases are justified as self-defence. Police training focusses on fast reactions. The first explanation, why there is a certain accumulation of legally dubious police lethal- shooting in Berlin, could be the unprofessional handling of the police with people in mental crises or mentally ill humans. The second explanation raises the question of whether a carried knife, which is either used for self-harm or threat, can justify a police firearm use in general and especially a life-threatening or lethal use of firearms.

Disregard of the legal powers of intervention and the rash appeal to the law of self-defence is the third explanation for the often lethal firearms use of the police. The biggest problem arises when the factors described above are combined. In the police shooting training, a distinction is made between a so-called "UZwG shot" and a "self-defence shot", and first of all a knife attack is simulated as a scenario during the self-defence shot and, secondly, a point-shot is trained in this case, then a lethal shot is fired, which finds no basis in law. This shall apply even if a lethal use of firearms is considered admissible in exceptional cases in the police legislation. In addition, the idea underlying the police shooting training that in all self-defence situations automatically a point-shot and thus a highly likely lethal shot are appropriate contradicts the applicable law. The analysis of police firearms use and police shooting training shows a frightening picture. A careless treatment of mentally ill people, the automatic grip on firearms, when the police opposite has a knife in his hand and the broadest negation of the legal basis for the police firearms use too often lead to the police lethal shots. In addition, statistics show almost only self-defence shots. Police shooting training provides an automatic mechanism that leads to the fact that the legal limits to the firearms use and police killings aiming at the vital triangle are almost

* Professor, PhD, Institut für Verwaltungsmodernisierung und Polizeireform in Mittel-und Osteuropa, Berlin School of Economics and Law, oesten.baller@hwr-berlin.de

inevitable. Remedy can only bring a professional training, which gives a lot of space in all situations of application of the range of options and, above all, the legal limits.

Keywords: police shooting, shooting training, self-defence, disoriented people, disregard of legislation

1. BERLIN POLICE ACT UNPROFESSIONALLY TOWARDS MENTALLY ILL OR BEHAVIOURALLY ABERRANT PERSONS

The fatal shots fired on 28 June 2013 inside the Neptun Fountain in central Berlin caused numerous disputes. A young male, obviously mentally disoriented, was found naked and with a knife in his hand inside the fountain. A police officer climbed the fountain and shot him dead on the spot. This event was the first culmination of a series of two similarly tragic events from previous years. On 6 October 2012, another mentally disoriented male, aged fifty, armed with an axe and two knives, was running along a street in Berlin Wedding. Excessive police violence, including gunshots, a police dog and massive application of pepper spray caused heavy injuries, of which the person shortly after died.[1] On 24 August 2011, the police were called to a supported living home to provide law enforcement assistance in a case where a female resident of this home was, by court decision, to be taken to psychiatric hospital. As police officers forced entry into the apartment, they detected a knife in the hand of the woman. Shortly afterwards, additional operating forces arrived and shot the woman dead in her apartment.[2] On 24 April 2014, RBB broadcast its documentary "Tödliche Polizeikugeln [Deadly Police Bullets]", which was the first to thematise the fateful consequences of police ignorance in dealing with mentally ill persons; at the same time it became known, what new tactics police were using in their operational and shooting training.[3] *Otto Diederichs'* statistics about fatal police shootings show a trend that in 2015 nine out of ten victims of fatal police shots were mentally ill or in a state of psychic crisis.[4]

A certain increase in the number of legally questionable fatal police shootings in Berlin may, according to the **first explanation**, be due to a frequent unprofessional police handling of individuals in psychic distress or mentally ill persons. This could be recognised and remedied, provided that, in domestic politics and within the police, there were any tendencies to halt this trend.

---

[1] Cf. Berliner Zeitung <http://www.berliner-zeitung.de/berlin/wedding-von-der-polizei-angeschossener-mann-tot-5824870>.

[2] Cf. Morgenpost <http://www.morgenpost.de/berlin/article105081709/Polizist-erschiesst-psychisch-kranke-Frau.html>.

[3] Cf. *Mats Kafke*, Führt das Berliner Schießtraining zu einem rechtmäßigen Schusswaffengebrauch durch Polizeiangehörige? [Does shooting training lead to legitimate use of firearms by the Berlin police?], Bachelor thesis at HWR Berlin, 2017.

[4] Bürgerrechte & Polizei/CILIP 111, October 2016, at 85; cf. also *Asmus Finzen*, „Wer mit einem Messer Polizisten angreift, muss damit rechnen, erschossen zu werden." Schlechte Karten für psychisch Kranke ["Knife-wielding police attackers must expect to be shot dead." Bad odds for the mentally ill] <http://apk-berlin.de/files/schusswaffengebrauch_gegen_psychisch_kranke_bei_polizei_final-1.pdf>.

2. DISREGARD OF LEGAL PROVISIONS AND RELEVANT COURT RULINGS

In almost all of the cited instances of mostly fatal use of firearms by police, the victim has employed a knife. The **second explanation** refers to this specific trend and poses the question, whether a knife used to endanger its carrier or to threaten another person would suffice to justify the police use of firearms in general or, in particular, a life-threatening or fatal use of firearms.

The specific provisions for the police intervention applicable to the Berlin police – as opposed to the relevant regulations in almost all other federal states, with the exception of Schleswig-Holstein, Mecklenburg-Vorpommern and Federal Law – initially do not provide rules for the lethal (final) rescue shot, as well as in e.g. Austria and in Switzerland.[5] Pursuant to Section 11 of the Use of Immediate Coercion Act (UZwG),[6] Berlin Police are authorised to shoot at persons in order to prevent them from committing a felony or a misdemeanour[7] while carrying or using firearms or explosives. Attempted suicide with a knife is neither prosecutable nor forbidden and therefore does not justify the police use of coercion and, even less so, of firearms. Threatening another person with a knife is deemed a misdemeanour and therefore justifies the use of firearms only under the condition that such act be committed with the obvious intent to inflict serious bodily harm or to kill. Infliction of bodily harm (Section 223 Criminal Code) and of bodily harm by dangerous means (Section 224 Criminal Code), where an attacker uses, e.g. a knife, are not felonies – the term 'felony' applies only to the infliction of grievous bodily harm and of bodily harm causing death (Sections 226, 227 Criminal Code). Pursuant to the established

---

[5] On problems of the final rescue shot in Germany cf. *Clemens Arzt,* Europäische Menschenrechtskonvention und polizeilicher Todesschuss – Zugleich eine Besprechung des Urteils des EGMR Makaratzis/Griechenland [European Convention on Human Rights and police fatal rescue shot - At the same time a discussion of the judgment of the ECtHR Makaratzis / Greece], Die öffentliche Verwaltung 2007, 230-237, *Heike Witzstrock,* Der polizeiliche Todesschuss [The police fatal rescue shot], Lang Frankfurt a.M. 2001; in Switzerland cf. *Gianni Giger*, Legitimation staatlicher Tötung durch den finalen Rettungsschuss – Rechtslage und Erkenntnisstand zum gezielten polizeilichen Todesschuss in der Schweiz unter Berücksichtigung rechtsvergleichender Aspekte und europäischer Standards [Legitimisation of state killing by the final rescue shot - Legal situation and state of knowledge on the targeted fatal shooting in Switzerland, taking into account comparative law aspects and European standards], Zürich: Schulthess Verlag, 2013; comparing these countries cf. *Thomas von Berg*, Der Finale Rettungsschuss. Ein internationaler Vergleich der verfassungs- und polizeirechtlichen Problematik am Beispiel Deutschlands, Österreichs und der Schweiz [The final rescue shot. An international comparison of the constitutional and police-legal problems with the example of Germany, Austria and Switzerland], Bachelor thesis at HWR Berlin, 2016.

[6] Gesetz über die Anwendung unmittelbaren Zwanges bei der Ausübung öffentlicher Gewalt durch Vollzugsbeamte des Landes Berlin [Law on the use of immediate public coercion by enforcement officers of the State of Berlin (UZwG Berlin)], 22.06.1970, with subsequent amendments. Cf. to this law: *Baller/Eiffler/Tschisch*, ASOG Berlin. Zwangsanwendung nach Berliner Landesrecht – UzwG -, Boorberg, Stuttgart 2004

[7] According to Section 12 German Criminal Code [Strafgesetzbuch (StGB)], in the version promulgated on 13 November 1998, with subsequent amendments:

(1) Felonies are unlawful acts punishable by a minimum sentence of one year's imprisonment, and

(2) Misdemeanours are unlawful acts punishable by a lesser minimum term of imprisonment or by fine.

judicial practice of the Federal Court of Justice, a decisive criterion is the particular dangerousness of attack, such as may result from a life-threatening action of the attacker.[8] Holding a knife and not dropping it when requested by the police, or moving towards the police with a knife in hand and not stopping upon the request does not comply with the requirements stated above, and yet the reason for why firearms were used was seen, as shown in the examples cited above, in such very circumstances.

Whilst Federal Law as well as the state laws of Baden-Württemberg, Hamburg and Saxony employ regulations similar to Berlin, most other states authorise the use of firearms also in situations where present danger to life or health must be averted.[9] Such additional prerequisite does not apply, where a knife is used for inflicting self-harm, or is just being carried in hand. There is no unequivocal legal understanding of situations where individuals with knives move towards police officers. The law, here, is intrinsically contradictory insofar, as the same circumstances may look different, either in view of imminent danger to life or health, or of the basic offences described earlier. Whichever interpretation to choose, the use of firearms is restricted by law to the effect, that the purpose of any shot must be the inability to attack, i.e. the shot must aim at the target person's legs. An intended lethal shot would accordingly be illegitimate, since, pursuant to provision governing the 'final rescue shot', a lethal shot is permissible only in order to avert imminent danger to life or imminent danger of grievous bodily harm. This is roughly analogous to the delimitation between a felony and a misdemeanour within the statutory offence of causing bodily harm. Although the enlarged regulations in force in most of the federal States aim at self-defence situations, many of them provide, as an additional option, that lethal shooting is permitted also in cases of self-defence and duress.[10] The law does not state unambiguously what kind of restrictions will apply to the self-defence shot.

Therefore it is not only the police, but, in many cases, also the prosecutors who regularly play the 'self-defence card', when they are to justify the police use of firearms, including the police fatal shooting. For 2012, statistics compiled by *Clemens Lorei* list 35 instances of the police use of firearms against persons, 34 of which were substantiated as self-defence or aversion of danger to health or life,[11] whereas in 2015 four shots at persons to prevent criminal offences and one shot to thwart escape appear little in comparison with the large number of self-defence shots, including shots to avert danger to health or life.[12] According to the official Firearms Statistics of the Deutsche Hochschule der Polizei [German Police University] in 2016, all cases of police firearm use were justified by self-defence.[13]

---

[8] Cf. BGH NStZ 2014, 477, BGHSt 57, 183, and BGH NStZ 2012, 207.

[9] Cf. § 67 Abs. 1 of the Police Law of Brandenburg [Gesetz über die Aufgaben, Befugnisse, Organisation und Zuständigkeit der Polizei im Land Brandenburg (Brandenburgisches Polizeigesetz - BbgPolG)], 19.03.1996, with subsequent amendments.

[10] The Federal government, Baden-Wuerttemberg, Hamburg, the Saarland, Saxony and Saxony-Anhalt rightly renounce this rule.

[11] Cf. <http://www.schusswaffeneinsatz.de/Statistiken_files/Statistiken_1.pdf>

[12] Cf. <http://www.schusswaffeneinsatz.de/Statistiken_files/Statistiken.pdf>.

[13] Cf. Welt <https://www.welt.de/politik/deutschland/article166675828/Wie-oft-deutsche-Polizisten-wirklich-zur-Waffe-greifen.html >.

All the options provided by the police powers of intervention, i.e. the use of firearms to prevent a criminal offence, to thwart escape, or to prevent freeing of prisoners clearly specify restrictions as to the 'whether' and 'how' in the use of firearms. The plea of self-defence, thus, is used quasi as a free ticket for the police use of firearms in general or of lethal shooting, in particular. There is a controversial debate about whether the police are at all entitled to plead their right to self-defence.[14] But it is more than questionable whether the police adherence to the Law (Section 20 Para 3 of the German Basic Law) allows for such differentiation that would leave it up to the individual police officer to shoot or even to fire fatal shots. However that may be, disregard for the legal powers of intervention and the rash claim of the right to self-defence serves as the **third explanation** for the fatal use of firearms by police.

3. QUESTIONABLE METHODS IN POLICE SHOOTING TRAINING

Pursuant to the Section 20 Para 3 of the German Basic Law[15], the executive power is bound to adhere to the Law. The sole purpose of the use of firearms by the police shall be, pursuant to the Section 9 Para 2 UZwG, to disable a person from attacking or fleeing. Both these requirements together constitute core milestones for the police shooting training. Firstly, such training must be precisely aligned with the legal framework and, secondly, the restriction to disabling attack and escape can be sustained only, provided that training is regular and is designed accordingly. In Berlin, the police shooting training is only partially in accordance with these two requirements, the same being true for other Federal States.

Police shooting training is based on the PDV 211[16]. With regard to the issue discussed here, it is important to consider that the trained shooting techniques distinguish between the so-called 'sighted shot (in German: Visierter Schuss)' and the so-called 'unsighted shot (in German: Deutschuss) '. In a sighted shot, the shooter takes aim, looking with one eye through the iron sight of his gun. This technique enables a shooting which is precise enough to comply with the legal requirements and restrictions, first of all the restriction to achieve disability to attack or to escape. Where, under pressure to act, the shooter takes aim less precisely, the result will be a 'roughly sighted shot (in German: Grob visierter Schuss) '. For an unsighted shot, which enables a fast response to an attack, the shooter

---

[14] Cf. <https://strafrecht-online.org/problemfelder/at/rw/notwehr/hoheitstraeger/>; *Hillenkamp/Cornelius*, 32 Probleme aus dem Strafrecht. Allgemeiner Teil [32 Problems in Criminal Law. General Part], 15. Ed.,Vahlen, Munich 2017, 43; dissenting *Andreas Hoyer*, in: Deiters/Hoyer et al, SK-StGB. Systematischer Kommentar zum Strafgesetzbuch [Systematc commentary on the Criminal Code], Vol. 1, 9. Ed., Carl Heynanns, Köln, 2017, § 32 para 15; affirming *Volker Erb*, Münchner Kommentar zum Strafgesetzbuch [Munich Commentary on the Criminal Code] , Bd. 1, 3. Ed., C.H. Beck, München 2017, para 189 ff.

[15] Grundgesetz für die Bundesrepublik Deutschland (GG) [Basic Law of the Federal Republic of Germany], 23.5.1949, with subsequent amendments.

[16] Polizeidienstvorschrift (PDV) 211 „Schießtraining in der Aus- und Fortbildung" [Internal Police Regulation „Shooting Training in Education and Further Training"] in its currently applicable 2005 edition (as per 08/2015).

holds the weapon in both hands, captures the target with both eyes open, points and shoots without sighting. This technique is applied with little or no regard for the described restrictions on the use of firearms.[17]

The details of the police shooting training are specified in various codes of practice, official instructions, edicts, manuals and directives, of which hardly any are publicly available. The sole exceptions are Hamburg and Hessen. Hamburg, which, besides Rhineland-Palatinate, is the only Federal State that has a modern transparency act, provides public access to the Instructions on the Hamburg police further shooting training.[18] Both these instructions and the annual shooting programme contain no specific information on the shooting techniques trained. Here, training for shooting in self-defence situations is just a component of the training programme and, as such, provides an indirect reference to the training of unsighted shots. In Hessen, the Edict on operational training has been published by the Hessen police authority.[19] This document explicitly mentions the training of 'unsighted shooting'. The descriptions of the modules for basic shooting training given in the manuals for the police bachelor study programme at the Hessische Hochschule für Polizei und Verwaltung draw a clear distinction between the defined shooting and the unsighted shooting.[20] This is not the case with the respective module description in use in Berlin.[21] Both of these, however, specifically refer to a shooting avoidance training. In any case, the publicly available sources demonstrate that the cited shooting techniques are standard content of the police shooting training in Germany.

What are then, in terms of their effects, the main differences between the 'sighted shot' (defined shooting) and the 'unsighted shot'? When performed in strict compliance with the Immediate Coercion Act, sighted or defined shooting at persons generally aims at the target person's arms and, first of all, his legs. This is similarly stated in sub-paragraph 38 of the Manual for the Berlin enforcement officers dated 20 June 2016[22], supplementing Section 9 of the Immediate Coercion Act. Under these conditions, survival is, at least,

---

[17] Cf. *Mats Kafke* (note 3), at 8.

[18] Dienstanweisung für die Schießfortbildung der Polizei Hamburg [Official instruction for further shooting training of the Hamburg Police], Az.: 11.88-12.

[19] Erlass über das Einsatztraining bei der hessischen Polizei [Edict on operational training of the Hessen Police],17.12.2013, Hessisches Ministerium des Innern und für Sport, Landespolizeipräsidium LPP 41 - PE - 7 t 10/8 e 12 05 – Gült.-Verz. 3100 –, StAnz. 4/2014 S. 76.

[20] Cf. the Manual for the uniformed police <https://www.hfpv.de/sites/default/files/public-type-files/04-Modulbuch_SchuPO_2016-09.pdf>.

[21] Studienordnung des Bachelorstudiengangs Gehobener Polizeivollzugsdienst des Fachbereichs Polizei und Sicherheitsmanagement der Hochschule für Wirtschaft und Recht Berlin [Study Regulations of the Bachelor Degree Programme Advanced Police Service of the Department of Police and Security Management of HWR] (StudO/Pol B.A.) 12.04.2016, last updated 15.11.2016, <http://www.hwr-berlin.de/fileadmin/downloads_internet/Mitteilungsblaetter/2017/Mitteilungsblatt_06-2017_FB_5_Studienordnung_Polizeivollzugsdienst.pdf>.

[22] Ausführungsvorschriften für Vollzugsdienstkräfte der Polizeibehörde zum UZwG Bln. (AV Pol UZwG Bln) [Executive regulations for the Berlin enforcement officers Immediate Coercion Act], 20 June 2016 <https://www.berlin.de/sen/inneres/sicherheit/polizei/rechtsgrundlagen/ [Legal basis]>.

possible, provided that first medical aid is carried out timely. With unsighted shooting, the situation is completely different. Here, the weapon aims at the so-called 'vital triangle', which comprises the chest and its vital organs: the heart and the lungs. Hits in this area usually cause death, especially due to the impact of the deforming ammunition the Berlin police have been using for a long time.[23]

4. FATAL CUMULATIVE EFFECTS

The biggest problem arises when the above described factors are brought together. Considering that at the core of the police shooting training lies a distinction between a so-called 'defined shot' (according to legislation) and a 'self-defence shot'", and that, firstly, the scenario underlying the self-defence shot is a simulated knife attack, while, secondly, in that case, unsighted shooting is trained, then training *de facto* aims at lethal shooting that has no basis in law. This is true even where State police legislation deems lethal use of firearms to be permissible in exceptional situations. Contradictory to the governing law is also the underlying idea in police shooting training, according to which in any self-defence situation unsighted shooting – in other words: lethal shots – is appropriate.

Section 32 Para 2 of the Criminal Code defines self-defence as 'any defensive action that is necessary to avert an imminent attack on oneself or another'. Within the framework of self-defence, such defensive action is deemed to be necessary, as, on the one hand, gives reason to expect immediate abortion of attack and, on the other hand, is the most sparing, i.e. the least harmful means to avert attack.[24] Such ban on excessive defence springs from the principle of proportionality. The principle of proportionality is constitutive of the legal regulation of police use of firearms. Section 4 of the Immediate Coercion Act commits enforcement officers to always give priority to measures with the least adverse impact on target persons. In addition, the law forbids the use of coercive action, where inflicted damage is evidently disproportionate to the envisaged success. Section 9 sub-paragraphs 1-3 of the Immediate Coercion Act govern the use of firearms by orders and prohibitions, of which all express the principle of proportionality. All of these restrictive provisions seem to be negated by the cumulative effect of the factors described above.

Another aspect is that the plea of self-defence is often made in classical police officers operative situations. As a result, the legal commitment is in such cases often stronger than in exclusively private self-defence situations. In police legislation, the understanding prevails that justifications, such as self-defence, provide no rationale for the exercise of intervention powers[25]. From this point of view, the commitments emanating from the exercise of legal powers interfere with the requirements for self-defence actions performed

---

[23] Cf. *Oesten Baller*, Neue Munition für die Polizei – Eine von Schein-Sachzwängen dominierte Diskussion [New ammunition for the police – a discussion dominated by bogus necessities) Bürgerrechte & Polizei/CILIP 65 (1/2000], 70.

[24] Cf. Lackner/*Kühl*, Strafgesetzbuch: StGB. Kommentar [Criminal Code. Commentary], 29. Ed., C.H. Beck, München 2018, § 32, paragraph. 9; *Andreas Hoyer* (note 14), § 32 paragraph 58 ff.

[25] Cf. for many others *Wolf-Rüdiger Schenke*, Polizei- und Ordnungsrecht [Police and regulatory law], 9. Ed., C.F. Müller Verlag, Heidelberg 2016, paragraph 40, at 562.

within the scope of sovereign duties.[26] When further following the understanding that a police officer in such a situation acts not as an official, but, instead, as a private person,[27] police shooting training appears to be even more questionable.

The first question is, whether it is legitimate to publicly fund training for private purposes. A positive answer can only from a synoptic point of view. When 'private' self-defence directly relates to the performance of police duties, it should be permissible to train police officers also for those situations, where they are confronted with unexpectedly high personal risk. Another question, however, asks, whether the behavioural pattern 'self-defence situation - unsighted shot - vital triangle' should become a standard training component. The answer is clearly negative, since the absolute denial of legal commitment – no matter, whether it derives immediately from self-defence rights, or from the police's right of coercion – implies a kind of legal nihilism that is incompatible with the legal commitments stated in the Section 20 Para 3 of the German Basic Law.

5. CONCLUSION

The analysis of police use of firearms and police shooting training shows a terrifying scenario. Mentally ill persons are often treated carelessly, firearms are frequently used when police opponents hold knives in their hands, the legal prerequisites of police use of firearms are widely neglected – all of these lead more often than not to fatal police shootings. Moreover, statistics show almost exclusively self-defence shots. Operative police shooting training aims at developing automatic response mechanisms. Ever less regard is given to the legal restrictions to the use of firearms. Targeting the vital triangle makes fatal police shooting almost inevitable. The only remedy would be a professional training plan which would grant ample space for the whole range of activity options in any operative situation and, above all, for the consideration of legal restrictions. Such training must clearly demonstrate that resorting to firearms is allowed only in extremely exceptional situations, and that, in the face of mentally ill persons, this can be a solution in very rare cases only. First of all, however, it is necessary to perform operative and shooting trainings frequently and on a regular basis, and thus to reveal all the peculiarities of the different operative situations. Reducing training to the simple alternative between defined shot (according to legislation) and self-defence shot will bring no solution, but, on the contrary, will aggravate the problem and increase the risk of becoming a victim of fatal police shooting.

---

[26] Even if one acknowledges a criminal justification for the plea of self-defence made by police officers, it implies a violation in terms of public law and therefore remains illegal.

[27] Cf. *Dieter Kugelman*, Polizei- und Ordnungsrecht [Police and regulatory law], 2. Ed., Springer-Verlag GmbH, Heidelberg 2011, at 11 (30).

6. REFERENCES

Arzt, Clemens, Europäische Menschenrechtskonvention und polizeilicher Todesschuss – Zugleich eine Besprechung des Urteils des EGMR Makaratzis/Griechenland. Die öffentliche Verwaltung 2007, 230-237

Baller, Oesten, Neue Munition für die Polizei – Eine von Schein-Sachzwängen dominierte Diskussion Bürgerrechte & Polizei/CILIP 65 (1/2000], 70

Baller/Eiffler/Tschisch, ASOG Berlin. Zwangsanwendung nach Berliner Landesrecht – UzwG -, Boorberg, Stuttgart 2004

Berg, Thomas von, Der Finale Rettungsschuss. Ein internationaler Vergleich der verfassungs- und polizeirechtlichen Problematik am Beispiel Deutschlands, Österreichs und der Schweiz, Bachelor thesis at HWR Berlin, 2016.

Deiters/Hoyer et al, SK-StGB. Systematischer Kommentar zum Strafgesetzbuch, Vol. 1, 9. Ed., Carl Heynanns, Köln, 2017

Diederichs, Otto, Polizeiliche Todesschüsse 2015, Bürgerrechte & Polizei/CILIP 111, October 2016, at 85.

Erb, Volker, Münchner Kommentar zum Strafgesetzbuch, Bd. 1, 3. Ed., C.H. Beck, München 2017

Finzen, Asmus, Wer mit einem Messer Polizisten angreift, muss damit rechnen, erschossen zu werden.“ Schlechte Karten für psychisch Kranke http://apk-berlin.de/files/schusswaffengebrauch_gegen_psychisch_kranke_bei_polizei_final-1.pdf>.

Hillenkamp/Cornelius, 32 Probleme aus dem Strafrecht. Allgemeiner Teil, 15. Ed.,Vahlen, Munich 2017

Kafke, Mats, Führt das Berliner Schießtraining zu einem rechtmäßigen Schusswaffengebrauch durch Polizeiangehörige?, Bachelor thesis at HWR Berlin, 2017

Kugelman, Dieter, Polizei- und Ordnungsrecht, 2. Ed., Springer-Verlag GmbH, Heidelberg 2011

Lackner/Kühl, Strafgesetzbuch: StGB. Kommentar, 29. Ed., C.H. Beck, München 2018

Schenke, Wolf-Rüdiger, Polizei- und Ordnungsrecht, 9. Ed., C.F. Müller Verlag, Heidelberg 2016

Witzstrock, Heike, Der polizeiliche Todesschuss. Lang Frankfu

UDK 352:614.8
https://doi.org/10.18485/fb_ic4hs.2018.14

LOCAL GOVERNMENTS' ENGAGEMENT IN INTEGRATING EMERGENCY AND ICT POLICYMAKING

Venelin TERZIEV[*], Vesela RADOVIĆ[**], Ekaterina ARABSKA[***]

Abstract: The role of local authorities has been recognized as a base for improving human security and community wellbeing in the twenty-first century. This role can be enormously improved with the application of information and communication technologies (ICTs). Emergency management is a fundamental challenge for public administration in any country, particularly at the local level. The problems facing less developed countries, characterized by regional inequalities, are among the greatest challenges facing the world today and this issue is of paramount importance for human security and sustainable development. Local authorities have provided the foundation for the current focus on adequate emergency management in the affected territory. The main goal of the research presented here is to discuss how local authorities could improve the safety of citizens by creating a specific policy which is going to integrate the actions of emergency services and the use of ICTs at the same time. ICTs have the potential to raise local income and improve emergency response at the local level and human security. ICTs can enable a two-way communication between citizens and local authorities, potentially resulting in profound changes in local emergency management processes, as well as in the outcomes of social innovation processes. The methodology used in this article is standard for social research: appropriate data is examined in a comparative/historical analysis in this "desktop study". The results confirm that there has been a consistent institutional and political lag in local public administration, which has yet to recognize emergency management in the mainstream of its activities or use ICTs in an adequate scope in the process of enhancing human security in communities.

Keywords: local authority, emergency, ICTs, policy, sustainability

---

[*] Professor, PhD, Vasil Levski National Military University, Veliko Tarnovo, Bulgaria, E-mail: terziev@skmat.com

[**] PhD, Institute for Multidisciplinary Research, University of Belgrade, Serbia, E-mail: vesela.radovic@imsi.rs

[***] Associate Professor, PhD, University of Agribusiness and Rural Development, Plovdiv, Bulgaria, E-mail: earabska@uard.bg

1. INTRODUCTION

The September 2015 United Nations agenda, titled "Transforming our world: the 2030 Agenda for Sustainable Development" and echoing human security principles, emphasizes a "world free of poverty, hunger, disease and want … free of fear and violence … with equitable and universal access to quality education, health care and social protection … to safe drinking water and sanitation … where food is sufficient, safe, affordable and nutritious … where habits are safe, resilient and sustainable … and where there is universal access to affordable, reliable and sustainable energy". This agenda contributed to the overdue recognition of the relationship between cities, sustainable development, socioeconomic factors, human settlement and natural resources. The world leaders' recognition of this relationship was materialized in the inclusion of Sustainable Development Goal (SDG) 11: "Make cities and human settlements inclusive, safe, resilient and sustainable" to strengthen resilience and the capacity to adapt to climate-related hazards and their impact on natural resources (United Nations, 2015). Furthermore, all 17 SGDs acknowledge the importance of the implementation of the adopted sustainable policy at the local level and the important role of local governments (Al-Zubi & Radovic, 2018).

It is widely recognized that there is a dynamic and potentially mutually reinforcing relationship between emergencies (disasters) and development: emergencies impact on development and development impacts on emergencies (Keating et al., 2014). This is obvious at the national level, but even more visible at the local level. In many countries, the state of local self-management has deteriorated over the last few years. The state of the least developed municipalities in the Republic of Serbia is quite alarming. Human security is severely jeopardized in various emergencies. Many plans and projects for different improvement programs have been devised, yet positive results are slow to come (Radović & Komatina-Petrovic, 2012; Radović, 2016).

The integration and use of information and communications technologies (ICTs) has enormous importance for emergency management at the local level. The role of ICTs is even more significant in the process of gaining access to information resources, which provide substantial benefits to emergency services. Therefore, the main objective of the current research is to review how ICT solutions can help local governments to communicate about existing risks, and hence about future sustainable development, increasing the awareness of the population and the mitigation of possible consequences for the affected population. The methodology used is related to the implementation of a "desktop study," document analysis, comparison, historical, etc. It allows the authors to review and analyze various documents from electronic databases, books, scholarly journals, official documents and positive practices from different countries.

The research also tackles the concepts of human security and environmental security as two concepts which intersect and overlap on the one hand, and diverge on the other. There are ongoing debates in the scientific community and the general public about what human security does or should mean so the authors have taken some account of the impact of environmental degradation on people and their communities, particularly in emergencies (Radovic, 2017). The results confirm that the need for creating a coherent emergency management policy for managing existing risks at the local level, which includes the deployment of ICTs, is a significant challenge.

2. EMBRACING ICTS IN THE PROCESS OF EMERGENCY MANAGEMENT AT THE LOCAL LEVEL

The emergency management system (EMS) is a structure for the coordination between the government, local emergency response organizations and other interested parties. It provides and facilitates the flow of emergency information and resources within and between the organizational levels of field response, local government, operational areas, regions and state management (Cao et al., 2018). The existing gap related to emergency management at the local level is noted in the Serbian national progress report on the implementation of the 2013–2015 Hyogo Framework for Action (Ministry of Interior, 2015). In this report, furthermore, the core indicator 3, related to priority of action 1, shows that specific legislation for the local level with a mandate for disaster risk reduction (DRR) exists in Serbia, but without a regular allocation for DRR to local governments. The same goes for the core indicator for priority of action 2 and 3, which states that achievements are neither comprehensive nor substantial despite the institutional commitment. Despite some positive actions (training of the local government, disaster management and preventive risk management, etc.), the most important actions are missing – e.g. guidance for risk reduction and availability of information on DRR practices at all community levels (Ministry of Interior, 2015: 27).

ICTs are an urgent need in the work of emergency services because the most important step towards reducing risks in community is to analyze the potential risks and identify measures that can prevent, mitigate or prepare for emergencies. Hence, local governments should be able to recognize the risks to which their communities are exposed. They must be actively involved in the design and maintenance of early warning systems and understand the relayed information in order to be able to advise, instruct or engage the local population in a manner that increases the safety and reduces the potential losses (Vujic et al., 2013). At the local level the use of ICT solutions for improving human security has to be promoted more efficiently. In this way, all stakeholders could contribute enormously to the extent to which community security, as one of the elements of human security, is being advanced through the security discourses and practices in emergency management.

David Kobia has said that "web programming helps communities facing catastrophe around the world". His creation, Ushaidi, is recognized by Ethan Zuckerman as one of the most globally significant technology projects. It has helped first responders, including members of the U.S. military, who used Ushaidi's map to set priorities, organize and reach distressed people in the aftermath of the Haiti earthquake in 2010 (Greenwald, 2010).

3. ICTS AS A DRIVER FOR MAXIMIZING COMMUNITY SECURITY IN EMERGENCIES

Local governments are faced with exciting challenges and opportunities in the twenty-first century. Their main activities are connected to compiling and assessing data and information on the current and foreseeable state of risks. These include an increased scientific understanding of hazards and societal responses, as well as revolutionary

technologies. The power of social ICTs is becoming enormous (in the media as well). In this area, social capital is the invincible link that inspires trust during mandatory evacuation, volunteers to participate in an exercise, donors for safety programs and support for critical infrastructure implementation. If social capital continues to grow via online connection, it is highly likely that there will be a further transformation in emergency management (For-mukwai 2012: 4).

In this process, it is necessary to mention the existence of the digital divide. This problem is often discussed in an international context, indicating that certain countries are far better equipped than other, less developed countries to exploit the benefits of rapidly expanding ICTs. This issue is visible if we consider regional inequalities in Serbia. At the local level, the proposed ICT frameworks are based on the communication and collaboration difficulties experienced during events in recent history as well as on the recommendations put forward by authorities from developed countries in their reports. In practice, the Intelligent Disaster Collaboration System (IDCS) model developed to improve collaboration patterns and the information flow during the emergency management process in the United Kingdom has proved to be very successful (Sagun et al., 2009).

In her first talk in the Serbian Parliament, Serbian Prime Minister Ana Brnabić stated: "Now is the moment to take a step further and to transfer our society, state and economy into the 21st century, which is marked by digitalisation. Digitalisation is an in-depth transformation of the manner in which we produce, spend, learn, work and exchange (Brnabić, 2017)." Hence, we have to embrace digitalization in the area of emergency management and understand how ICT can be more useful in the process of increasing human security. In the Republic of Serbia, where the ICT framework is not fully established, local governments have to bear in mind the advantages and deficiencies of different ICT frameworks in coordinated actions with competent authorities. Each time that communication networks services, considered as an important part of critical infrastructure, are unavailable when disasters strike, this creates evident societal problems for people who are desperately seeking for information or trying to communicate with each other. The COST Action CA15127 states: Resilient communication services protecting end-user applications from disaster-based failures (RECODIS) has tried to fill this gap by offering the respective solutions to provide resilient communications in the presence of disaster-based disruptions of all types for existing communication networks (e.g. IPv4-based, current Internet), as well as emerging architectures of the global communications infrastructure (i.e. the Future Internet) (European Union, 2018).

4. CONCLUSION

Disaster-based disruptions which seriously degrade the performance of any communication network (resulting from natural disasters, technology-related disasters or malicious attacks) are now gaining importance due to the observed increase of their intensity and scale. Experts therefore propose more advanced ICT frameworks with a focus on automated, intelligent or self-healing ICT systems and on interoperability and information security during an emergency. Local governments have to develop and implement more effective emergency management solutions, closely linked with other

local public policies, which rely on sophisticated mutual aid networks, ICTs and partnerships, not only among first responders but also throughout all functions of stakeholders in a community. Hence, this action has to be involved in all kinds of local policies, in which the use of ICTs has to become an unavoidable precondition. Serbian policymakers have to be more aware of their leading role in creating new opportunities and redefined the emergency system at all levels due to digitalisation.

ACKNOWLEDGEMENT

This article is a part of research related with ongoing COST Action CA15127: Resilient communication services protecting end-user applications from disaster-based failures (RECODIS).

5. REFERENCES

Al-Zubi, M., & Radovic, V. (2018). Sustainable Cities and Communities: Towards inclusive, safe, and resilient settlements. Emerald Publishing Limited.

Cao J., Zhu L., Han H., Zhu X. (2018) Overview of Emergency Management. In: Modern Emergency Management. Springer, Singapore.

European Union. COST Action CA15127. (2018, August 30). Resilient communication services protecting end-user applications from disaster-based failures (RECODIS). Retrieved from: http://www.cost.eu/COST_Actions/ca/CA15127. Accessed: 13.09.2018.

For-mukwai, G.F. (2012). The Transformative Power of Social Media on Emergency and Crises Management. In: Murrey, J. Managing Crises and Disasers with Emergining Techologies. IGI Global, Hershey, Pensylvania, USA.

Greenwald, T. (2010). David Koba about Ushahidi. Techology Review, 46-47.

Keating, A., Campbell, K., Mechler, R., Michel-Kerjan, E., Mochizuki, J., Kunreuther, H., Bayer, J., Hanger, S., McCallum, I., See, L., Williges, K., Atreya, A., Botzen, W., Collier, B., Czajkowski, J., Hochrainer, S., & Egan, C. (2014). Operationalizing Resilience against Natural Disaster Risk: Opportunities, Barriers, and a Way Forward. Zurich Flood Resilience Alliance. Retrieved from: http://opim.wharton.upenn.edu/risk/library/zurichfloodresiliencealliance_ResilienceWhitePaper_2014.pdf. Accessed: 13.09.2018.

Ministry of Interior. Serbia National progress report on the Implementation of the Hyogo Framework for Action (2013-2015). Retrieved from: http://www.preventionweb.net/english/hyogo/progress/reports/. Accessed: 13.09.2018.

Radovic, V., (2016). Mitigation Efforts in Rural Communities after Extreme weather Events- New Insights for Stakeholders. Journal of Innovations and Sustainability, 2 (3): 37-56.

Radovic, V. (2017). Corporate Sustainability and Responsibility and Disaster Risk Reduction: A Serbian Overview. Book CSR 2.0 and the New Era of Corporate Citizenship, Chapter 8, Ed.: Camilleri, M. IGI Global, 147-164.

Radovic, V., & Komatina-Petrović, S. (2012). From failure to success: Serbian approach in mitigation of global climate change and extreme weather events., Journal of Environmental Protection and Ecology, 4 (13): 2207-2214.

Sagun, A., Bouchlaghem, D., & Anumba, Ch. J. (2009). A scenario-based study on information flow and collaboration patterns in disaster management. Disasters 33 (2): 214-238.

United Nations. (2015). Transforming our world: The 2030 Agenda for sustainable development. United Nations. New York.

Vujić, B., Radovic, V., & Lečić, D. (2013). Application of ICT as a necessary tool of emergency response in urban areas. University of Novi Sad, Faculty of Technical Sciences "Mihajlo Pupin" International Conference Ecology in urban areas, Zrenjanin, 518-524.

National Assembly of the Republic of Serbia. 28 June 2017 KEYNOTE ADDRESS BY SERBIAN PRIME MINISTER DESIGNATE ANA BRNABIĆ. Available on: http://www.parlament.rs/upload/documents/activities/28.06.2017.%20KEYNOTE%20ADDRESS%20BY%20SERBIAN%20PM%20DESIGNATE%20ANA%20BRNABIC.pdf

UDK 627.51:351.79
https://doi.org/10.18485/fb_ic4hs.2018.15

FLOOD RISK REDUCTION AS A CRITERION FOR VALIDATING TECHNOLOGICAL INNOVATION STRATEGIES WITH RESPECT TO HUMAN SECURITY

Zoran KEKOVIĆ[*], Jelena DINIĆ[**]

Abstract: Heavy rainfall that has caused floods worldwide in the last few decades has resulted in a great death toll, a significant number of displaced persons and severe destruction of material goods. The importance of planning in the process of disaster impacts mitigation has been recognized in numerous disaster risk reduction strategies developed by international organizations. In this paper, the authors point out the concepts of preparedness and prevention as the key criteria for validating certain innovation strategies, in particular those with an important technological component regarding flood risk reduction. A holistic approach is implemented in assessing the relevance of innovation opportunities with respect to flood prevention and risk management. In accordance with the conceptual framework for flood risk management, the authors use normative, physical, informational, environmental, social and political indicators. Also, a number of agents of change that may affect future flood risks are investigated: climate change, community development and changes in land use, changes in population, the condition of flood mitigation systems (success of system maintenance, changes in system configuration, etc.), changes in the watershed etc. Special attention will be paid to human security aspects of flood risk reduction as a criterion for validating technological innovation strategies. Floods generate human insecurity due to numerous human casualties, diseases, environmental pollution, critical infrastructure destruction and the potential disruption of other institutional activities. Human security and vulnerability as a framework for disaster risk reduction research has great potential in measuring changes related to the public perception of flood risk and new technologies usage as well as measuring a community's confidence in state and non-state security providers.

Keywords: floods, risk reduction, technological innovations, human security.

---

[*] Full Professor, PhD, Faculty of Security Studies, University of Belgrade; zorankekovic@yahoo.com
[**] PhD Student, Faculty of Security Studies, University of Belgrade; e-mail: ydinic@yahoo.com

1. INTRODUCTION

Disaster management systems include people, infrastructure, and the environment. Each element is vulnerable to natural hazards or human error. Using a systems view, Simonovic (2011: 49) states that disaster losses are the result of interaction among three systems and their many subsystems: the Earth's physical systems (the atmosphere, biosphere, hydrosphere, etc.); human systems (e.g. population, culture, technology, social class, economics, and politics); and constructed systems (e.g. buildings, roads, bridges, public infrastructure, and housing). All of the above systems and subsystems are dynamic and involve constant interactions between and among subsystems and systems. Changes in the size and characteristics of a population and changes in the constructed environment interact with changing physical systems to generate future exposure and define future disaster losses (Simonovic, 2011: 49). By the end of the twentieth century, the concept of flood risk management had been widely accepted in Europe and was beginning to take hold in the United States. The current approach to flood risk analysis does not address certain components that are critical to a modern flood risk analysis. These include uncertainties in risk perception, the consequences that result from human behavior during actual flooding, and the probabilities of success of actions such as, for example, the evacuation of the elderly and disabled. Capturing these factors in the methodological approach to flood risk analysis is the source of the modern risk-based analysis.

When it comes to the theoretical framework, vulnerability theory and preparedness theory can be used for a better understanding of flood risk reduction in the context of human security issues (Richey, 2009).

2. HUMAN VULNERABILITY AND RISK PERCEPTION AS A FRAMEWORK FOR DISASTER RISK REDUCTION

Disaster risk reduction from the human security perspective is almost universally confused by the imprecision of human judgment. According to Simonovic, this is perhaps the most important misconception that blocks the way to more effective societal disaster risk management. The ways in which a society manages disaster risks appear to be dominated by considerations of perceived and subjective risks, while it is the objective risks that kill people, damage the environment, and create property loss (Simonovic, 2011: 102). Furthermore, risk perception is assumed to be the trigger for human behavior during disasters – including emergency response practice – in such a way that many incidents have involved an inadequate reaction of people and their misconception of certain events. People respond to hazards according to their perceptions of the risks those hazards pose. What they perceive, why they perceive it in that way and how they will subsequently behave are matters of great importance to industries and governments trying to assess and implement new technologies (Peters & Slovic, 1996). Furthermore, people's perceptions of the risks posed by a specific hazard vary based on their personalities, experience, knowledge and many other criteria, and these perceptions vary among individuals and groups as well based on their awareness of a particular hazard (professionals vs. laypeople), personal and cultural differences, and hazard characteristics. Psychometric

paradigm studies have demonstrated that perceived risk is quantifiable and predictable (Slovic et al., 1981).

In addition to technological difficulties, management should be aware of and prepared to deal with human factor limitations. Risk perceptions by various groups should be communicated and discussed until a common vision is achieved on the existing hazards and required controls, based on all available information and professional analysis (Ivensky, 2016). In practice, many communities may not distinguish between high potential and low potential hazards in such a way that many strategies try to prevent and respond to all actual events, minor and major, while high potential hazards might go unrecognized. These strategies also risk losing population support if they are perceived as creating an unnecessary burden and controls for situations that are perceived (correctly or incorrectly) to pose only minor risks, or, conversely, as providing insufficient support or control of critical, high potential hazards.

3. CHALLENGES OF THE HUMAN SECURITY ASPECTS OF FLOOD RISK REDUCTION

Continued urbanization and industrialization, and consequently higher population densities result in more people who could be affected by evacuations, or depending on the supply with daily goods, in the shortening of the reaction times of practitioners.

Floods generate human insecurity by causing numerous human casualties, diseases, environmental pollution, critical infrastructure destruction and potential disruptions of other institutional activities. The vulnerability of the population to flood risk varies greatly depending on risk drivers such as geographical exposure (floodplains), the quality of urban planning and housing conditions, combined with climate change. The risk reduction approach to the human security aspects of flood disaster management goes beyond the focus on reducing physical damage to infrastructure to help draw a more dynamic picture of risks and enhance contingency planning and response operations by emergency authorities. Developing resilience indicators for human security harmed by an event can help better inform disaster response plans and accelerate recovery.

The list of key criteria established in the Sendai framework (such as the number of deaths, of missing or injured people, etc.) is not complete without other indicators of human security (MacFarlane et al., 2006) as they have been recognized in scholarly literature and related projects, but it helps to point out the main challenges for individual security in response to disaster as follows:[1]

3.1. CIVIL PROTECTION RESOURCES

Civil protection resources include material and personnel issues, but also organizational challenges, such as spontaneous volunteers or questions of standardization.

---

[1] D1.1 – DAREnet Challenges and RDI Topics, H2020- SEC-21–GM-2016/2017, Deliverable submission date (16 April 2018) DAREnet. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 740750.

Material challenges comprise the technical equipment available to the respondents, where functionality and robustness are of key importance. In the field of flood management, this can be having barrier systems substituting classic sand bag barriers, having trucks equipped for mud and high-water levels or boats capable of operating in flooded urban areas. Ensuring the supply with the right equipment or goods at the right place and the right time is essential for a sustainable and efficient disaster response. Events like floods usually demand a high number of responders. Many civil protection units rely on volunteers; therefore if they are not immediately available, this requires mechanisms to make them available and mitigate possible economic damage for them or their employer.

A relatively new phenomenon is the engagement of citizens who spontaneously volunteer.[2] This can be very helpful, yet there are new challenges, for example liability issues or lack of training and understanding of disaster management structures (e.g. the chain of command). The efficient involvement of spontaneous volunteers requires training for the responders and the preparation of structures and processes in advance. During the Danube and Elbe floods in 2013 many spontaneous volunteers showed up and wanted to help. Their workforce was a good addition at sandbag filling stations, where they supported the logistics, filling bags or preparing them for transportation. However, new standardization approaches to the classical coordination of responders during emergency situations are required.[3] International Standard - *ISO 22319 Security and resilience - Community resilience - Guidelines for planning the involvement of spontaneous volunteers* provides the guidelines for planning the involvement of spontaneous volunteers (SVs) in incident response and recovery. Spontaneous volunteers can provide a significant resource of timely labor, skills and abilities to enhance the capacity of incident response organizations, provide valuable local knowledge and personalize the response and recovery in an area by members of its local community. However, in large numbers, SVs can overwhelm incident response organizations, interfere with operations and create additional risks. SVs who provide relief outside of official operations can put themselves in danger, as well as those they aim to help. It is important to understand and implement best practices for involving and mobilizing SVs, and the integration of SVs into response and recovery activities needs to be carefully managed.[4] This topic also resembles a communicational challenge. For cross-border incidents in particular, lacking standardization is a huge challenge, which ranges from used terminology to specific

[2] A spontaneous volunteer is an individual who is not affiliated with existing incident response organizations but who is motivated to contribute unpaid work during and following incidents. The range of tasks performed by SVs can require only basic planning (e.g. for people who are first on the scene), or a plan that is more complex (e.g. for people who travel to the affected area to volunteer)

[3] See: **ISO 22315** Societal security – Mass evacuation – Guidelines for planning; **ISO 22319** Security and resilience – Community resilience – Guidelines for planning the involvement of spontaneous volunteers.

[4] Duncan Shaw (UK), the project leader responsible for writing ISO 22319.

equipment norms. This intersects with challenges in the field of communications, where the lack of standardized protocols becomes even more evident. Demographic change in most European countries is another challenge. On the one hand, disaster management is faced with older volunteers, underlining the need for ergonomic technical solutions and aid. On the other, it means that the population is also becoming older and potentially less mobile or that it depends on assistance (e.g. medical supply or mobilization), which is challenging when dealing with e.g. evacuations. Emphasizing self-protection could be key in building resilience to disasters caused by natural hazards.

Security culture is important for the vulnerability of a society. Are people aware of certain dangers and willing to act accordingly? This becomes even more obvious when the dependence on technical standards is taken into account. For example, when communication technologies change to digital formats, there will be a high dependence on electricity to guarantee those services compared to classical landline services. The individual resilience of the affected is directly linked to the safety culture, e.g. do they have the necessary reserves (e.g. food and water) to be self-sufficient for a period of time, or do they know how to build a sand bag dam to protect their property? These determine their ability to self-protect.

Governmental preparedness takes into account questions related not to individuals, but to groups or society as a whole. In this area, the state of citizens' preparedness is a huge challenge. In this context, widespread warning systems resemble a challenge to enable timely warning and information. Efficient information management is another potential issue, especially in terms of a uniform language and access to data. Legal regulation has made flood risk maps and management plans obligatory in Europe. However, proper training of the people involved is necessary to enable a proper usage of those documents in case of an emergency.

Another area in the category of information is ensuring that the public is informed as a very important task in reducing vulnerability. Also important is the high quality and transparency of information from authentic and verified sources, to avoid the spreading of "fake news" and preserve the trustworthiness of information services. This also affects the previously mentioned spontaneous volunteers, since specific information can enhance the efficiency of their involvement, while uncoordinated communication could cause problems or frustration, e.g. due to controversial information on where to help.

Political aspects usually set the frame, mainly due to a legal framework that enables effective disaster management and the availability of communication resources. Another political challenge is creating the incentives for prevention and collaboration, as well as fostering the understanding of consequences. This is especially true for rivers, since all measures undertaken upstream, might directly or indirectly influence the outcome downstream.

3.2. CITIZENS AND VULNERABLE GROUPS CHALLENGES

A prepared society is less vulnerable and the ability of self-protection is demanded by many flood directives and strategies. Here, information on dangers as well as options to protect property are helpful. This could also mean, for example, trainings on how to

handle sand bags and build simple barriers. Supportive recommendations might lead to a better preparation for disasters (e.g. storage of food, water, batteries).

Continuous urbanization leads to higher population densities in urban areas, but also bears the danger of pushing living space into flood-prone areas. The general public needs to know about evacuation concepts, such as safe routes, timing and execution. Evacuation plans should be partly accessible to the public. Also, a well-established marking of safe routes would increase efficiency. In cases of evacuation or temporary supply, responders would need to know where special aid is needed, for example respiratory support systems requiring power supply or oxygen bottles for exchange. In cases of evacuations, certain information, e.g. about immobile persons, would be valuable to efficiently plan these types of operations.

In remote areas, or areas that have become isolated due to infrastructural failures (e.g. the collapse of bridges), temporary solutions for (emergency) medical services are particularly needed. In the case of flooding, regular medical service might be interrupted due to devastated hospitals or doctors' offices or a possible cut-off of some places. Temporary support from e.g. truck-based doctors' offices could maintain a basic service to residents in the affected area. The increasing number of elderly people requires a critical review of whether existing concepts are sufficient in terms of maintaining basic medical services during response or recovery in flooded/affected areas. In cases of massive disruptions in power, potable or waste water supply, temporary supply concepts are needed such as transportation into the affected area, but also concepts regarding the recovery of such systems. Flooding events usually require a huge logistical effort. Concepts established in advance as well as decentralized logistics hubs would therefore decrease reaction and supply times. Time is critical, especially during emergency situations. Decentralized material and logistic support centers help avoid long transportation paths and enable better availability to local/regional responders.

It is also important to emphasize the role of technological innovations in improving human security in the context of flood risk management. Integrated disaster management systems include integrating situational awareness or decision support based on modern but system-oriented technologies. From the civil protection point of view, building higher dikes might be a local solution, yet it poses a higher risk to the protected area in case of a dam failure.

4. CONCLUSION

Critical re-evaluations of the applied concepts in risk reduction strategies from the perspective of human security call for the identification of the affected parties in an emergency.

It can be anticipated that in the years ahead, advances in technology will permit more effective and efficient capabilities to identify and deal with risk. At the same time, increased communications capabilities will better prepare the population at large to understand and participate in the development and use of risk strategies.

Open communication channels between all levels of an organization and between organizations in multiemployer projects are critical for ensuring an effective exchange of

risk-related information. While it may be difficult to quantify risk, the management must have complete data and must "deal in a world of reality in understanding technological weaknesses and imperfections well enough to be actively trying to eliminate them" (Ivensky, 2016).

In addition to technological difficulties, the management should be aware of and prepared to deal with human factor limitations. Risk perceptions by various groups should be communicated and discussed until a common vision is achieved on the existing hazards and required controls, based on all available information and professional analysis.

While conducting a risk reduction and hazard analysis, disaster management teams need to be sure that all parties, including the management, the responders and citizens, share the perceptions of hazards, controls and residual risks that match those of experts.

The psychometric paradigm is typically applied in public risk perceptions management from higher to lower in order to avoid fear, panic and outrage. Important trends, such as climate change, urbanization growth or the ageing of populations, need to be recognized and a reverse application needs to be suggested where risk uncertainties and potential dreadful outcome scenarios are emphasized to move the perceived hazard from lower to higher. This would result in increased risk perceptions and increased support of risk reduction strategies by the population and affected groups and individuals. Focusing on high to medium-potential hazards versus all flood hazards may increase the resilience of citizens in case of hazard events like floods. Efficient communication strategies are needed in order to have resilient systems, capable of reaching the public.

5. REFERENCES

Glenn Richey Jr, R. (2009). The supply chain crisis and disaster pyramid: A theoretical framework for understanding preparedness and recovery. International Journal of Physical Distribution & Logistics Management, 39(7), 619-628.

Ivensky, V. (2016). Managing Risk Perceptions: Safety Program Support Outcomes. Professional Safety, 61(08), 44-50.

MacFarlane, S. N., & Khong, Y. F. (2006). Human security and the UN: A critical history. Indiana University Press.

Peters, E., & Slovic, P. (1996). The Role of Affect and Worldviews as Orienting Dispositions in the Perception and Acceptance of Nuclear Power 1. Journal of applied social psychology, 26(16), 1427-1453.

Simonovic, S. (2011). Systems approach to Management of disasters, Methods and applications, Wiley.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1981). Perceived risk: psychological factors and social implications. Proc. R. Soc. Lond. A, 376(1764), 17-34.

Wishart, D. (2004). A combined catchment and reach-based assessment of historical channel planform change in a UK upland gravel-bed river. PhD Thesis, Durham University, UK.

Reports

D1.1 – DAREnet Challenges and RDI Topics, H2020- SEC-21–GM-2016/2017, Deliverable submission date (16.04.2018) DARENET. This project has received funding from the European union's Horizon 2020 research and innovation programme under grant agreement no. 740750

National Research Council. (2012). Disaster resilience: a national imperative.

Web sources

Published ISO Standards, http://www.isotc292online.org/publications/ 22/07/2018

UDK 551.583:316.42
https://doi.org/10.18485/fb_ic4hs.2018.16

INCREASE IN CLIMATE CHANGE AND ITS IMPACT ON THE VULNERABILITY OF SOCIAL COMMUNITIES

Miloš TOMIĆ[*], Sandra TOŠIĆ[**]

Abstract: Climate change is one of the most important ecological threats of the twenty-first century, and it has significant implications for the quality of life of millions of people across the globe. Findings of numerous empirical studies show that the effects of climate change, such as temperature increase, melting of ice, rising sea and ocean levels and changes in rainfall rates, have a significant impact on the functioning of human society. At the beginning of new millennium, climate change has significantly contributed to the emergence of extreme natural disasters. Namely, the increasingly frequent occurrence of floods, droughts, earthquakes, storms, volcanic eruptions, hurricanes, and tsunamis is directly proportional to the increase in the vulnerability of human communities. Climate change will also continually endanger agricultural production and the safety of food supplies. Production and availability of food and water, human health, transport, energy supply are just some of the elements on which the functioning of human communities is based, and which are highly dependent on climatic conditions and which can be significantly destabilized by climate change. This state of affairs is confirmed by a large number of scientific studies that indicate that the use of obsolete technologies and common rules of behaviour dramatically accelerate temperature disproportions that negatively affect the basic conditions of human life (access to drinking water, food, use of the natural environment). Anthropogenic activities, in addition to natural ones, are considered to be the main cause of greenhouse gas emissions, resulting in a global increase in average air temperature. By developing and applying modern technology, gases contributing to the greenhouse effect would be greatly reduced. The rise of average temperature induces sudden meteorological changes at all levels (global, regional and national). The uneven distribution of the impact of climate change caused the need for an effective preventive response, especially due to the fact that the poorest countries are extremely vulnerable. An effective response to climate change and its inevitable consequences depend on several factors: the seriousness of the situation (familiarizing the public with the problem of climate change), programme policy (strategic documents) and the development of institutional capacity. Solving the climate change problem will

[*] PhD Student University of Belgrade Faculty of Security Studies, milosttomic@yahoo.com
[**] PhD Student, University of Belgrade Faculty of Security Studies, sandratosic93@hotmail.com

inevitably determine the future economic and, therefore, social development of many countries in different parts of the world.

Keywords: climate change, vulnerability of social community, lack of resources, natural disasters, modern technologies.

1. INTRODUCTION

The increasingly frequent occurrence of extreme natural disasters and other climatic phenomena with devastating consequences that necessarily accompany them has led to the need for an effective strategic response to the ever-growing climate change. Climate risk management, especially in those underdeveloped[1] and less developed parts of the world, reduces the vulnerability of social communities while providing necessary prerequisites for stable social and economic development.

The increased concentrations of greenhouse gases (GHG) (carbon dioxide, methane, and water vapour, amongst others) in the atmosphere are accelerating the occurrence of a natural phenomenon known as the greenhouse effect. The proliferation of GHG in the atmosphere is elevating the mean temperature of the world, both of land and sea, at a much faster rate than ever seen before on the planet (Intergovernmental Panel on Climate Change (IPCC), 2012; World Meteorological Organization (WMO), 2013). Accordingly, Arndt and associates state that this can cause serious climate modifications (see Figure 1) with certain growth indicators (Arndt, et al., 2010) whereby security threats occur as the direct consequences that threaten the social, political, environmental and economic values of a country.

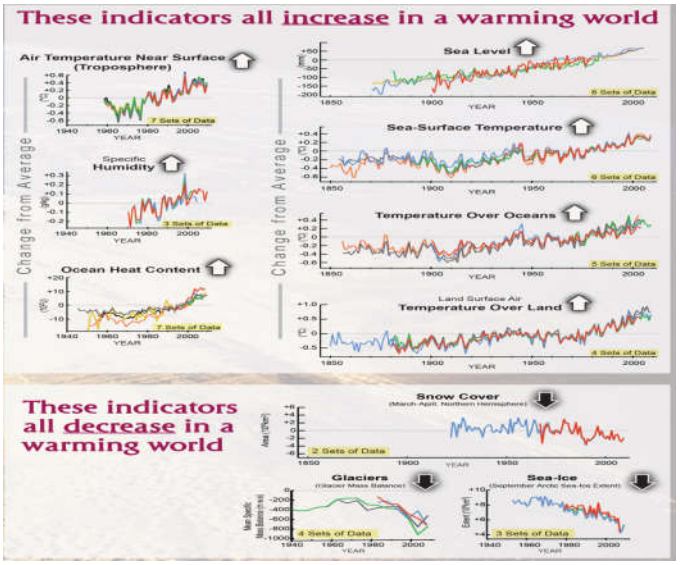


Figure 1. Indicators of climate change

Source: Arndt, et. al., 2010

[1] Poverty is an important aspect of vulnerability because of its direct association with access to resources which affects both baseline vulnerability and coping from the impacts of extreme events (Adger, 1999).

Therefore, it is necessary to seriously address the problem of climate change, especially due to the fact that it represents a catalyst for the development of unwanted climatic and other events. Although studies suggest that these changes will not be negative for all countries and territories, they do indicate that these transformations will inevitably alter current livelihoods (IPCC, 2012).

2. DEFINING VULNERABILITY

In scientific literature, the notion of vulnerability is often unevenly defined. Kelly and Adger (2000) state that 'the concept of vulnerability is broadly defined and categorized depending on the level (functionality) and scope of the analysis.' The very concept of vulnerability has developed over time through various scientific disciplines (political ecology, human ecology, physical science, and spatial analysis), modelling a number of definitions conditioned primarily by concrete methodological and epistemological approaches (Cutter 1996; Thywissen, 2006; Deressa et al., 2008).

Two major vulnerability research traditions have arguably been the source of ideas for research into integrated human–environment vulnerability, namely, analysis of vulnerability as 1. 'lack of entitlements in livelihoods', traditionally used to explain food insecurity, and 2. social impacts of 'natural hazards', developed to explain the commonalities between different types of natural catastrophes and their societal impacts (Adger 2006).

Intergovernmental Panel on Climate Change (IPCC) in its Fourth Assessment Report defines vulnerability as: 'the degree to which a system is susceptible to, or unable to cope with, adverse effects of climate change, including climate variability and extremes. Vulnerability is a function of the character, magnitude, and rate of climate variation to which a system is exposed, its sensitivity, and its adaptive capacity' (IPCC, 2007: 93).

Therefore, the basic constituent elements of the definition proposed by the IPCC are exposure, sensitivity, and adaptive capacity[2]. These three elements are considered the main components of the concept of vulnerability in extreme natural disasters (floods, droughts, volcanic eruptions, storms, hurricanes, tsunamis and earthquakes) caused by climate change.

3. CONSIDERATION OF THE CONCEPT OF SOCIAL VULNERABILITY TO CLIMATE CHANGE

Essential feature of a model of social vulnerability[3] to climate change is, first of all, that it focuses on social aspects of the phenomenon (Adger, 1999). The principal finding of the

[2] *Exposure* component is related to the nature and degree to which a system is exposed to a series of changes, particularly in the valued constituents ??. *Sensitivity* can be viewed as the degree to which a system is affected by climate variability or change. *Adaptive capacity* is related to the potential of a system to develop and integrate certain measures in order to effectively deal with the expected impacts (Parry et. al., 2007).

[3] In many cases social vulnerability is most often described using the individual characteristics of people (age, race, health, income, type of dwelling unit, employment) (Shirley et al., 2012).

social vulnerability studies is that it is the social processes that 'generate unequal exposure to risk by making some people more prone to disaster than others, and these inequalities are largely a function of the power relations operative in every society' (Hilhorst and Bankoff, 2007:2).

Climate change presents an uncertain but potentially serious threat to vulnerable populations (Bohle et al., 1994). Climate events can result in irreversible losses of human and physical capital and may cause poverty traps (Heltberg et al., 2009). Developing countries are particularly vulnerable to climate change impacts because of exposure and sensitivity to climate change and because some elements of the capacity to adapt may be limited: hence biophysical and social vulnerability (McCarthy et al, 2001). Furthermore, climate change is directly affecting the living conditions of most of the people in developing countries, through increasing variability and uncertainty of the conditions in which people try to pursue their livelihoods (IPCC 2007).

A longitudinal study in Zimbabwe followed children that were less than 2 years old (the at which children are most susceptible to malnutrition) when a severe drought hit in the early 1980s (Heltberg et al., 2009). Those that survived the famine were found to be stunted, translating into lower schooling achievements, inferior adult health, and an estimated 14% reduction in lifetime earnings (Alderman et al., 2006).

The last decade of the twentieth century was marked by the appearance of extreme natural phenomena. Kelly and Adger (Kelly & Adger, 2000:332-333) describe in their work the devastating effects of the Linda Storm that hit South Vietnam in 1997. Namely, the authors state that the material damage amounted to US$ 600 million, with 778 people being killed while 2132 persons were missing.

Agriculture is inherently sensitive to climate conditions and is among the most vulnerable sectors to the risks and impacts of global climate change (Parry and Carter 1989; Reilly 1995; Desanker & Magadza, 2001; Smit, & Skinner, 2002). In many countries around the world, food production plays a central role in modelling and implementing a national policy for maintaining general well-being and health of people. Piao and colleagues (Piao et al., 2010) cite the example of China as a country in which the effects of climate change dramatically jeopardize (directly or indirectly) the safety of food production and the survival of over 1.3 billion people. In addition, the authors emphasize that each state must individually take the necessary measures for strengthening adaptive capacities through appropriate program policies (adoption of 'ecological' laws, application of modern technology with low emission of pollutants, sustainable use of drinking water) and efficient institutional response at all levels of government), because understanding of the present climate variability in society will reduce the impacts of climate change (Adger, 1998) on individuals and society.

4. MITIGATION OF AND ADAPTATION TO CLIMATE CHANGE

Social communities that are facing reduced quality of life due to climate change have at their disposal two basic response strategies: mitigation of climate change and adaptation to climate change (Dimitrijevic, 2010). Mitigation refers to limiting the consequences of global climate change through reducing greenhouse gas emissions and increasing carbon dioxide absorption capacity (IPCC, 2014). Adaptation is primarily aimed at alleviating

harmful effects of inevitable climate change through a wide range of actions which target an endangered system (Füssel, & Klein, 2006; Locatelli, 2011). The objective of mitigating climate change is to adopt measures to limit the volume of climate change.

Adaptation and mitigation, as two basic responses to climate change, differ from one another, especially with regard to the objectives of implementation. Mitigation is directed at causes, while the adaptation is focused on the impact of climate change. The results of various research studies show that confronting climate change involves the use of both approaches (Fussel, 2007; Schipper, 2006; Ringius et al., 2002; Muller, 2001). Even with a reduction in greenhouse gas emissions, an increase in global temperatures and other climate change is expected (Zhang, et al., 2011). On the other hand, the adaptation will not be able to eliminate all the negative effects. Accordingly, adaptation and mitigation are key to limiting changes in the climate system. In addition to the goal, the difference between mitigation and adaptation is related to spatial impact. Mitigation has a global, while the adaptation has, at best, regional, but mostly local domain (Klein, et al., 2005).

Mitigation refers to reducing the vulnerability of the community using different technical solutions. Among the potential solutions proposed for mitigation of climate change, the greatest attention in the scientific literature and public debates is paid to two different approaches, related to the concentration of carbon dioxide and other gases that contribute to the greenhouse effect in the Earth's atmosphere. Stabilization of carbon dioxide concentration in the atmosphere can be achieved by reducing emissions (carbon sources) or by the natural adoption of atmospheric carbon dioxide by the ocean and terrestrial ecosystems. The second technique consists of the artificial absorption of carbon dioxide from the atmosphere (based on physical and chemical processes) followed by its injection. Mitigating the effects of climate change involves the implementation of different approaches, such as solar radiation management, abatement of emissions, carbon trapping in biomass carbon capture, and geological storage (Zhang, et al., 2011)

Adaptation is the process of adapting ecological, social or economic systems in response to actual or expected climate stimulation and their effects or impacts (IPCC, 2014: 1758). Adaptation is a socio-institutional process that involves cycles of anticipation and response to a variety of stressors (Tschakert & Dietrich 2010). Effective adaptation to climate change depends on the availability of two important prerequisites: information on what to adapt and how to adapt (Adger, et al., 2005). Adaptation involves a wide range of measures, including technical, institutional, legal, educational and other measures. Research and data collection can also be considered adaptive measures (in the broad sense) because they facilitate the implementation of climate risk mitigation measures (Fussel, 2007: 266).

Adapting to climate change and risks takes place in a dynamic social, economic, technological, biophysical and political context that differs in time, location and sector. These complex conditions determine the capacity of the adjustment system (Smit & Pilifosova, 2003). Adaptive capacity is the potential or ability of a system, region or community to adapt to the effects or impacts of climate change (IPCC, 2014: 169). Improving adaptive capacity is a practical means of overcoming changes and uncertainties in the climate, including variability and extremes. The main characteristics of communities

or regions that seem to determine their adaptive capacity are: economic wealth, technology, information, infrastructure and institutions (Smit & Pilifosova, 2003).
The application of different adaptation technologies can reduce the current and future vulnerability to climate change. Adaptation technology can be defined as 'the application of technology to reduce vulnerability or increase the resilience of natural or human systems to the impacts of climate change' (UNFCCC, 2005: 5). These technologies can be classified as 'heavy' technologies, such as equipment and infrastructure, and 'soft' technologies, including management practices and institutional arrangements (Christiansen et al., 2011). This division is conditional because some technologies, such as new varieties of crops, are not easy to classify.

5. CONCLUSION

The last two decades have been characterized by a significant increase in academic interest in investigating the impact of climate change on all types of natural and social systems. The direct effects of climate change are the rise in temperature, ice melting, rise in sea and ocean level, and changes in precipitation patterns. These consequences are causing significant problems in the functioning of social communities. The change in weather conditions threatens food production; the rise in sea level will have an impact on the coastal environment and infrastructure, extreme weather conditions will become more and more serious and can cause destruction (IPCC, 2014). The increase in the frequency of catastrophic events such as floods, droughts, fires is also a consequence of climate change. It is very likely that mankind will be exposed to an increased risk of such occurrences. At the beginning of the 21st century, the issue of climate change has come into focus of the international community's interest. The international scientific community has concluded that there are two main approaches to dealing with climate change and reducing the vulnerability of social communities: mitigation and adaptation. The inability to overcome the effects of climate change through the application of adequate technologies makes developing countries more vulnerable to instabilities and conflicts.

6. REFERENCE

Adger, W. N. (1998). Indicators of social and economic vulnerability to climate change in Vietnam. London: University College London.

Adger, W. N. (1999). Social vulnerability to climate change and extremes in coastal Vietnam. World development, 27(2), 249-269.

Adger, W. N., Arnell, N. W., & Tompkins, E. L. (2005). Successful adaptation to climate change across scales. Global environmental change, 15(2), 77-86.

Arndt, D. S., et. al. (Eds.). (2010). State of the Climate in 2009. Bulletin of the American Meteorological Society. 91 (7), 79-106.

Alderman, H., Hoddinott, J., Kinsey, B., 2006. Long term consequences of early childhood malnutrition. Oxford Economic Papers 58 (3), 450–474.

Bohle, H. G., Downing, T. E., & Watts, M. J. (1994). Climate change and social vulnerability: toward a sociology and geography of food insecurity. Global environmental change, 4(1), 37-48.

Christiansen, L., Olhoff, A., & Trærup, S. (2011). Technologies for adaptation: perspectives and practical experiences. UNEP Risø Centre, Roskilde.

Desanker, P. and Christopher M. (2001). Africa. In McCarthy, JJ et al. Climate Change 2001: Impacts, Adaptation and Vulnerability (Contribution of Working Group II to the Third Assessment Report of the Intergovernmental Panel on Climate Change). Cambridge: Cambridge University Press.

Dimitrijević, D., (2010) Trendovi ekološke bezbednosti u XXI veku, Univerzitet u Beogradu, Fakultet bezbednosti, Beograd

Füssel, H. M., & Klein, R. J. (2006). Climate change vulnerability assessments: an evolution of conceptual thinking. Climatic change, 75(3), 301-329.

Fussel, H.M. (2007). Adaptation planning for climate change: concepts, assessment approaches, and key lessons. Sustainability Science, 2(2), 265-275.

Klein, R. J., Schipper, E. L. F., & Dessai, S. (2005). Integrating mitigation and adaptation into climate and development policy: three research questions. Environmental science & policy, 8(6), 579-588

Kelly, P. M., & Adger, W. N. (2000). Theory and practice in assessing vulnerability to climate change and Facilitating adaptation. Climatic change, 47(4), 325-352.

IPCC (2007). Climate Change 2007 : Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Fourth Assesment Report of the Intergovernmental Panel on Climate Change. Cambridge: Cambridge University Press.

IPCC. (2012). Managing the risks of extreme events and disasters to advance climate change adaptation. Cambridge: Cambridge University Press..

IPCC, (2014). Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change, Cambridge University Press, Cambridge, United Kingdom and New York.

Locatelli, B. (2011). Synergies between adaptation and mitigation in a nutshell. CIFOR.

Muller, B. (2001). Varieties of distributive justice in climate change: an editorial comment. Climatic Change, 48(2-3), 273-288.

McCarthy, JJ; Canziani, OF; Leary NA; Dokken DJ; and KS White. 2001 Climate Change 2001: Impacts, Adaptation and Vulnerability (Contribution of Working Group II to the Third Assessment Report of the Intergovernmental Panel on Climate Change). Cambridge: Cambridge University Press.

Parry, M. L., et. al. (Eds.). (2007). Climate Change 2007: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge and New York: Cambridge University Press..

Parry, M.L. and Carter, T.R. (1989). 'An assessment of the effects of climatic change on agriculture', Climate Change 15, 95–116.

Protocol, K. (1997). United Nations framework convention on climate change. Kyoto Protocol, Kyoto, 19.

Piao, S., Ciais, P., Huang, Y., Shen, Z., Peng, S., Li, J., ... & Friedlingstein, P. (2010). The impacts of climate change on water resources and agriculture in China. Nature, 467(7311), 43.

Ringius, L., Torvanger, A., & Underdal, A. (2002). Burden sharing and fairness principles in international climate policy. International Environmental Agreements: Politics, Law and Economics, 2(1), 1-22.

Reilly, J. (1995). 'Climate change and global agriculture: Recent findings and issues', American Journal of Agricultural Economics 77, 727–733.

Tschakert, P., and Dietrich, K.A. (2010). Anticipatory Learning for Climate Change Adaptation and Resilience. Ecology and Society, 15(2): 11

Thywissen, K. (2006). Core terminology of disaster reduction: A comparative glossary. In .Birkmann, J. (ed.) Measuring vulnerability to natural hazards: Toward disaster resilient societies. Press. Hong Kong: United Nations University.

Smit, B., & Pilifosova, O. (2003). Adaptation to climate change in the context of sustainable development and equity. Sustainable Development, 8(9), 9.

Schipper, E.L.F. (2006). Conceptual history of adaptation in the UNFCCC process. Review of European Community and International Environmental Law (RECIEL), 15(1), 82-92.

Shirley, W. L., Boruff, B. J., & Cutter, S. L. (2012). Social vulnerability to environmental hazards. In Hazards Vulnerability and Environmental Justice (pp. 143-160). New York: Routledge.

Smit, B., & Skinner, M. W. (2002). Adaptation options in agriculture to climate change: a typology. Mitigation and adaptation strategies for global change, 7(1), 85-114.

Kely, P. M. and Adger, W. N. (2000). Theory and practice in assessing vulnerability to climate change and facilitating adaptation. Climatic Change. 47 (4), 325-352.

Hilhorst, D. & Bankoff, G. (2007). Introduction : Mapping Vulnerability In: Bankoff, G., Frerks, G. & Hilhorst, D. (eds.) Mapping Vulnerability : Disasters, Development and People. London: Earthscan.

Heltberg, R., Siegel, P. B., & Jorgensen, S. L. (2009). Addressing human vulnerability to climate change: toward a 'no-regrets' approach. Global Environmental Change, 19(1), 89-99.

Zhang, T. C., Ojha, C. S. P., Tyagi, R., & Kao, C. (2013, February).Climate Change Modeling, Mitigation, and Adaptation. American Society of Civil Engineers.

WMO. (2013). WMO statement on the status of the global climate in 2012. Geneva: World Meteorological Organization.

UDK 614.841.45
https://doi.org/10.18485/fb_ic4hs.2018.17

EVACUATION CALCULATION AND MODELING: THE NEED FOR IMPROVING HUMAN LIVES SAFETY IN CASE OF FIRE

Mirjana LABAN[*], Slobodan ŠUPIĆ[**], Suzana DRAGANIĆ[***], Sanja MILANKO[****]

Abstract: One of the essential concepts of fire safety in buildings is the rapid and adequate evacuation of all the occupants of the building in case of fire. Many of the fire safety measures introduced in the design and operation of the building are aimed at ensuring that the occupants can safely leave the building before they are overtaken by heat and toxic products, and before the building collapses. Estimating the time required for evacuation is particularly important for buildings with large numbers of occupants, such as large residential, commercial and public buildings. The time required for the evacuation of all persons who could be present in the building when a fire occurs depends on a number of factors, some of which are very difficult to predict – for example, human behaviour. In our engineering practice, the calculation model is usually applied to determine the evacuation time. On the other hand, modelling and simulation are useful modern tools for the development of virtual scenarios and predictions and they are very important for obtaining dynamic information during an evacuation and identifying the critical points along the evacuation path. These evacuation models could help reduce the consequences of a wide range of adverse events, and can also be used for exploring how certain changes within the real system could affect the efficiency of evacuation and fire safety in a building even before they are implemented. A computer model of the Amphitheatres building in the Faculty of Technical Sciences in Novi Sad has been created using the Pathfinder simulation software, and the results of an experimental simulation of evacuation represent a basis for the assessment of safety in case of fire in public buildings with large numbers of occupants. A comparative analysis of the calculation and computer

[*] Associate Professor, PhD, University of Novi Sad, Faculty of Technical Sciences, Novi Sad, Serbia, mlaban@uns.ac.rs

[**] Teaching Assistant, MSc, University of Novi Sad, Faculty of Technical Sciences, Novi Sad, Serbia, slobodansupic@gmail.com

[***] Assistant – master, University of Novi Sad, Faculty of Technical Sciences, Novi Sad, Serbia, suzanav@uns.ac.rs

[****] BSc. Hon., MA Student / Disaster Risk Management and Fire Safety University of Novi Sad, Faculty of Technical Sciences, Novi Sad, Serbia, sanya6216@gmail.com

model points to the need for future research and for the improvement of evacuation scenarios.

Keywords: evacuation, fire risk, simulation, modelling

1. INTRODUCTION

Over the last few decades, the understanding of human behaviour in fire has shifted away from the assumption that evacuees' responses are dominated by panic, (i.e., irrational and even self-destructive responses), and moved toward an acceptance of evacuees as adaptive and cooperative decision-makers sensitive to the information available (Kinsey et al., 2018). Several case studies (John Drury and Chris Cocking, 2007) have shown that, during mass emergency evacuations, there is rarely evidence of mass panic; behaviour is generally rational, mutual concern and help are common, and, there is evidence of a strong sense of shared social identity, especially amongst groups with some shared interests or affiliation. This new theory has had a significant impact on the area of fire safety design, influencing architectural/civil engineering design and enabling emergency planning and evacuation modelling.

Buildings are currently designed and constructed in accordance with prescriptive and performance-based methodologies to ensure the required level of safety. Prescriptive approaches rely on the application of a predetermined set of rules, such as simple engineering equations, used to determine the required safe egression time. These equations do not take into account evacuee behaviours (e.g. information seeking), or the factors influencing them, and make simplified assumptions regarding performance (Kuligowski et al., 2017). For example, the movement of the population is determined using the number of people in a space and the floor space available (area, distance, obstacles). These simplified assumptions may underestimate the time needed for a population to reach safety, possibly reducing design safety levels.

In contrast, performance-based designs rely on a quantitative assessment of the fire and the achieved evacuation performance levels. Over time, sophisticated computational tools have appeared. These tools can represent the evacuating population as individual agents and often more accurately represent the nature of the space and individual attributes. They also have the potential for representing factors that influence agent behaviour and agents' decision-making processes (such as pre-evacuation time, travel speed of different groups of people, width of evacuees' shoulders, social behaviour, etc.).

A case study of the Amphitheatres building at the Faculty of Technical Sciences (FTS) in Novi Sad and the results obtained by means of an experimental evacuation simulation could contribute to the fire risk assessment process in similar buildings. The evacuation time was determined using the Pathfinder simulation software based on the parameters defined by technical recommendations *SRPS TP 21*.

Future research on this subject would include examining the influence of walking speeds for different groups of people, including vulnerable groups, on evacuation time through evacuation exercises. This would lead to more accurate results on evacuees' behaviour and their walking speeds, as well as indicate the critical points along the evacuation corridor.

The incorporation of these data into evacuation models would contribute to the validity of the models.

2. BASIC DATA ON THE BUILDING

When assessing the fire risk of buildings, it is necessary to take into account all the information relevant to fire protection, such as a building's infrastructure, the number of floors, its structural characteristics in terms of fire resistance, the purpose and content of the building, the applied fire protection measures, its distance from the fire brigade, etc.

The faculty of Technical Sciences is located in the central part of the University campus in Novi Sad, in Liman I city area. It consists of seven buildings and one of them, the Block of Amphitheatres, is the research subject of this paper (Fig. 1).

Access roads to the location from the professional firefighting rescue unit of Novi Sad are paved roads, of adequate width and capacity for firefighting vehicles. The travel distance of professional fire-rescue units to the location via the primary route is 4.2 km, or the same distance in case of the alternative route (Fig. 2). The estimated time of arrival is seven minutes.

The Faculty is located on flat terrain; however, there is a depression in the Amphitheatre area so fire brigade interventions, in case of fire, have to be performed from a certain distance.

Fig. 1 University campus in Novi Sad:
Location of buildings of FTS: 3- Amphitheatres

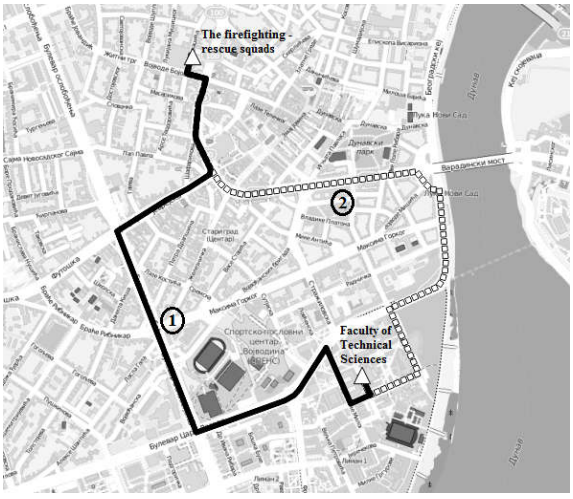


Fig. 2 Fire brigade's access roads to the location:
1-Primary route; 2-Alternative route;

FTS is a public building, which consists of a cellar, the ground floor and the first floor. As the height of the top floor does not exceed 30 m in relation to the surrounding ground, the building does not belong to the class of high-rise buildings. The main entrance (with a windshield) is from the Vladimir Perić Valter Street. The block of Amphitheatres is

connected with the Administrative building, the Teaching block, ITC and Block F by pedestrian passages (Fig. 3).

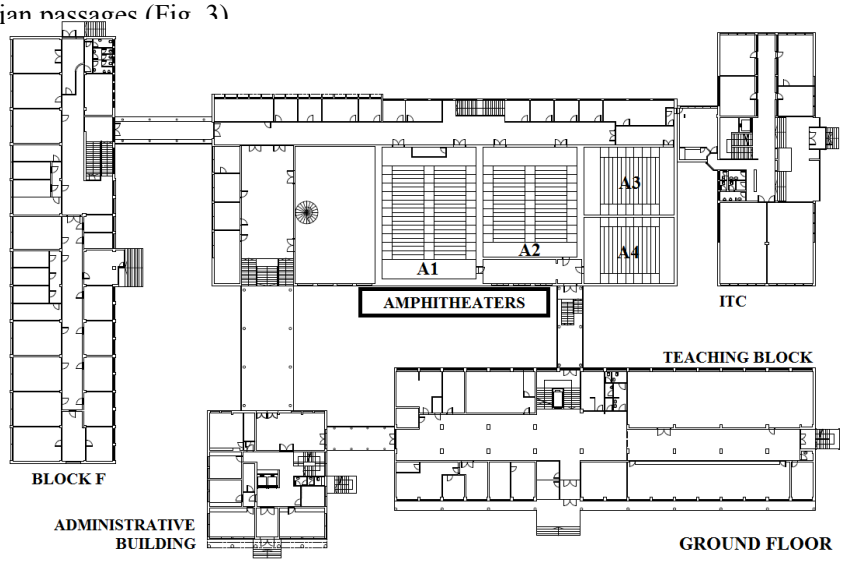


Fig. 3 Amphitheatres' connection to other FTS buildings

The load-bearing structure is made of reinforced concrete (henceforth: RC) and a RC canvas which serves to stiffen the structure. The exterior walls are plastered and made of brick. The roof is flat, impassable. Partition walls mainly consist of plastered and painted interior brick walls, although there are subsequently built partition walls made of plaster boards or lightweight wooden partitions. The windows and entrance portals are made of black metalwork with aluminium – strips and double glazing. The internal doors are wooden. The headroom is 345 cm high, while the maximum height in the amphitheatres is 740 cm. The building's vertical communications consist of a three-way RC staircase positioned opposite the main entrance. The passages are made of RC, they are glazed and have a sufficient length to prevent the fire from spreading from one building to another. However, in case of a fire in this block, adjacent buildings would be endangered by smoke, so it is necessary to provide a full opening or breaking of glazed portals, to ensure smoke extraction from the evacuation routes and to prevent the spread of smoke through the related facilities. The corridors' floors are terrazzo floors or floors lined with marble slabs, while the floors in the amphitheatres, the library, the reading room, the classroom, the offices and cabinets are wooden floors or floors made of plastic materials. The walls are plastered and painted with dispersive colours. In the amphitheatres, the walls are partly covered with wooden boards. The floors and walls in the sanitary facilities have ceramic tiles. The ceilings are plastered and painted.

Aside from the four amphitheatres, a reception desk, a bookstore, a copy shop, a library, offices, storage rooms, a post office, a printing office and toilets are also located on the ground floor; a hall with exits from the amphitheatres and offices, a hall, a library, a copy shop, a bookstore, and offices are located on the first floor, and above the amphitheatres

there is a classroom with a capacity for 30 people. The post office, printing office, bookstore and library have direct entrances / exits. The complete area of individual floors is approximately 2040 m^2, while the total surface area is 3500 m^2.

The maximum number of persons who could fit in the amphitheatres (mostly students) during a fire event or another event with catastrophic consequences is 830, while the total number of people (with employees) who could be present in the building amounts to 1200.

3. SIMULATION SCENARIOS

The evacuation simulation model was created using the Pathfinder simulation software (Fig. 4).

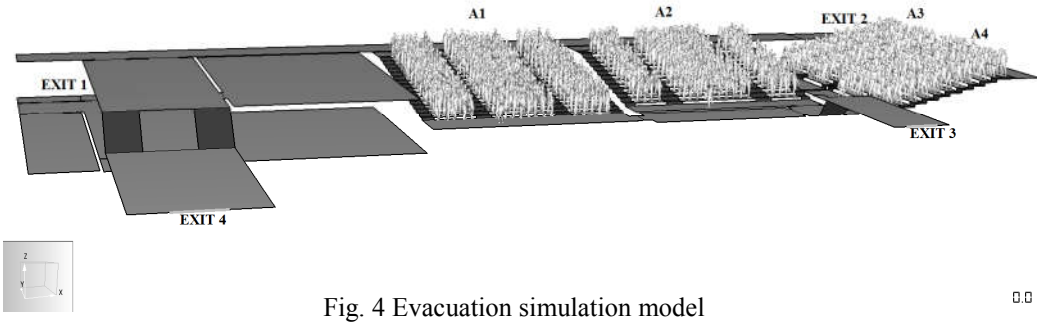


Fig. 4 Evacuation simulation model

The simulation scenarios were based on the layout of the building and the occupants' density in the case of a real fire incident. The walking speeds were defined using technical recommendations SRPS TP 21. The characteristics of the occupants (shoulder width, etc.) were randomized, in order to take into account different egress behaviours of different evacuees.

The scenarios foresee an evacuation where the occupants from all amphitheatres are being evacuated at the same time. The model includes the maximum number of people – 830 – corresponding to the seating capacity. People from other buildings are not taken into account because it is unlikely that a fire will occur in all buildings at the same time.

All actors in the evacuation were assigned walking speeds in the interval between 1.2 m/s and 1.5 m/s, where the walking speeds represent moving downstairs and the normal walking speed, respectively.

For the purpose of the research, three different scenarios were created, differing in terms of the actors' exit selection and undertaken fire safety measures.

3.1. SIMULATION SCENARIO 1

This simulation scenario is the worst case scenario in terms of the conditions. The occupants from the Amphitheatres A1 and A2 are evacuated through the upper exit doors, then through the hall on the ground floor level of the Block, down the stairs into the hall at the basement level, toward the main exit of the building (Exit 1) and to a safe place (Path 1).

The evacuation of the occupants from Amphitheatre A3 takes place from the amphitheatre's exit through the hall and the foyer connection with the building ITC (Exit

2). ITC can be considered as a safe place if the opening in the wall that separates the two buildings is a fire- and smoke-proof door, and if we remove combustible materials from the passage. For now, this route is only the shortest escape route. The evacuation path leads through the passage to the ITC ground floor, down the staircase and into the hall to the main exit (Path 2). Due to the small capacity of the exit door of this communication, the escape route is not suitable for the evacuation of people from the other rooms of in the Amphitheatres block.

The evacuation of the occupants from Amphitheatre A4 is performed from the exit of the amphitheatre through the hall; up the stairs to the passage that connects this block with the Teaching Block, then through the hall and downstairs to the ground floor of the Teaching Block; and finally down the hall to the main entrance (Exit 3, Path 3). If for any reason this exit is inaccessible, it is possible to perform the evacuation by an alternative path from the landing of the main staircase downwards, towards the cellar and then through the hall to the Faculty's students' club and through the club outside.

3.2. SIMULATION SCENARIO 2

This simulation scenario represents the scenario closest to a real evacuation situation. It is realistic to expect that a number of the persons present will begin evacuating from Amphitheatres A1 and A2 through the lower exit doors, and their evacuation route is the same as the evacuation route of the occupants present in Amphitheatre A4 (Path 3). This scenario foresees an evacuation where one third of the actors use Path 3, while the other two thirds use Path 1 at the beginning of the evacuation until they arrive to the staircase. The actors then do not go down, but continue their evacuation through the passage leading through the Administrative Building to its exit (Exit 4). In this case, an unrestricted intervention of the fire brigade would be enabled as Exit 1 would be clear. Also, it can be expected that half of the occupants would instinctively follow the actors from A1 and A2.

3.3. SIMULATION SCENARIO 3

This simulation scenario represents the best case scenario in terms of the conditions, or an improved simulation scenario 1. It is possible to significantly speed up the evacuation by opening a direct way out to the parking lot of the Faculty at basement level. In this case, everyone on the premises related to the ground floor corridor and the amphitheatres would be able to evacuate down the stairway connecting the two levels from the hallway and go outside directly. Also, opening an exit to the inner yard of the building would significantly unburden the escape route, i.e. Path 3.

In this scenario, one third of the occupants would evacuate from Amphitheatres A1 and A2 through the upper exit doors, through the hall and down the stairs leading to the newly-opened exit and out into the parking lot. One third of the occupants from these amphitheatres would take Path 1, while the other occupants from A1 would evacuate through the lower exit doors and then through the newly-opened exit to the inner yard of the building. Other A2 occupants, as well as the occupants from Amphitheatre A4 would take Path 3 during the evacuation. The occupants from Amphitheatre A3 would use Path 2 to reach the exit.

4. RESULTS DISCUSSION

The total times (the average evacuation time obtained from 10 simulations) required to evacuate all persons from the amphitheatres, obtained using a computer model and based on the chosen simulation scenario are the following:

- Simulation scenario 1: 5 min. 9s
- Simulation scenario 2: 4 min. 5s
- Simulation scenario 3: 3 min. 28s

Analysing the evacuation flow in simulation scenario 1, it can be noticed that while occupants are exiting through the upper amphitheatres' door, bottlenecks appear, as well as queues in the hall on the first floor (Fig. 5). This indicates the need for the disburdening of Path 1. The total time required for the evacuation of all persons, obtained in this scenario, amounts to 5 minutes 9 seconds.

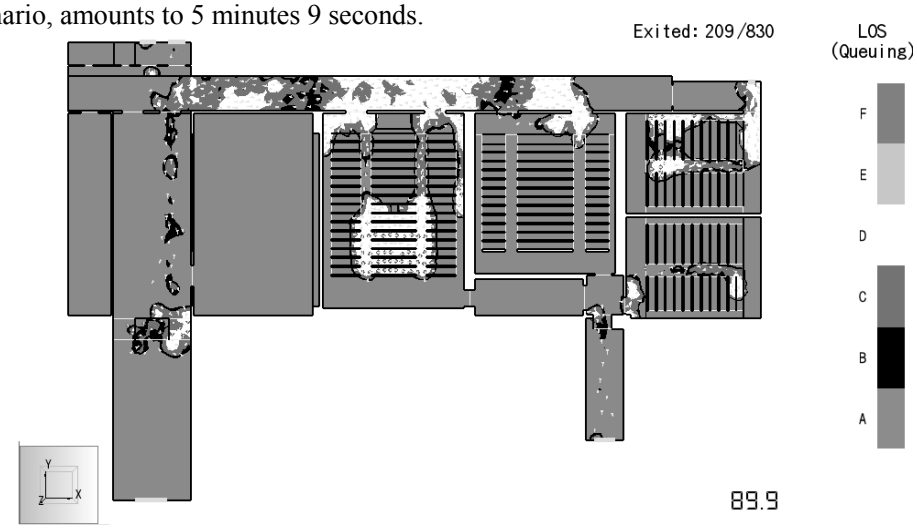


Fig. 5 Simulation scenario 1: Queuing of occupants in the hall above the amphitheatres

The implementation of the proper organizational measures predicted by simulation scenario 2 could reduce the evacuation time. This would require all employees to know their role in the fire event, to know who should try to extinguish the fire, who directs the human stream towards the evacuation exit, who directs people away from the building, etc. The total time required for the evacuation of all persons, obtained in this scenario, amounts to 4 minutes 5 seconds. If the doors are disburdened, it leads to the reduction of the evacuation time. There are still queues of people in the halls, but to a much lesser extent compared to the previous scenario (Fig. 6).

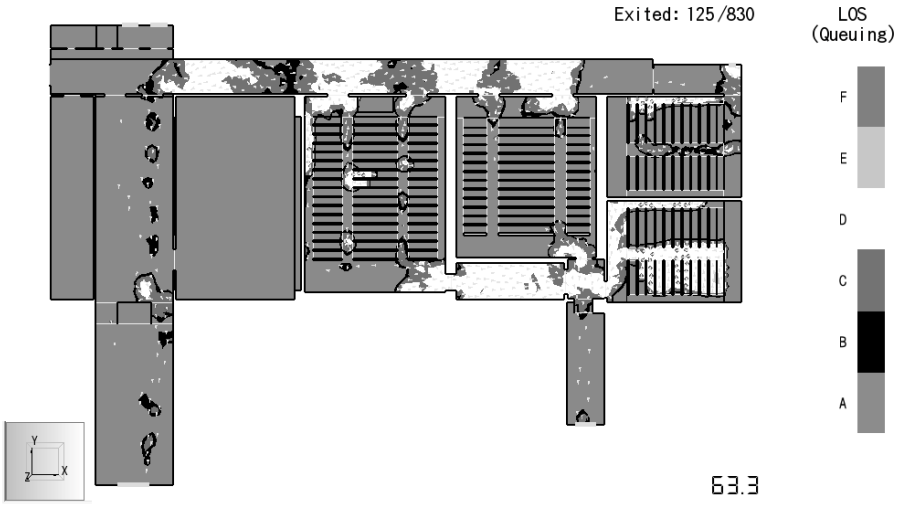


Fig. 6 Simulation scenario 2: Reduced evacuation time due to the disburdening of the doors

The implementation of the proper technical measures predicted by simulation scenario 3 could significantly reduce the evacuation time with regard to both previous scenarios. Opening a new exit door would also disburden the evacuation corridors (Fig. 7). This, of course, also requires the application of appropriate organizational measures. The total time required for the evacuation of all persons, obtained in this scenario, amounts to 3 minutes 28 seconds.

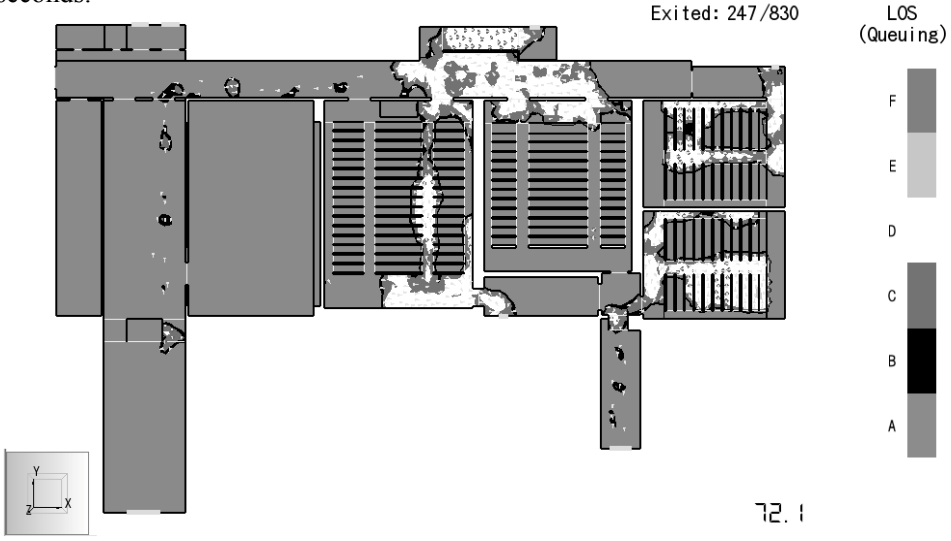


Fig. 7 Simulation scenario 3: Disburdening of the corridors and reduction of evacuation time by opening a new exit

5. CONCLUSIONS

The time required for the evacuation of all persons who could be present in a building during a fire event depends on a number of factors. Many of them, including the nature of the space, the characteristics of the occupants (speed distribution, shoulder width, etc.), as well as their behaviour (social identity, exit choice etc.), are predictable, which enables evacuation modelling and the creation of different scenarios.

In this case study, three different scenarios were analysed: the worst-case scenario and another two scenarios as its improved versions gave the directions to act. Organizational measures – fire drills – should improve the occupants' awareness, and technical measures could improve the efficiency of the evacuation process.

Special attention should be paid to evacuation modelling involving vulnerable groups. The walking speeds of children, the elderly and people with disabilities differ from the usual walking speed (Long Shi et al., 2009). In order to ensure a safe evacuation, it is recommended that each member of these groups (evacuee) has an assigned person to take care of them during evacuation exercises.

In both of the improved versions of the simulation scenario the evacuation time was reduced. It leads us to the conclusion that, besides technical measures, education and regular drills for staff and students, training and preparing them for a real fire event would increase their chances of survival.

Simulation evacuation models enable the development and analysis of multiple scenarios of events. Based on these scenarios, adequate evacuation routes can be defined. This also goes for fire protection measures that could afterwards be implemented. Although these scenario simulations include major evacuation elements, such as: pre-evacuation time (the time for the evacuees to initiate response), physical movement characteristics (travel speed and flow conditions), route availability (the routes available to the evacuees), route usage/choice (the routes selected by the evacuees), they still represent the evacuee and the evacuee's decision-making in a grossly simplified form. In none of the existing evacuation models is the purposive evacuee decision-making process comprehensively represented. Thus, a comprehensive model of evacuees' decision-making and behaviour is required, which is left for future research.

ACKNOWLEDGMENTS

The paper presents part of the research realized in the project "Theoretical and experimental research and improvement of educational process in civil engineering" conducted by the Department of Civil Engineering and Geodesy, Faculty of Technical Sciences, University of Novi Sad.

6. REFERENCES

Erica D. Kuligowski, Steven M. V. Gwynne, Michael J. Kinsey, Lynn Hulse - *Guidance for the Model User on Representing Human Behavior in Egress Models*, Fire Technology, 2017

John Drury and Chris Cocking - *The mass psychology of disasters and emergency evacuations: A research report and implications for practice*, University of Sussex, 2007.

M. J. Kinsey, S. M. V. Gwynne, E. D. Kuligowski, M. Kinateder - *Cognitive Biases Within Decision Making During Fire Evacuations*, Fire Technology, 2018.

SRPS TP 21: *Technical recommendations for urban and civil engineering measures of fire safety for residential, commercial and public buildings*, 2003, Belgrade, Serbia

Long Shi, Qiyuan Xie, Xudong Cheng, Long Chen, Yong Zhou, Ruifang Zhang - *Developing a database for emergency evacuation model*, Building and Environment 44, 2009

UDK 614.8.086
https://doi.org/10.18485/fb_ic4hs.2018.18

CONTEMPORARY CBRN (CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR) THREATS AND ADEQUATE RESPONSE – REAL SITUATION TRAINING

Boris RAJČIĆ[*], Gvozden TASIĆ[**], Vladimir KARIĆ[***], Bojan RADAK[****], Dubravka MILOVANOVIĆ[*****]

Abstract: Testing and training in the field of chemical, biological, and radiation detection, for decontamination and protection against radiological agents, toxic chemicals and biological agents, are emerging security fields. They are gaining significance due to the increasing number of events involving the use of these substances in public places. Indoor (laboratory) and outdoor testing and training processes are both necessary for developing an adequate response and adequate procedures. Testing is required for decontamination equipment and agents, as well as for decontamination process efficiency. It is important to investigate and compare the effects of real outdoor conditions and standard laboratory conditions. Periodical trprljavainings are crucial for enabling first-responders to prevent or respond to and recover from the full spectrum of chemical, biological, radiological and nuclear threats. Various scenarios for outdoor trainings are being developed in order to make the trainings as realistic as possible. For example, these scenarios may include small quantities of pyrotechnics as simulators of dirty bombs when the detection of the scattered material in the environment is the subject of training. Also, the trainings can include toxic materials found in the environment as a result of accidents, natural disasters, misuse, as well as radiological emitters (open and sealed). The safety strategy during the trainings includes using highly effective protective clothing and equipment. Trainings in realistic conditions and with live agents, even proxies, are generally regarded as the only way to

[*] MSc, Research Assistant,Vinca Institute of Nuclear Sciences, University of Belgrade, Belgrade, Serbia, boris@vinca.rs

[**] Research Assistant, Vinca Institute of Nuclear Sciences, University of Belgrade, Belgrade, Serbia, gvozden.tasic@vin.bg.ac.rs

[***] MSc, Research assistant ,Vinca Institute of Nuclear Sciences, University of Belgrade, Belgrade, Serbia, ppz@vinca.rs

[****] Science Advisor Vinca Institute of Nuclear Sciences, University of Belgrade, Belgrade, Serbia, bradak@vin.bg.ac.rs

[*****] PhD, Vinca Institute of Nuclear Sciences, University of Belgrade, Belgrade, Serbia, duca@vinca.rs

fully prepare first-responders and other specialists for adequate procedures, the stress level and decision-making capabilities in cases of high-risk events.

Keywords: CBRN agents, training, detection, decontamination, PPE

1. INTRODUCTION

In recent years, the number of terrorist attacks involving toxic and deadly agents has been increasing. They underscore the magnitude and importance of emergency response procedures in cases of events that include chemical, biological, radiological, or nuclear (CBRN) agents. Besides the situations where CBRN agents are released as an act of war or terrorism, there are everyday situations where accidents involving toxic materials can occur. To ensure a proper reaction of first-responders (police, firefighters, the military, explosive specialists, medical personnel), it is necessary to develop and constantly improve specific training and testing programs which can provide realistic threat training, while remaining within safety and legislative boundaries (Cekovic, et al., 2004; Fatah, et al., 2001; Yang, et al., 1992). Testing and training includes the detection of agents, as well as the use of personal protection equipment, sampling procedures (if needed), and decontamination procedures (Bodurtha & Dickson, 2016). Testing and training should include a theoretical and practical part. The theoretical part is delivered in classrooms, and the practical part is delivered both indoors, in a laboratory, and outdoors, at specialized sites. Besides their significance for the training of first-responders, these practical indoor and outdoor activities are important for the evaluation and comparison of the detection and decontamination effects between outdoor conditions and standard laboratory conditions (Šutulović & Ceković, 2004; Guzman, et al., 2016).

2. CHARACTERISTICS AND TYPES OF CBRN AGENTS

Hazardous chemical substances have the potential to harm or destroy living tissue or disrupt vital processes, leading to incapacitation, illness or death. Of all CBRN substances, the chemical ones are the most common, due to their ubiquity in the supply chain, economy and everyday life. Besides Chemical Warfare Agents (CWA), there are other toxic chemicals and explosive precursors, the most common of which are Toxic Industrial Materials (TIM). Some TIMs are: ammonia, chlorine, cyanogen chloride, hydrogen cyanide, phosgene, etc. (Ghosh, et al., 2010; Sandor, 2014; Fatah, et al., 2001).

It is common knowledge that ionizing radiation is dangerous to health and life due to the changes it causes in cell metabolism, disrupting the functioning of an organism and sometimes leading to death. There are two types of ionizing radiation: electromagnetic radiation (gamma, X-ray, and UV radiation) and corpuscular radiation (alpha and beta particles, protons, neutrons, and fragments of heavy atomic nuclei) (Cekovic, et al., 2004; Kumar, et al., 2010). Radiological agents have an impact on deoxyribonucleic acid (DNA) itself, which causes disorder in DNA synthesis i.e. has a detrimental effect on blood, reproductive organs, and young cells.

Biological agents have many ways of causing mass casualties due to their high lethal potential, which is generally higher than that of chemical agents. The equipment and means

for producing bio-agents are fully available on the civilian market (even from internet shops), and are not always sold under the supervision of relevant security services. Bio-weapons are easy to hide and colourless and odourless, unlike chemical weapons. Biological agents include pathogenic bacteria, fungi, viruses, and biological toxins. These agents can cause fatal or chronic illness, leading to epidemics, mass panic, and the disruption of social order (Lu, et al., 2010). The Centers for Disease Control and Prevention (CDC) classifies biological agents into three categories: A, highest-priority pathogens (Bacillus anthracis, Clostridium botulinum toxin, Variola mayor, filoviruses-ebola), B, second highest-priority bio-agents (Brucella species, Salmonella species, Escherichia coli, Chlamydia psittaci, Ricin), and C, emerging pathogens that could be engineered for mass dissemination (Nipah virus, Hantavirus, Yellow fever virus, Multi-drug-resistant tuberculosis) (Cekovic, et al., 2004; Chomiczewski, 2003; Masthan, et al., 2012).

Nuclear weapons are by far the most dangerous weapons on Earth. They can jeopardize the natural environment and the lives of future generations on a long-term basis, destroy cities and even countries, killing millions of people. Fortunately, they have only been used twice in warfare. The best protection against such catastrophic weapons is disarmament; a number of multilateral treaties have been established with the aim of preventing nuclear proliferation and testing (United Nations Office for Disarmament Affairs, 2018).

3. TRAININGS FOR CBRN THREATS

It is possible to efficiently enable first-responders to adequately prevent, prepare for or respond to, and recover from the full spectrum of CBRN threats if they undergo trainings with real or proxy CBRN agents.

When designing a training course, it is important to consider the entry knowledge of the trainees. For example, Vinča Institute offers different difficulty levels of CBRN trainings – using entry tests to determine the appropriate level. The type of training can also vary – the course needs to be adapted to each specialist group of first-responders.

The basic-level CBRN general and safety awareness training is a classroom course which familiarizes the trainees with CBRN materials, their respective properties and the measures that can be taken for protection. CBRN detection training covers detection techniques for the agents. In CBRN decontamination training, the participants master decontamination techniques. Advanced live agent trainings, CBRN forensics, and scenario trainings are intended for participants with considerable entry knowledge, since those trainings cover analyses of CBRN agent incidents to determine the magnitude of the problem, sampling and operating as a group within a live CBRN environment. Training with live agents and in realistic situations is invaluable in evaluating the behaviour and real capabilities of individuals and groups.

In responder training for CBRN threats, the responders must become familiar with all aspects of CBRN activities. The theoretical part of the training should provide them with knowledge of CBRN agents and their physiochemical properties (colour, odour, density, ways of entering the human body, etc.). Knowing the types of decontamination equipment and the categories of Personal Protective Equipment (PPEs) is mandatory. All theoretical

knowledge should be enacted in realistic situations in the practical part of the course. The scenarios should include some simulators of dirty bombs, e.g. small quantities of pyrotechnics; simulators of scattered material in the environment; contaminated objects from everyday life (seats, vehicles, suitcases, etc.).

After the trainees decontaminate the scenario area, the most important part of the training is removing the PPEs in the right way and correct order. The concept of three zones can be applied, depending on the level of the CBRN hazard and contamination: the hot zone, where significant contamination with CBRN agents has been confirmed or is strongly suspected, but not characterized, and presumed to be life threatening (both skin contact and inhalation); the warm zone, where contamination is possible but active release has ended and initial monitoring exists; the cold zone, where contamination is unlikely – this zone covers the area beyond the expected significant dispersal range of the initial event and the secondary contamination range caused by traffic and emergency responders. When the detection and decontamination in the hot zone are done, the undressing process starts. This process has several stages. First, special equipment (detection instruments, decontamination fitment, communications, etc.) is put aside and deposed in protective shield containers. The process of assembling the equipment and undressing the trainees must be supervised by a safety officer. Next comes decontamination and the disposing of the PPE during the transit from the hot to the warm zone. The PPE must be decontaminated in a manner deemed appropriate for the identified hazard (biocide preparation, water, decontamination solution, detergent). The disposal order is: coveralls half way up → overboots → gloves → all of the coveralls. In CBRN operations, using protective clothing is required, with at least two pairs of gloves, of which the inner gloves are removed at the end. The mask with a filter should be removed from the face as late as possible. This is usually done during the transit from the warm to the cold zone. Without enough practice or on impulse, trainees may remove the mask at the beginning of the undressing process, exposing the person to a facial skin infection or the inhalation of a

dangerous agent. The preparation and implementation of decontamination in a safe way requires repeated training and exercise.

The trainees get in contact with detection equipment/instruments, PPE, and practical decontamination procedures and techniques. Here, we outline the protective equipment and decontamination activity only.

Because of the limited capacity of human senses to detect CBRN agents, detection and identification is supported by instruments or appropriate sets. Detection is not just realizing that there is a threat, but also locating it with more or less precision, depending on the instrument. There are many instruments and detection kits for the rapid detection and identification of chemical agents.

First-responders sent to a potential CBRN contamination area must be provided with accurate up-to-date information. The organizers must assess the risk of a hazardous substance release and the conditions present, instruct the responders, and base Personal Protective Equipment (PPE) selection on that knowledge. Two basic aspects are of significance: respiratory protection and skin (dermal) protection. Based on these, the PPE is a set comprising a respiratory mask and a personal protective ensemble. Personal protective clothing typically consists of: an over-garment – protection for the body (torso, arms, legs), footwear – protection for the feet (overboots on top of regular footwear), and gloves – protection for the hands (made from air-impermeable materials or butyl rubber gloves and butyl rubber gloves additionally coated with neoprene).

At low hazard levels, air-permeable protective clothing selection is suitable. To protect the hands, gloves made of air- and liquid-impermeable materials are mandatory. High CBRN hazard levels, i.e. severe liquid contamination, may dictate the use of a PPE suit based on impermeable materials. An alternative to a non-ventilated impermeable protective suit is based on a simple, lightweight, disposable air- and liquid-impermeable material with an absorptive liner underneath. This concept solves the problems of decontamination, the effect of pinholes, bad closures and occlusion. When only radioactive dust hazard exists, using a full-face respirator, gloves, disposable overboots and lightweight disposable dust-impermeable coverall wear on top of regular working clothing is sufficient (Holland & Cawthon, 2014).

4. DECONTAMINATION OF CBRN AGENTS

Decontamination is simply the removal of the contamination agent by mechanical or chemical means or by dilution.

Mechanical methods are the simplest and fastest to implement; removing the outerwear results in reducing the pollution by 85–90%. It should be implemented in the case of mass casualties. The chemical way is to neutralize the toxic effect of a hazardous substance by changing its chemical structure to a new, non-hazardous or less hazardous one. A biological agent can be neutralized by its chemical destruction (Holland & Cawthon, 2014; Oudejans, et al., 2016). The most common method of decontamination is dilution – reducing the concentration of the hazardous substance by scattering it into a thinner one. In the contaminated area, the fastest available thinner is water. In practice, this is done

using a water jet or a so-called decontamination booth. This is also the most economical way of execution. However, in most cases, the use of water does not alter the composition of a hazardous substance and only lowers the concentration. The usual decontamination solutions for chemical decontamination are: 10% $Ca(ClO)_2$ (calcium hypochlorite), 5% Na_2CO_3 (sodium carbonate), 5% Na_3PO_4 (sodium phosphate), 1% HCl (hydrochloric acid), a water solution with detergent (Cekovic, et al., 2004; Amitai, et al., 2010; Šutulović & Ceković, 2004).

5. CONCLUSION

Today's CBRN threats are becoming more probable, more complex, and are developing both in type and ways of occurrence. Staying up-to-date with all of their aspects is vital. These threats come not only from war-related activities, but also arise in everyday life situations in accidents involving toxic or harmful materials. They are now omnipresent, in industry and also in civilian life. Methods of harmful agent detection therefore need constant improvement. Testing is required for protection and decontamination equipment, as well as for decontamination process efficiency.

Realistic situation experience outdoors is invaluable, both in training and in testing the methods and equipment:

- Comparing laboratory results with effects in outdoor real situations;
- Testing the efficiency of detection and decontamination methods in the field;
- Using realistic scenarios, with live agents (real or proxy) as the key to fully preparing personnel for operations, stress levels, and decision-making in a CBRN event;
- Revealing important flaws in individual or group preparedness so that they can be rectified (psychological adequacy, group support, group cohesion and synchronization, etc.);
- Tailoring the trainings is important, so that they are most effectively adopted by groups of different compositions and levels of knowledge, experience, purpose, etc.

6.REFERENCES

United Nations Office for Disarmament Affairs. (2018). Retrieved from United Nations: https://www.un.org/disarmament/wmd/nuclear/

Amitai, G., Hironobu, M., Andersen, J., Koepsel, R., & Russell, A. (2010). Decontamination of chemical and biological warfare agents with a single multi-functional material. Biomaterials, 31(15), 4417-4425.

Bodurtha, P., & Dickson, E. (2016). Decontamination science and Personal Protective Equipment (PPE) selection for Chemical-Biological-Radiological-Nuclear (CBRN) events. Alberta: Defence Research and Development Canada.

Cekovic, B., Mladenovic, V., Lukovic, Z., Karkalic, R., & Krstic, D. (2004). Comparative Research on Chemical, Radiological and Biological Decontamination Efficiency of Present Decontaminants and of Multipurpose Emulsion-Based Decontaminant (in Serbian). Belgrade: Scientific Technical Information, Military Technical Institute.

Chomiczewski, K. (2003). The bioterrorism threat. Epidemiological review, 57(2), 349-353.

Fatah, A., Barrett, J., Arcilesi, R., Ewing, K., Lattin, C., Helinski, M., et al. (2001). Guide for the Selection of Chemical and Biological Decontamination Equipment for Emergency First Responders. Washington, DC: DIANE Publishing.

Ghosh, T., Prelas, M., Viswanath, D., & Loyalka, S. (2010). Science and Technology of Terrorism and Counterterrorism (2nd ed.). Boca Raton: CRC Press Taylor & Francis Group.

Guzman, R., Navaro, R., Ferre, J., & Moreno, M. (2016). RESCUER: Development of a Modular Chemical, Biological, Radiological, and Nuclear Robot for Intervention, Sampling, and Situation Awareness. Journal of Field Robotics, 33(7), 931-945.

Holland, M., & Cawthon, D. (2014). Personal protective equipment and decontamination of adults and children. Emergency Medicine Clinics of North America, 33(1), 51-68.

Kumar, V., Goel, R., Chawla, R., Silambarasan, M., & Sharma, R. (2010). Chemical, biological, radiological, and nuclear decontamination: Recent trends and future perspective. Journal of Pharmacy & Bioallied Sciences, 2(3), 220-238.

Lu, T., Yiao, S., Lim, K., Jensen, R., & Hsiao, L. (2010). Interpretation of biological and mechanical variations between the Lowry versus Bradford method for protein quantification. North American Journal of Medical Sciences, 2(7), 325-328.

Masthan, K., Shanmugam, K., Aravindha, B., & Tathagata, B. (2012). Virus as a biological-weapon. International Research Journal of Microbiology, 2(6), 237-239.

Oudejans, L., O'Kelly, J., Evans, A., Wyrzykowska-Ceradini, B., Touati, A., Tabor, D., et al. (2016). Decontamination of Personal Protective Equipment and Related Materials Contaminated with Toxic Industrial Chemicals and Chemical Warfare Agent Surrogates. Journal of Environmental Chemical Engineering, 4(3), 2745-2753.

Sandor, S. (2014). Latest technologies suitable for chemical decontamination of sensitive equipment and interior for the Hungarian defence forces. Katonai Technical Scineces, 130-136.

Šutulović, L., & Ceković, B. (2004). Overview of Perspectives for the Destruction of Toxic Chemicals and CWA According to the Chemical Weapons Convention. 4th International Conference of the Chemical Societies of the South-East European Countries on Chemical Sciences in Changing Times: Visions, Challenges and Solutions. II, p. 148. Belgrade: Serbian Chemical Society.

Yang, Y., Baker, J., & Ward, R. (1992). Decontamination of Chemical Warfare Agents. Chemical Review, 92, 1729-1743.

UDK 659.3:614.8
https://doi.org/10.18485/fb_ic4hs.2018.19

SOCIAL MEDIA AS AN EMERGENCY MANAGEMENT TOOL IN THE CONTEXT OF HUMAN SECURITY

Nevena ŠEKARIĆ[*], Filip STOJANOVIĆ[**]

Abstract: The technological revolution has brought new forms of connecting and communication between people. Development of new technologies has led to the Internet based applications known as 'social media' that enable people to interact and share information through the media that were non-existent or widely unavailable 15 years ago. Examples of social media include blogs, chat rooms, discussion forums, wikis, YouTube Channels, LinkedIn, Facebook, Instagram, Twitter, etc.

Bearing in mind that emergencies and disasters affect people's lives, properties and livelihoods, human security is directly concerned with reducing and, when possible, removing the insecurities caused by these phenomena. Considering the key role of crisis communication in case of emergencies, social media, with all their advantages, connect stakeholders in the emergency management. Namely, this (relatively) new concept in communication facilitates the vital two-way communication between the emergency management agencies and the public, and allows to quickly and specifically share information with state and local authorities and the public as well. Through the use of social media, especially Twitter and Facebook, someone can disseminate important information to individuals and communities, while also receiving essential real-time updates from those with first-hand awareness. Moreover, social media are considered an imperative to the emergency management because the public use these communication tools on daily basis.

There are many studies among academics that focus on the role of social media in the emergency management practice and policy. Many of these papers and reports describe how a wide range of international, state, and local organisations have successfully used social media during emergencies and disasters and how they can be used to improve response and recovery capabilities and to create disaster-resilient communities. Based on literature review, this paper summarises how social media have been used by the emergency management officials and agencies. It also examines the potential benefits as

[*] PhD Candidate, University of Belgrade Faculty of Security Studies, nevenasekaric@gmail.com
[**] MA, Researcher, Public Policy Research Centre, stojanovicgf@gmail.com

well as the implications of using social media during emergencies and disasters in the context of human security.

Keywords: social media, emergency management, human security, communication tool, disasters

1. INTRODUCTION

Since social media (SM) have permeated almost every aspect of social life, security domain has not remained an exception. Due attention has been paid to the nexus of SM usage and prevention of disasters and emergencies as a notable part of the security domain. Viewed through human security's lenses, natural disasters and emergencies, driven by climate and human-induced changes, increasingly reduce access to and quality of natural resources that are crucial to sustain livelihoods. Accordingly, the emergency management (EM) has become the most important tool in combating disasters and emergencies. Since the EM requires timely disposition of relevant information and coordination of all stakeholders' activities, SM use enables dissemination of relevant information to individuals and communities and receiving real-time updates from those with first-hand awareness. Most recent researches show how SM, especially Twitter and Facebook, can be used in EM. Some of them highlighted that SM "give emergency mangers abilities to communicate, interact with, and respond to the public on a hitherto unseen scale" (Latonero & Shklovski, 2011: 14), that it can cross data from social media in order to visualise data and geographic analysis (MacEachren *et al.*, 2011: 2), "can facilitate the right authorities to enhance their awareness of time-critical situations and make better decisions for emergency response" (Yin *et al.*, 2012: 4238), and, last but not least, it can increase public confidence in emergency management institutions (Panagiotopoulos *et al.*, 2016: 21).[1]

2. HUMAN SECURITY-DISASTERS AND EMERGENCIES NEXUS

The UNDP Human Development Report identifies two main aspects of human security: first, "safety from such chronic threats as hunger, disease and repression", and, second, "protection from sudden and hurtful disruptions in the patterns of daily life – whether in homes, in jobs or in communities" (1994: 23). Since this Report, the concept of human security has been broadly discussed in the literature. Talking about the need to establish much broader concept for analysing security issues apart from exclusively military terms, Kofi Annan stressed that "...environmental disasters present a direct threat to human security..." (2000: 4). In terms of vulnerability as a defining characteristic of the concept of human security, Astri Suhrke recognised victims of natural disasters as one of the vulnerable categories (1999: 272).

The problem of human security becomes especially tangible when it comes to the disturbance of habitat where people live. Namely, "while the focus of human security is

[1] In addition to this, Reuter & Kaufhold noticed that "...it appeared that nearly no emergency exists without articles on the use of social media there" (2018: 42).

the individual, the processes that undermine or strengthen human security are often external to the locality of communities where individuals reside" (Barnett & Adger, 2007: 641). As a result, disasters and emergencies and lack of sustainable resources as a consequence, are being framed as a security problem. This problem does not require only the actions of emergency officials, but also of the whole community. According to Birkmann, "emergency management and disaster response units play crucial role" during disasters (2006: 34-35), thus representing key security providers in crises times. Emergencies could undermine "the capacity of states to provide the opportunities and services that help people to sustain their livelihoods" (Barnett & Adger, 2007: 639). Consequently, all the mechanisms employed for strengthening human security, at individual or community level, are likely to be used in order to achieve positive results.[2]

3. SOCIAL MEDIA'S ROLE IN EMERGENCIES

Common characteristic of SM definitions is the view that SM, with all their performances, affect the nature of contemporary communication.[3] Today, SM include blogs, discussion forums, chat rooms, wikis, YouTube channels, LinkedIn, Facebook, Twitter etc.

In recent years, SM have been quickly revealed as an emergent, significant and often accurate form of public participation and backchannel communication (Palen, 2008: 76). The emergency management organisations (EMOs) have started to integrate SM services into their communication practices, either in a day-to-day communication or during emergency events. Various studies and European countries' practises show that the SM can be useful tool in the emergency communication when the emergency authorities are expected to provide timely and reliable information as a signal of keeping the situation under control. Using such information, SM users (and not only them) interpret emergency risks and make decisions about their own actions (Comfort, 2007: 189). "Social media is being used as an alternative way for emergency managers to communicate with the public and with each other" (White, 2011: 2); furthermore, existing studies focus both on natural (earthquakes, hurricanes, floods, tsunamis) and human-induced disasters (terror attacks, uprisings). Testifying to the increased use of SM in emergencies, White *et al.* point out

[2] Ehnis has noticed a shift in emergency management sector from seeing the general public as something that needs to be protected to strengthening communities as a valuable resource to mitigate the effects of an emergency event (2018: 41). This shift is nearly connected with the concept of strengthening community resilience where the community is actively prepared for potential emergency events. According to this author, social media services are one aspect through which emergency management organisations are supporting community resilience (2018: 42).

[3] According to Boyd and Ellison, social network sites are "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system" (2007: 211). Kaplan and Haenlein offer definition of social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content" (2010: 61). More straightforward determination of social media reads "Internet-based applications that enable people to communicate and share resources and information" (Lindsay, 2011: 1).

that numerous emergency response institutions use Facebook[4] for disseminating information, communicating with each other, and coordinating emergency management activities (2009: 377-378). For example, Facebook and Twitter took an ever growing role in disaster response during Hurricane Sandy[5] (Cohen, 2013; Simon *et al.,* 2015) and Katrina, Haiti earthquake[6] (Sarcevic *et al.*, 2012), 11/9, Boston Marathon bombings, Serbian floods[7], etc.[8]

Especially important issue when it comes to SM usage is the *situational awareness* of the public in time of emergencies. Namely, studies have shown that many citizens across Europe are already using SM to share and look for information during emergencies and it is expected that their usage will only increase in the future (Reuter & Spielhofer, 2017: 176). The main beneficial reasons for using SM as an information source during emergencies is that they have been seen as faster (76%) and more accessible (54%) than conventional media (*Ibid.*).

Lindsay points out that SM usage for emergencies and disasters on an organizational level may be conceived as two broad categories. First, SM can be used somewhat passively to disseminate information and receive user feedback via incoming messages, wall posts, and polls.[9] However, SM presence is not limited to disseminating information to a wider public; it can be used to *interact* with the audience which makes the SM presence a valuable two-way communication channel during emergency events. Thus, second approach involves the systematic use of SM as an EM tool. Systematic usage might

---

[4] Interesting fact is that the creators of social media recognise their importance in crisis communication. Thus, Facebook has developed a research platform (*Facebook Research*) where great attention is paid to inquiries on the use of new technologies in the emergencies.

[5] According to Simon *et al.,* Hurricane Sandy in 2012 was a "turning point where the majority of emergency authorities and first responders from the East Coast in the United States adopted social media as the main communication channel with the public" (2015: 615).

[6] Yates and Paquette stressed that Haiti earthquake was the first time ever that the U.S. Government extensively relied on the social media to coordinate knowledge and action between cooperating response agencies including the U.S. Agency for International Development (USAID), the U.S. State Department, and the U.S. armed forces (2011: 7).

[7] For example, during the floods in Serbia in 2014, in the period from 14 to 21 May, Twitter users exchanged 814.751 tweets (558.301 with *#poplave* and 256.450 with *#SerbiaFloods*) (Numbers are available at: http://www.tvitni.me/index.php?strana=blog&blog_id=181).

[8] In line with the above, Rasmussen and Ihlen conducted a research on published literature on social media's usage in risk and crisis communication (2017). The results show that the number of studies on social media, risk, and crisis communication are increasing – in 2009, there were only 9 academic articles published in relevant academic journals related to crises and disasters or information management. But in 2015, that number increased to 49 articles (2017: 6). Additional research conducted for this purpose through *Google Scholar* has shown that in period 2016-2017 at least 50 academic articles on this topic (the research was conducted by keyword search, according to a custom, two-year range (2016-2017)) were published. In Rasmussen and Ihlen and in our research as well, Twitter dominates the articles which analyse particular social media in crisis. Still, in Serbia there is no research (qualitative or quantitative) on SM role in emergencies.

[9] This is how most emergency management organisations, including the Federal Emergency Management Agency (FEMA), have used social media.

include: (1) a SM usage as a medium to conduct emergency communications and issue warnings; (2) using SM to receive victim requests for assistance; (3) monitoring users' activities and posts to establish situational awareness; and (4) using uploaded images to create damage estimates, among others (2011: 1).[1011]

Broadcasting, engagement, intelligence and dispatching are seen as main social media capabilities of EMOs, according to Ehnis (2018: 278). Broadcasting refers to the information distribution through social media, engagement is related to the interaction with the audience, intelligence is concerned with the utilisation of social media channels as a source of information for the organisations, while dispatching relates to the utilisation of a social media channel as the basis for dispatching emergency resources to respond to an event (2018: 276).

According to Simon *et al.*, SM as a tool of our daily lives may serve as an integral and significant component of crises responses. Authors underline several findings on the benefits of SM usage in emergencies: (1) during disasters, SM provides access to relevant and timely information; (2) SM has changed the information dissemination pathways in emergencies; (3) SM enables transformation of the ways in which emergencies are tracked; (4) Social media are reliable during disasters when other channels are overwhelmed; (5) SM can self-regulate misinformation in emergencies through the masses (2015: 609-619).

4. DISADVANTAGES OF SOCIAL MEDIA'S USAGE IN EMERGENCIES

The risk of missing those parts of population who are most vulnerable in emergencies and with limited access to the Internet and, thus, most in need for relevant information, is recognised as the biggest disadvantage of SM usage in emergencies. Particularly, citizens with low socio-economic status are those with the lowest Internet accessibility (Zickuhr, 2013: 3).

The possibility of the escalation of a problem where obsolete, incorrect or false information can be distributed through SM during emergencies is another problematic issue.[12] Apart from having a negative impact on the reaction of the authorities, incorrect

[10] Lindsay points out that most emergency management organisations have confined their use of social media to the dissemination of information because of the underdevelopment of different stages of their systematic use (2011: 2). Regarding this, there is an attitude that all stakeholders in charge of emergency management that want to use social media should reach a consensus on the goals that are to be achieved by using these applications (White, 2011: 32).

[11] Summing up 'lessons learned' and 'best practices' in the domain of social media's usage in emergencies, Lindsay highlights the need to: (1) identify target audiences for the applications, such as civilians, nongovernmental organisations, volunteers, and participating governments; (2) determine appropriate types of information for dissemination; (3) disseminate information the public is interested in; and (4) identify any negative consequences arising from the application – such as the potential spread of faulty information – and work to eliminate or reduce such consequences (2011: 6).

[12] For example, in the case of a Japanese earthquake and tsunami in 2011, tweets referring to requests for victim assistance were retweeted after the victims had already been rescued (Acar & Muraki, 2011: 398).

information can obscure the perception and level of awareness of the current situation, jeopardising the security of both first responders and a wider population.

Another disadvantage refers to the deliberate attempts to provide incorrect information in order to interfere with or disable an adequate response in emergencies. Therefore, as the main preventive mechanism, it is recommended to adopt a comprehensive initiative, strategy or system of sanctions aimed at minimising the effects of disinformation and such intentions (Lindsay, 2011: 7). Latonero & Shklovski's findings have shown that the validity of user-based information is very questionable when it comes to officials' acting on the basis of this information (2011: 10-12). Increasing amount of public information can produce less control over the particular situation by officials, thus resulting into the validation of their authenticity under pressure (Zook *et al.*, 2010: 27-29). Therefore, the knowledge and ability to utilise SM effectively within EMOs is of paramount importance.

Technological limitations of SM are considered as another disadvantage of social media's usage in emergencies. In other words, "Although social media may improve some aspects of emergency and disaster response, overreliance on the technology could be problematic under prolonged power outages" (Lindsay, 2011: 7), primarily due to the inability of smartphone and tablet batteries to last for more than a couple of hours, thus confronting us with the need to reconsider alternative options for alarming in these circumstances.

5. CONCLUSION

Existing studies highlight global and extensive usage of SM during emergencies, influencing people's communication in day-to-day interactions and during crises. As the literature review has shown, SM have a significant role in enhancing human security in disasters and emergencies, both on individual and community level.

Beside few disadvantages, social media have been a driver of emergency communication so far. Nevertheless, their role in peacetime should not be neglected. It can be used in informing, educating and promoting relevant content to the EMOs activities, thus raising awareness and public confidence in authorities. It is important to point out that not everyone uses SM, hence it can be only upgraded, but certainly not as a replacement for conventional warning and informing systems.

Concrete benefits of SM usage in emergencies can be outlined as follows: (1) SM provide access to relevant and timely information; (2) SM are reliable when other mechanisms are overloaded; (3) SM provide transformation of the ways of emergency monitoring; (4) officials can regulate disinformation in emergencies through SM and disseminate information the public are interested in; (5) SM enable visualisation of relevant data (maps, statistics, infographics, photos, videos, etc.); (6) Surveys can be distributed anytime through SM in order to get quick feedback, (7) SM are cheap, timely, adaptable, available, and transparent way of communication which makes them additional and reliable channel of emergency communication. Considering that SM are of increasing importance to EMOs, which are still in the stage of learning and evaluating their effectiveness, there is certainly a need to create and establish the best know-how practices.

6. REFERENCES

Acar, A., & Muraki, Y. (2011). Twitter for crisis communication: lessons learned from Japan's tsunami disaster. *International Journal of Web Based Communities*, *7*(3), 392-402.

Annan, K. (2000). *Report of the Secretary-General on the work of the Organization*. United Nations General Assembly. Retrieved from: http://www.un.org/documents/sg/report00/a551e.pdf.

Barnett, J., & Adger, W. N. (2007). Climate change, human security and violent conflict. *Political geography*, *26*(6), 639-655.

Birkmann, J. (2006). Measuring vulnerability to promote disaster-resilient societies: Conceptual frameworks and definitions. *Measuring vulnerability to natural hazards: Towards disaster resilient societies*, *1*, 9-54.

boyd, d. m., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of computer‐mediated Communication*, *13*(1), 210-230.

Cohen, S. E. (2013, March). Sandy marked a shift for social media use in disasters. *Emergency Management*. Available at*:* http://www.emergencymgmt.com/disaster/Sandy-Social-Media-Use-in-Disasters.html.

Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review*, *67*, 189-197.

Ehnis, C. F. (2018). *Social Media within Emergency Management Organisations-A case study exploring Social Media utilisation for Emergency and Disaster Management*. PhD Thesis. Sydney: The University of Sydney Business School.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, *53*(1), 59-68.

Latonero, M., Shklovski, I. (2011). Emergency Management, Twitter, and Social Media Evangelism, *International Journal of Information Systems for Crisis Response and Management*, 3(4), 1-16.

Lindsay, B. R. (2011, September). Social media and disasters: Current uses, future options, and policy considerations. CRS Report for Congress. Retrieved from: https://ofti.org/wp-content/uploads/2012/07/42245_gri-04-11-2011.pdf.

MacEachren, A. M., Robinson, A. C., Jaiswal, A., Pezanowski, S., Savelyev, A., Blanford, J., & Mitra, P. (2011, July). Geo-twitter analytics: Applications in crisis management. In *25th International Cartographic Conference* (pp. 3-8).

Palen, L. (2008). Online social media in crisis events. *Educause Quarterly*, *31*(3), 76-78.

Panagiotopoulos, P., Barnett, J., Bigdeli, A. Z., & Sams, S. (2016). Social media in emergency management: Twitter as a tool for communicating risks to the public. *Technological Forecasting and Social Change*, *111*, 86-96.

Rasmussen, J. & Ihlen, Ø. (2017). Risk, Crisis, and Social Media: A systematic review of seven years' research. *Nordicom Review 38*(2), 1-17.

Reuter, C., & Kaufhold, M. A. (2018). Fifteen years of social media in emergencies: a retrospective review and future directions for crisis informatics. *Journal of Contingencies and Crisis Management, 26*(1), 41-57.

Reuter, C., & Spielhofer, T. (2017). Towards social resilience: A quantitative and qualitative survey on citizens' perception of social media in emergencies in Europe. *Technological Forecasting and Social Change*, *121*, 168-180.

Sarcevic, A., Palen, L., White, J., Starbird, K., Bagdouri, M., & Anderson, K. (2012, February). "Beacons of hope" in decentralized coordination: Learning from on-the-ground medical twitterers during the 2010 Haiti earthquake. In *Proceedings of the ACM 2012 conference on computer supported cooperative work* (pp. 47-56). ACM.

Simon, T., Goldberg, A., & Adini, B. (2015). Socializing in emergencies—A review of the use of social media in emergency situations. *International Journal of Information Management*, 35(5), 609-619.

Suhrke, A. (1999). Human security and the interests of states. *Security Dialogue*, *30*(3), 265-276.

Tvitni.me (2014, May). Dešavanja na tviteru za vreme #poplave kroz reči i brojeve. Available at: http://www.tvitni.me/index.php?strana=blog&blog_id=181.

United Nations Development Program (UNDP). (1994). *Human Development Report 1994*, New York: Oxford.

White, C. (2011). *Social media, crisis communications and emergency management: Leveraging Web 2.0 technology*. Boca Raton, FL: CRC Press.

White, C., Plotnick, L., Kushma, J., Hiltz, S. R., & Turoff, M. (2009). An online social network for emergency management. *International Journal of Emergency Management*, *6*(3-4), 369-382.

Yates, D., & Paquette, S. (2011). Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake. *International journal of information management*, *31*(1), 6-13.

Yin, J., Lampert, A., Cameron, M., Robinson, B., & Power, R. (2012). Using social media to enhance emergency situation awareness. *IEEE Intelligent Systems*, *27*(6), 52-59.

Zickuhr, K. (2013). *Who's Not Online and Why.* Pew Research Center. Retrieved from: http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_Offline%20adults_092513_PDF.pdf.

Zook, M., Graham, M., Shelton, T., & Gorman, S. (2010). Volunteered geographic information and crowdsourcing disaster relief: a case study of the Haitian earthquake. *World Medical & Health Policy*, *2*(2), 7-33.

UDK 659.3:343.85
https://doi.org/10.18485/fb_ic4hs.2018.20

THE ROLE OF MEDIA IN VIOLENCE PREVENTION

Aleksandra ILIĆ*

Abstract: Violence has always been one of the topics that attracts great public attention. It is visible today in everyday news reports on crime with violence as dominant issue. Also, violence is the common topic of films and television series. The conclusion that can be derived from it is that violence is everywhere around us. On the other hand, it seems that society is very sensitive when it comes to some forms of violence acts. In that sense the role of media in violence prevention can be understood as both positive and negative. Media are the most powerful source of information and have great influence on public understanding of the problem of violence. Public reaction to violence depends usually on media construction of it. The problem with media construction of violence is its deviation from reality to a greater or lesser extent. Media image of violence is a combination of real information and construction and is usually based on sensationalism. The positive side of media's focus on violence is that they inform the public on the dimensions and characteristics of some forms of violence, which is one of the important aspects of its prevention. Also, a better understanding of the crime is crucial in its suppression. This is especially true when it comes to domestic violence, paedophilia, rape or juvenile delinquency. On the other hand, very often these mentioned crimes are presented in the media in an inadequate way which causes moral panic reaction with all its negative consequences as an irrational fear of crime or labelling some groups of people as common perpetrators. All of it could hamper the efforts of different subjects, especially law enforcement agencies in dealing with violence. In that sense, the conclusion is that only true and unbiased media reporting of violence could make some positive changes in its prevention.

Keywords: media, construction, violent crime, prevention, moral panic;

1. INTRODUCTION

Given the current advent and development of mass media, the influence of the media as a source of knowledge about crime is enormous. A substantial part of social knowledge is gained symbolically from the media, and some of the authors are concerned over media

* Associate Professor, PhD,University of Belgrade Faculty of Security Studies, aleksandra.ilic@fb.bg.ac.rs

content (Surette, 2007:34). That this concern is not unreasonable is indicated by some of the latest criminological research, according to which four fifths (80%) of citizens' views on criminality in general, as well as on some of its types, are based on the information obtained through the media (Ignjatović, 2009:176). We live at the time when the media have taken over a guarding role from the family, replaced the churches as headquarters of cultural values, instead of schools they have started to educate children and youth and to set priority national goals (Ott & Mack, 2010:11). It is therefore necessary to pay special attention to the analysis of the role of the media as a source of knowledge about criminality and their contribution to the creation of a social construction of crime.

Certain forms of crime instinctively attract people and keep their attention for longer time, while other topics, despite being a bigger problem, arouse much less interest. When choosing news, the media also take into account this circumstance, which means it is more effective to draw public attention to 'appropriate' topics such as a violent crime, which causes fear among citizens, and therefore they do not try to do the same with some forms of property crime in relation to which there is greater tolerance.

The choice of crime news is often related to discouraging public attention from real social issues such as unemployment, poverty, economic crisis or other 'burning' issues. In the background of this concealment, there are, by the rule, the efforts of certain political groups to maintain social peace and to achieve the narrow interests of those who possess power. In other words, the control of information in the media represents the very basis of political power. In this sense, the ability to form a convincing discourse for public consumption is vital for sustaining that power (Prajs, 2011:552).

2. MEDIA CONSTRUCTION OF VIOLENCE

As a society we are fascinated by the crime. The stories of crime are ubiquitous not only in movies, newspapers, books, magazines, articles, on the Internet, television, radio, but also in everyday communication. In other words, crime is a central point of discussion (Muraskin & Domash, 2007:13). This fascination is especially evident when it comes to violent crime. Through media coverage of violence, people can experience extreme situations without actually being part of it. In that way people have access to those emotional aspects that are not usually part of everyday life (Svensen, 2008:95).

Violent events meet the need of media to improve readership of newspapers or TV channel ratings. Almost daily, the media present the data on the chances of a woman or child being victims of various forms of violence, and interviews with various experts, psychologists, pedagogues, etc. who provide alarming information on the epidemic proportions of these problems, which is accepted without reserve by the public. It is a general conclusion that all forms of violence are in a constant growth despite the fact that official statistics say the opposite. Important aspects of media construction of crimes are symbolic crimes which usually emphasise the worst, most heinous types of crimes and the most innocent victims (Surette, 2003:44).

It can be said that violent crime has the 'ability' to attract great public attention, which leads to the creation of moral panic. No other form of criminal activity is so much

connected with the issue of morality and attacks on some of the basic values of every modern society (Kosloski, 2010:16). All forms of manifestation of moral panic in relation to violence and stereotypes that are inherent in them have their roots in the stereotype of a bloodthirsty criminal or predator, where such super-predatory discourse distorts reality (Moriearty, 2010:852).

The crimes that dominate public consciousness and policy debates, whose actors are predatory criminals, are not common crimes, but the rarest ones. Our desire to understand and control these incomprehensible and uncontrollable criminals is long-standing and is reflected in much of classical literature. However, the modern mass media have raised the spectre of the predatory criminal from a minor character to a common, ever-present image (Surette, 1994:131,132).

The most common image of a predatory criminal is that he is different from all other 'normal' people. His criminality stems from individual problems. He freely chooses his criminality and is not bound or restrained in any way by normal social rules and values. The predator is always a stranger who suddenly appears in order to commit a crime whereby the choice of the victim is generally not subject to some specific criteria. Predatory victims are in most cases random, helpless and innocent (Surette, 1994: 134,135).

3. MEDIA AND SPECIFIC FORMS OF VIOLENT CRIME

When it comes to specific forms of violent crime, moral panic usually occurs in connection with domestic violence, rape, paedophilia and violent behaviour of young people. Often the media explanation of these forms of violence emphasises what is characteristic of predatory crimes, both in terms of the basic feature of the perpetrators and the typical profile of the victims.

While moral panic is basically a negative consequence of excessive and sensational media coverage of a subject, media coverage of violence can have a positive effect. Violence generally, as well as all its special forms of manifestation, are negative phenomena which must be suppressed both on a preventive and repressive plan. In both cases, the media play an important role, since in order to achieve mentioned effects, it is necessary to provide a consensus in the society. In other words, through continuous and adequate reporting on the problem of violence, public awareness can be raised.

In this sense, the positive effects of the public and thus the media dealing with the phenomenon of domestic violence are the corresponding changes in the criminal legislation of the Republic of Serbia that happened more than sixteen years ago. Namely, in March 2002, the amendments1 to the then valid Criminal Code2 (Article 118a) introduced a relatively new criminal offense of domestic violence that did not exist under

[1] Law on Amendments and Additions to the Criminal Code of the Republic of Serbia ("Official Gazette of the Republic of Serbia", No. 10/02).

[2] Criminal Code of the Republic of Serbia ("Official Gazette of the Republic of Serbia", No. 26/77, 28/77 - corr., 43/77 - corr., 20/79, 24/84, 39/86, 51/87, 6/89 , 42/89 and 21/90 and "Official Gazette of the RS", No. 16/90, 26/91 - decision of the CCJ No. 197/87, 75/91 - decision of the CC RS No. 58/91, 9/92, 49/92, 51/992, 23/93, 67/93, 47/94, 17/95, 44/98, 10/02, 11/02 - corr., 80/02 other law, 39/03 and 67/03).

that name, although various forms of its manifestation were sanctioned earlier in other criminal offenses (murder, serious bodily injury, rape, etc.) (Stojanović &Delić.2013:108). By introducing the mentioned incrimination, the phenomenon of domestic violence has become more visible because the sphere of marriage and family relations has always been treated as a predominantly private sphere of individuals, any interventions being extremely rare, and so the cases of violent behaviour within it have been taboo topic.

After complete silence regarding the issue of domestic violence, a period of intense and constant engagement with this topic in our country started almost two decades ago. However, reporting on domestic violence became at one point overstated. The public began to get the impression that domestic violence is a relatively new phenomenon, i.e. that it had not existed before or that it had been present in a much lesser extent. Over time, ordinary concern has become a moral panic with all its consequences.

The exaggeration in media coverage of the scale and characteristics of domestic violence can cause great harm to the institutions of marriage and family. In this respect, it seems that for the future of family and marriage as institutions the view that these spheres represent sites of (largely masculine) violence, sexual abuse and murder is particularly dangerous (Jewkes, 2004:121). In this way, science is used to reinforce prejudices and stereotypes instead of combating them. Objectivity and moderation are the keys to the proper understanding of each problem, and in this, the media continue to play an important role.

On the other hand, rape is one more criminal offense which attracts great public and media attention. Boundaries of criminal protection in the Republic of Serbia in this area have spread over the past thirteen years, including forms that had not been sanctioned before, inter alia, rape in marriage and rape of male victim which are present in current Criminal Code.[3] All of these changes are also the result of a long-standing public campaign with the aim of raising public awareness of this phenomenon.

However, like domestic violence, the media image of rape is a construction that has been created on many myths and misconceptions. To many people, and the media, rape is largely about sexual gratification (Howitt, 1998:91). Although it is implied that this gratification also involves the manifestation of aggression, the emphasis is still put on the sexual plane.

Numerous studies have shown a significant discrepancy between the media construction of the typical rapist and the reality that can be determined by insight into the official statistical data. Media claim that danger exists not from ordinary men but immensely troubled and pathological individuals (Howitt, 1998:121). The myth of a rapist as an abnormal person can also be found in the statements of government officials, which is probably the key contribution in the creation of moral panic (Burchfield et. al., 2014:109).

The image of women victims of rape is often distorted and is the result of a replaced discourse that often emphasises the contribution of women to the commission of rape, but ignores the fact that violence is being used against her and that the perpetrator should be responsible regardless of the circumstances of the particular case. The stigmatisation of

[3] Criminal Code of the Republic of Serbia („Official Gazette of the Republic of Serbia", No. 85/05, 88/05 - corr., 107/05 - corr., 72/09, 111/09, 121/12, 104/13 and 108/14).

women through the dominant media coverage of victims of sexual offenses in general, and especially victims of rape, would disappear only if those victims were taken seriously without hiding behind the stories of their innocence and virginity (Boyle, 2005:29).

The children as victims of violent crimes are always in the focus of media. Apart from domestic violence, children are at the heart of the media interest and when it comes to paedophilia. Philip Jenkins argues that any criminal offence that involves children as victims or perpetrators, and especially when it deviates from the existing moral consensus, has the greatest media attention (Jewkes, 2004: 56, 57).

The dominant media discourse on paedophilia is that unknown persons represent the greatest threat to children. This discourse supports the stereotypical presentation of a typical pedophile ignoring the reality that is different. Typical pedophiles in the media construction are rather grubby, inadequate loners, a misfits who are not 'one of us' (Jewkes, 2004:96). It is true that child abusers are mostly men aged between 20 and 30, in 60-80% of cases involving persons who are acquaintances or even relatives of the victim. The estimates of the dark number of violence against children range from 1:6 to 1:20 (Ignjatović & Simeunović-Patić, 2011:67), and most of them are the cases where the perpetrator is known to the victim. In this sense, one of the myths regarding paedophilia is about the home as a safe area, due to which the public ignores the problem of sexual abuse of children in the private sphere.

The consequences of misconceptions about paedophilia can be very serious. The price that the whole society pays is high: the actual perpetrators can be overlooked and even avoid justice; wrongful arrests can be made; the police can lose valuable time; the public can behave vengeful; trials may be questioned for misrepresentation; and very serious damage can occur in affected families and related communities (Wykes & Welsh, 2009:21). Nevertheless, the highest price that can be paid is the non-recognition of the most common cases of sexual abuse of children or their late recognition when nothing more can be done.

Finally, it should be mentioned that violent behaviour of young people is always interesting to the media. It is interesting that the excessive public reaction is caused mainly because of the behaviour of young people who do not deserve such attention. These are usually those acts that can be attributed to juvenile delinquency in a wider sense, such as the difficulties in education and petty offences of young people, which appears as a typical "youth rebellion against the adult world" (Ignjatović, 2015:15).

Continuous and constant presentation of the youth in a negative sense has significantly contributed to the creation of an atmosphere of fear regarding the aggressiveness of young people and it usually reaches culmination when a minor commits some serious crime (murder, robbery, etc.). However, these most serious crimes of juveniles are not the most common forms of the manifestation of juvenile delinquency that appear on the daily basis in courts (Wykes & Welsh, 2009:134). However, dramatic and excessive reporting of juvenile offenses often leads to more severe punishment (Shepherd, 1999:688). From the one definitely difficult situation, but very rare, the media create an entire show that should present young people only in a negative context.

4. CONCLUSION

The positive and negative roles of the media in the context of violence are constantly intertwined. Without the media, it is almost impossible to accomplish any important social task, and in that sense, concrete steps must be taken to prevent violence. The analysis of the media image of violence in general and its specific forms of manifestation provides important information about the public's attitude. On the other hand, scientific dealing with the dimensions and characteristics of various forms of violence indicates the misconceptions and myths that are part of that media picture. To this end, it is necessary to understand the undertaking of activities whose aim is the prevention of violence. Without breaking the misconceptions and demystification of the phenomenon of violence, there is no effective prevention. That is why it is important that media reporting is complete and truthful.

Media construction of the reality of a crime and moral panic as its consequence will not disappear, but they must be controlled if we want the media to be allies in the prevention of violence. All important social actors must be engaged for this purpose, representatives of formal social control, subjects that are part of civil society and the academic community, which must be more actively involved in the realisation of this idea.

5. REFERENCES

Boyle, K. (2005). Media and Violence: Gendering the Debates. London: Sage Publications.

Burchfield, K., Sample, L. L. & Lytle, R. (2014). Public Interest in Sex Offenders: A Perpetual Panic? Criminology, Criminal Justice Law, & Society, 15(3), 96-117.

Criminal Code of the Republic of Serbia ("Official Gazette of the Republic of Serbia", No. 26/77, 28/77 - corr., 43/77 - corr., 20/79, 24/84, 39/86, 51/87, 6/89 , 42/89 and 21/90 and "Official Gazette of the RS", No. 16/90, 26/91 - decision of the CCJ No. 197/87, 75/91 - decision of the CC RS No. 58/91, 9/92, 49/92, 51/992, 23/93, 67/93, 47/94, 17/95, 44/98, 10/02, 11/02 - corr., 80/02 other law, 39/03 and 67/03).

Criminal Code of the Republic of Serbia („Official Gazette of the Republic of Serbia", No. 85/05, 88/05 - corr., 107/05 - corr., 72/09, 111/09, 121/12, 104/13 and 108/14).

Howitt, D. (1998). Crime, the Media and the Law. Chichester: John Wiley & Sons.

Ignjatović, Đ. (2009). Metodologija istraživanja kriminaliteta. Beograd: Pravni fakultet u Beogradu.

Ignjatović, Đ. (2015). Kriminologija. Beograd: Pravni fakultet u Beogradu.

Ignjatović, Đ. & Simeunović-Patić, Đ. (2011). Viktimologija. Beograd: Pravni fakultet u Beogradu.

Jewkes, Y. (2004). Media and Crime. London: Sage Publications.

Kosloski, A. (2010). Violent Offenders. In: Transnational Criminology Manual, 2, (pp. 31-47). Nijmegen: Wolf Legal Publishers.

Law on Amendments and Additions to the Criminal Code of the Republic of Serbia ("Official Gazette of the Republic of Serbia", No. 10/02).

Moriearty, L. P. (2010). Framing Justice: Media, Bias, and Legal Decisionmaking. Maryland Law Review, 69, 849-909.

Muraskin, R. & Domash, S. F. (2007). Crime and the Media: headlines versus reality. New Jersey: Pearson Prentice Hall.

Ott, B. L. & Mack, R. L. (2010). Critical media studies: an introduction. London: Wiley-Blackwell.

Prajs, S. (2011). Izučavanje medija (Media Studies, translator: Kolović, V.). Beograd: CLIO.

Roberts, V. J. (1992). Public Opinion, Crime and Criminal Justice. Crime and Justice, 99-180.

Shepherd, R. E. Jr. (1999). Film at Eleven: The News Media and Juvenile Crime, Quarterly Law Review, 18, 687-700.

Stojanović, Z. & Delić, N. (2013). Krivično pravo-posebni deo. Beograd: Pravni fakultet Univerziteta u Beogradu.

Surette, R. (1994). Predator Criminals as Media Icons. In: Media, Process, and the Social Construction of Crime: Studies in Newsmaking Criminology, (pp. 131-158). New York: Garland Publishing.

Surette, R. (2003). The Media, the Public, the Criminal Justice Policy, Journal of the Institute of Justice & International Studies, 39-52.

Surette, R. (2007). Media, Crime and Criminal Justice: Images, Realities and Pollicies. Belmont: Thomson Wadsworth.

Svensen, L. Fr. H. (2008). Filozofija straha (Frykt, translator Rajić, Lj.). Beograd: Geopoetika.

Wykes, M. & Welsh, K. (2009). Violence, Gender & Justice. London: Sage Publications.

UDK 351.851:004
https://doi.org/10.18485/fb_ic4hs.2018.21

USAGE OF MODERN WIRELESS TECHNOLOGIES FOR CHILDREN'S PRESENCE AND LOCATION ANALYTICS AT EDUCATIONAL INSTITUTIONS - TECHNICAL, SECURITY AND LAW DILEMMAS

Milenko MARKOV[*], Nenad PUTNIK[**], Mladen MILOŠEVIĆ[***]

Abstract: One of the basic tasks in the management of educational institutions is to create and realize a security policy aimed at the protection and safety of students, staff and material resources. Formulating a security policy is a form of proactive action that minimizes risk materialization and prevents harmful consequences.

Information and communication technology (ICT) is used in the educational system for performing technical and administrative tasks and teaching activities. However, its range of use is broadening with a view to increasing students' safety. In recent years, for example, US educational institutions have been using software tools to monitor students on social networks in order to prevent electronic peer violence. It is necessary to monitor students effectively, not only in the virtual but also in the physical world, where the management of an educational institution is responsible for the safety of its students within the school perimeter.

In this paper, we will discuss the possibility of using various modern wireless technologies for presence and location calculation in order to increase the security of children (or people and goods in general) in open spaces and around public venues such as schools. The paper will discuss technical, ethical and legal challenges related to the implementation of such solutions.

We will consider GSM/GPS-based tracking, tracking of Wi-Fi and user devices such as mobile phones and tracking of BLE (Bluetooth Low Energy) or IEEE 802.15.4 enabled devices and passive and active tags in detail. In addition to a thorough technical overview and the working principle of these technologies, the paper will discuss the potential pitfalls

[*] BScEE, Technical Consultant at Hewlett Packard Enterprise, milenko.markov@hpe.com

[**] Associate Professor, PhD,University of Belgrade Faculty of Security Studies,Serbia, nputnik@fb.bg.ac.rs

[***] Associate Professor, PhD, University of Belgrade Faculty of Security Studies,milosevic@fb.bg.ac.rs

and drawbacks of the analyzed solutions such as battery life, range limitation, and precision.

In the era of Big Data, IoT and analytics, we would like to compare these technologies from the perspective of reliability of collected data, reporting and alarming systems, legal compliance (e.g. the latest GDPR legislation), security of collected data (risks related to data misuse) as well as other legal, ethical and security dilemmas about how justified it is to apply new technologies, which arise as a consequence of the need to protect personal privacy on the one and increase the safety of individuals, especially children, on the other hand.

Keywords: child security, risk prevention, presence/location analytics, ICT, GDPR legislation

1. INTRODUCTION

Contemporary information and communication technologies play a special role in the life of students, fulfilling their cognitive, value-related, cultural, and general socio-psychological needs.

But for parents, schools, and security experts, new technologies are viewed as a source of new potential problems because they require a broader scope of prevention measures and the addressing of security challenges, risks and threats in order to protect the students' psychophysical integrity, both in the physical and virtual space. (Milošević, Banović & Putnik, 2014; Kovačević & Nikolić, 2015). Consequently, Schwartz and associates recognize twelve types of technologies for school security, the most important of which are: access control, video surveillance, metal detectors, alarm systems, alerting and warning systems, and social networks monitoring (Schwartz et al., 2016: xii).

However, each technology is neutral in value; it can be useful, but also misused. In this paper, we examine the possibilities of implementing modern wireless technologies with the aim of controlling students' presence and determining their spatial location in educational institutions.

2. GPS-BASED TRACKING

GPS-based location services rely on the ability of the end-user device to receive a radio signal from multiple positioning satellites at the same time and calculate its coordinates based on the received signal. Since it is the most popular, we are going to discuss the Navstar GPS system. The Navstar GPS system (or simply GPS) is used by almost all currently available mobile devices such as mobile phones, tablets, car tracking systems, etc. (Norton, 1982).

The Navstar system consists of 24 main satellites, orbiting the Earth every 12 hours and sending a synchronized signal from each individual satellite. As the satellites are moving in different directions, users on the ground receive the signals at slightly different times. When at least four satellites get in touch with the receiver (or when at least four of them are visible to it), the receiver can calculate where the user is – often achieving one-meter accuracy for civilian use.

The calculated data represent geographical latitude, longitude, and altitude. Additionally, the end-user device can be an accurately synchronized precise time source. The Navstar GPS system is unidirectional in its essence, meaning that the end device (the receiver) is by definition able to calculate its location, but the system is not aware of the location of its receiver. In terms of its implementation, this arguably means that user location information should be communicated and processed by some other means, such as GSM, GPRS or a Wi-Fi network.

The fact that it is the most popular positioning system has influenced its price, features, and availability. The cost of receiving a module with an integrated antenna is relatively low (~ 5USD), its precision is high (~1m), it has a high percentage of coverage without additional infrastructure, and low power consumption, so battery-operated devices are commercially available. Major drawbacks of GPS-based systems are that they do not support indoor operation (there must be 'radio visibility' between the satellite and the receiving device), they are affected by weather conditions (cloudy weather), there is a delay in initial location calculation ('time to first fix'), and the system needs an additional channel of communication in order to determine client location (to share the client's location), like Wi-Fi or 3G/4G/LTE, etc.

3. WI-FI-BASED TRACKING

When discussing Wi-Fi-based tracking in this paper, we will focus on Wi-Fi as defined in the IEEE 802.11 standard, which provides wireless connectivity to mobile devices. In a typical environment, we would have a set of Wi-Fi access points (each of them covering approximately 100 square meters) that transmit the signal to and receive it from mobile devices. Wi-Fi access points have a wired connection to the rest of the network. Wi-Fi systems can be implemented to have both indoor and outdoor coverage.

Wi-Fi systems can be (and usually are) implemented in such a way that all access points act as a part of the same Wi-Fi infrastructure, so that end-users have seamless *roaming* between access points when moving around the object (hotel, shopping mall, school, warehouse, etc.). In order to achieve this, a Wi-Fi system must constantly measure the client's radio signal level, in order to determine the optimal access point that will provide the connection service to the specific client.

In order to uniquely represent themselves to the system, Wi-Fi devices (clients) use a 48-bit long unique identifier called a MAC address. The same MAC address is usually used even if the client is not connected to the system (in some cases there is a process called randomization, that randomizes the MAC address of a non-connected client). When this information (the MAC address) is combined with the signal level of each station, two pieces of information can be extracted: a) client presence – if (and when) the client is seen in the range (area around) of an access point and b) approximate location of the client within the infrastructure.

The signal level of a specific client is usually streamed from the wireless infrastructure using a RTLS (real time location service) protocol to the location engine that is aware of the physical infrastructure, so that exact presence and location information can be

extracted. Presence information is extracted from the fact that AP is reporting that it "sees" the specific client with the given signal level. Combining the presence information from at least three sources (access points) using triangulation, location information can be extracted. It can be provided in absolute coordinates (latitude, longitude, floor (level)). Usually, the timestamp (exact time) of the provided data is also provided (*Aruba Analytics and Location Engine API Guide*, 2018).

The Wi-Fi tracking system provides relatively inaccurate position data (approximately 5 meters, depending on the implementation) but exact presence data. These systems can be implemented by using the existing infrastructure (if the infrastructure supports a RTLS service) and they do not require separate end-user devices (existing mobile phone/terminals could be used). There are also dedicated battery-operated "Wi-Fi" tags. Wi-Fi tracking systems can be used both indoors and outdoors. Since the position is calculated by the system and not by the end-user device, their location is easily shared by other components of the infrastructure.

4. BLE BEACONS AND MICRO-LOCATION SERVICES

As previously discussed, GPS systems rely on the radio visibility between the receiver and the satellite, and therefore have limited operation indoors. In order to overcome this limitation, the industry is working hard on a solution for this problem.

One of the approaches is to use BLE beacons to provide location services to clients. BLE (Bluetooth Low Energy) or Bluetooth 4.x technology is slightly different from previous Bluetooth versions, at least as far as the following is concerned: a) it does not require 'pairing' so some information can be exchanged between devices without previous negotiation ('connectionless communication') b) BLE is of such low power consumption that the battery-powered beacon emitter can last for years without battery replacement.

A BLE beacon is a device that constantly emits the same radio message at a constant rate, usually once per second. This message consists of the unique beacon identifier and, optionally, the battery level of the beacon. On the client's side (usually a mobile device), there is a receiving process, which accepts beacon messages, measures the radio level of the received signal, and sends this information (via Wi-Fi or 3G/4G/LTE) to a location server that calculates and returns the client's position. In that way, both the location server and the client are aware of the client's location.

BLE beacon systems can be used for both presence (e.g. student presence in the class) and location services (e.g. indoor navigation). Having been developed with GPS's limitations in mind, it provides location information in such a way that seamless switchover from GPS to an indoor service is possible (e.g. it uses GPS while the client is outdoors and switches over to the beacon positioning system when the client does not have GPS coverage).

BLE beacon systems, if implemented appropriately, have high location accuracy (1m). They require clients (e.g. smart phones) with a specific service/application that supports the BLE positioning service. They work in both indoor and outdoor environments and are conservative in energy use. The BLE beacon positioning system requires specific

infrastructure (beacons and a location processor) in order to provide location services. By its nature, the location information is available to both the clients and the system (*Google Beacon Project*, https://developers.google.com/beacons/; *Aruba Location Services*, https://www.arubanetworks.com/products/location-services/).

5. PASSIVE AND ACTIVE TAGS AND ID CARDS (RFIDS).

In this paper, we will classify them in the same group although they are significantly different from the perspective of the technology used. The concept behind them is that, by using active 'gates' (doors or passages), the system controls access to specific regions, so that the information about someone's presence can also be extracted. For example, by using a passive RF tag (a tag that does not have a power source or a battery but would rather use radio-inducted power in order to communicate with the gate), the system could control access to a specific region of an object. As every RF tag could have a unique identifier, by pulling information from the gate, the system could determine information such as presence, time and a people count for every specific region of an object.

These systems cannot provide location but provide presence information. This information is available to the system only (in the case of passive tags) and to both the system and the client (in the case of active tags). Their power consumption is relatively low, but the system requires dedicated gates and door control. This creates additional challenges as the system must address other safety requirements (e.g. the behavior of doors in case of fire or another emergency).

6. CONCLUSION

Cases of peer violence outside schools and the continuous increase in crime rates among young people clearly point to the need for students to be monitored with a view to preventing unfortunate events and their consequences. Every type of surveillance and control suggests a number of other questions and dilemmas – technical (what logical and technical means and tools to use to control access and successfully ensure prevention) and ethical (the necessity of monitoring, application limitations, privacy rights), but also legal, psychological, etc. (Putnik & Milošević, 2016).

As with many other technologies, there is no ideal solution for all implementations. For example, the GPS system provides high accuracy and a low cost of implementation, but does not provide indoor operation. On the other hand, Wi-Fi tracking could provide almost no cost of operation for indoor coverage (as the system already provides a connectivity service), but has low accuracy. BLE beacons-based systems offer high precision but bring additional costs of operation. There is high probability that RFID systems are already being implemented, but they are usually isolated from other systems and are not used for presence/location services.

Preventive action is neither simple nor is it possible is only logical and technical means are employed. The implementation of modern wireless technologies with the aim of access control can certainly bring results. However, we believe that a wider approach must be taken to combat peer violence and prevent accidents outside the school perimeter, which

would include not only logical and technical tools, but also the harmonization of national legislation with international standards in this field, consultations with ethics experts, as well as the education of students, parents, teachers and non-teaching school staff.

However, the usage of modern wireless technologies for children's presence and location analytics introduces numerous legal issues, especially those concerning privacy rights. The need for improving national, local or corporate security (or, in this case – the security of educational institutions) often violates the inalienable human right to privacy. The balance between human rights and security is hard to achieve and maintain, but a lack of this balance brings serious concerns. In the light of the General Data Protection Regulation (GDPR), which has finally been approved by the EU Parliament on 14 April 2016 (after four years of preparation and debate) and came into force on 25 May 2018, those concerns look even greater (Directive 95/46/EC). The GDPR replaced the Data Protection Directive 95/46/EC and it can be seen as a step forward in the protection of the rights to privacy (Blackmer, 2016). The regulation has established rules which are designed to harmonize data privacy laws across Europe, protect and empower all EU citizens' data privacy and change the way all institutions and organisations deal with privacy issues. The GDPR norms are a challenge for every organisation, including schools, because it is not an easy task to comply with the regulation and meet its demands. The GDPR rules will present serious hurdles in the usage of contemporary technologies while the need for balance in the relation between security and law is increasing and becoming more of a challenge.

The creation and development of ethical standards and principles concerning the use of information and communication technology for security purposes is of great importance. Questions of privacy, democracy, property rights, and others can be included in such issues. The establishment and development of these norms and principles is of paramount importance because they could find application in all those cases of security violations that do not violate the law, but are perceived as socially unacceptable behavior. In the historical sense, unfortunately, the field of computer ethics has been reactive in relation to technology – computer ethics have followed technological development and only subsequently reacted to it (Johnson, 2006).

The challenge faced by the educational institutions that apply or intend to implement measures of control over their students include an approach to solving the problems of crime, violence and other abuses, and the issue of preventing the application of technical measures and resources and strategies from eroding the confidence of students in the institution.

The primary and also the best protection against peer violence and other forms of bullying or crime is – knowledge. In the Enlightenment, the motto was *sapere aude* (dare to know). This term implied that if the detection of something is not unequivocally dangerous, then at least it presents a challenge and requires great work. This maxim is still valid today and is applicable to the process of acquiring knowledge in the sphere of information and communication technologies. The constant growth of innovations in the field of technology and virtual communications requires continuous education on both their purposefulness and safe use.

7. REFERENCES

Aruba Analytics and Location Engine API Guide. (2018). https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/30756/Default.aspx, retrieved 03/09/2018

Aruba Location Services, https://www.arubanetworks.com/products/location-services/, retrieved 03/09/2018

Blackmer, W.S. (2016). GDPR: *Getting Ready for the New EU General Data Protection Regulation*, Information Law Group, InfoLawGroup LLP.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, 1995.

Džonson, D. (2006). *Kompjuterska etika*. Beograd: Službeni glasnik.

Google Beacon Project, https://developers.google.com/beacons, retrieved 03/09/2018

Kovačević, A. & Nikolić, D. (2015). Automatic Detection of Cyberbullying to Make Internet a Safer Environment. In: Cruz-Cunha, M.M. & Portela, I.M. (Eds.) (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*. Hershey: International Science Reference, pp. 277-290.

Milošević, M., Banović, B., Putnik, N. (2014). Nasilje i drugi oblici ugrožavanja bezbednosti u obrazovno-vaspitnim ustanovama i mogućnosti krivičnopravne i prekršajne zaštite. U: Popović Ćitić, B., Đurić, S. (urednici), *Modeli unapređenja bezbednosti u obrazovnovaspitnim ustanovama*. (str. 37-55). Beograd: Fakultet bezbednosti

Norton, J.H. (1982). Navstar Global Positioning System, *International Hydrographie Review*, Monaco, LIX (1), pp. 23-30

Putnik, N., Milošević, M. (2016). Smernice za izradu politike bezbednosti informaciono-komunikacionih resursa i njihovih korisnika u obrazovno-vaspitnom sistemu. U: Popović Ćitić, B., Lipovac, M. (urednici), *Bezbednost u obrazovno-vaspitnim ustanovama: osnovna načela, principi, protokoli, procedure i sredstva* (str. 97-116). Beograd: Fakultet bezbednosti

Schwartz, H.L. et al. (2016). *The Role of Technology in Improving K-12 School Safety*. Santa Monica: RAND Corporation

UDK 323.28:004.738.5
https://doi.org/10.18485/fb_ic4hs.2018.22

THE PROPAGANDA OF THE RIGHT-WING EXTREMISM ON THE INTERNET

Marija ĐORIĆ[*]

Abstract: This paper will analyse the ways contemporary right-wing extremism uses the Internet for propaganda. The author will be using comparative analyses for making comparisons among different types of web addresses, with the aim to provide more objective, more valid and scientific insights into the so-called 'black propaganda' within the cyber space. The second type of methods used in this paper will be content analysis which implies analysis of program aims of prominent extremist organizations. Important part of the research will be focused on the web addresses which have substations in many countries and international domain, such as Blood and Honour, Combat 18, Stormfront, etc. The conclusion of this paper underlines that contemporary right-wing extremism is based on the elitist principle promotion and that it uses ideologies such as neo-Nazism, racism, fascism or extreme nationalism, additionally reinforced by violence.

Keywords: right-wing extremism, the Internet, violence, propaganda, social networks.

1. INTRODUCTION

Contemporary right-wing extremism uses numerous means and methods for propagating their violent ideas. One of the most attractive instruments used for the recruitment of new members and for promoting their ideology is – the Internet. That is why the research question of this paper is: How do the right-wing extremists use the Internet for their propaganda?

Modern means of communicating primarily based on virtual relating have given birth to 'dark net', misuse of social networks, blogs, video games, etc., which are being abused in order to achieve extreme right-wing political ideas. Within the right-wing extremist spectrum, security awareness – the realisation of the need to protect oneself, especially on the Internet – has increased (Bundesamtfür Verfassungsschutz, 2017, p. 5). Extremists use the Internet in most cases in order to conduct the following activities:

1. Creation of websites – to promote the work of certain groups, movements and organizations.

[*] Research Associate, Institute for Political Studies, Belgrade, mara.djoric@yahoo.com

2. Use of social networks (Facebook, Twitter, Instagram…) – to connect members of these groups with potential new members.
3. Promotion of certain events, such as the so-called summer schools, martial arts camps, or concerts. The influence of WPM (White Power Music) is especially dangerous, when speaking of forming a young individual's value system, who might, thanks to song lyrics, adopt negative messages of hatred.
4. Placement of video contents (most often via YouTube) that are often of a violent character and that depict the organization's activism.
5. Creation of new video games that encourage religious, national or racial hatred and bigotry.[1]

2. CONTEMPORARY RIGHT-WING EXTREMISM – DETERMINATION

It is believed that extremism (and thus also right-wing extremism) is one of the most variable social phenomena that cannot be easily defined. There are several reasons for that: duality of political standards and morals, hiding extremists under the 'quasi-democratic' ideas, different perceptions of extremism in various socio-political environments, etc.

Right-wing extremism is "a behaviour and point of view that is borderline permissible, with a tendency to cross the border. As a political phenomenon, right-wing extremism is typical for movements, groups and organizations (and rarely for individuals) that use Nazi-fascist tools and methods in achieving 'grand' plans. Depending on the type of collectivity they belong to, right-wing extremists fight for supremacy of a certain group, nation, race or religion, diminishing everything that differs from their value system" (Djoric, 2014, p. 134-145).

Unlike the former Nazism and Fascism, contemporary right-wing extremists often conceal their behaviour by quasi-democratic actions, and thus, at first glance, they are not that easily distinguishable. Besides, modern right-wing extremism involves different ideas, starting from neo-Nazism, neofascism, violent clericalism and nationalism, anti-globalism, vigilantism, etc. Their resistance towards globalization is especially important, given the fact that they oppose denationalization and desovereignisation, on which 'the new world order' insists.

Right-wing extremists also differ depending on the part of the world they live in. While, for example, in America, right-wing extremists build their ideology on racism (i.e. Ku Klux Klan), in Europe, the right-wing extremism is the consequence of migration movements and xenophobia, caused by newcomers from Africa and the Middle East (of which, the majority are Muslims). On the other hand, right-wing extremism in the Balkans has emerged as a consequence of civil wars in the nineties of the 20th century, after the escalation of violent nationalism.

[1] For example, Humgarian fascists created a game called We will destroy Trianon which revives the memory of "The Great Hungary", a country that lost two thirds of its territory by signing the Treaty of Trianon. According to: Đorić, M. (2014). Ekstremna desnica, Nauka i društvo, Beograd.

3. RIGHT-WING EXTREMISM AND THE INTERNET

The topics of right-wing extremists on the Internet are usually linked to racial, ethnic and religious issues, antiglobalism, xenophobia, various types of ethical issues (such as abortion), etc. Extremists also use violence, manipulation, irrationality (they target emotions), but also humour as well, for the purpose of propagating their ideology.

Stormfront is one of the most influential Internet forums used by right-wing extremists for the purpose of interconnection and promotion of political goals. It emerged in America in the eighties of the 20th century under the patronage of Ku Klux Klan , and nowadays it operates world-wide. Apart from racism (based on the white race's supremacy), Stormfront also strongly supports the idea of Nazism, glorifying the work and life of Adolf Hitler. On the home page of this forum, the essence of their ideology is presented: "We are a community of racial realists and idealists. We are White Nationalists who support true diversity and a homeland for all peoples. Thousands of organizations promote the interests, values and heritage of non-White minorities. We promote ours" (Stormfront.org, n.d.).

According to the Stormfront official website, (Stormfront.org, n.d.), it is interesting that the majority of posts on this blog come from their British chapter (1 047 388), in comparison to Croatian (73 788). It is also worth mentioning that Stormfront chapters might be also found in countries such as Russia and Serbia, even though these countries' population suffered to a great extent by the hands of Nazis during World War Two. In Jasenovac concentration camp alone, over 700.000 people were killed, and, along with Roma and Jewish population, the Serbs suffered terrible casualties (Neubacher, 1957). Apart from classical Internet actions, Stormfront also has its own radio station which propagates WPM.

Stormfront financing is multidimensional, and includes the following donations (Don Black, 2012):

- "Each $5 extends your Sustaining Membership by one month.
- Each $50 one year.
- Each $1000 one lifetime.
- Stormfront CORE Support Membership $30/month".

On the international level, apart from Stormfront, there is another popular social group that supports extreme right-wing members. Blood & Honour is a neo-Nazi (predominantly anti-Semitic) political network founded in 1987 in Great Britain, and it still has a huge number of supporters world-wide. This neo-Nazi network is famous for generating WPM, which started with its famous concerts even in the seventies in Britain, under the name Rock Against Communism. Ian Stuart Donaldson , 'the icon' of the Blood & Honour, was the frontman of the rock band named Skrewdriver, and the network was later named after their song . In 1988, this network also founded a journal named Blood & Honour.

We can also notice a very powerful connection with the Ku Klux Klan chapters in America (Texas KKK, Imperial Klans of America…), but also with European extremists (Veneto Fronte Skinheads, Nationalist Romania, Rasna Zavest…). The entire Blood & Honour movement represents the apologia for the work of Ian Stuart, which is best seen on the home page of their website: "This is our dedication to Ian Stuart, Blood & Honour & National

Socialism. When all others become unfaithful, we remain true! HAIL IAN STUART, HAIL BLOOD & HONOUR, HAIL THE NEW DAWN". (B & H Worldwide, n.d.).

At the end of this research, we will analyse another organization that propagates right-wing extremism via the Internet. It is the Combat 18 - an organization founded in Great Britain, but later expanded to the United States. Combat 18 was formed under the umbrella of the British National Party in 1992. This organization has expressed special animosity towards migrants, left-wing oriented individuals, as well as ethnic minorities. Also, the link between the Combat 18 and hooligan groups is also very interesting. The main idea of these Neo-Nazis is the conception of the 'white revolution' that would be conducted with the help of recruitment of teachers and professors that would later form the value system of their students (Lockley, 2016).

Combat 18 publishes its propaganda on a mutual site with Blood and Honour (www.skrewdriver.net). Together, they co-act with the help of publishing houses such as ISD Records, Blood and Honour radio stations. Combat 18 is a leaderless resistance organization. This means that it bases its activities on individual actions without any overemphasized hierarchy, which is not the case with the rest of neo-Nazi organizations. Generally speaking, Combat 18 is very active on YouTube, given the fact that, when searched on this website, it provides us with 11 400 000 results.

3. CONCLUSION

It is evident that, in the contemporary society, right-wing extremism uses every possible tool for spreading its violent ideology, within which the Internet represents their most significant tool for spreading propaganda. This might be explained by the fact that the Internet provides fast interconnection for free, it enables concealing identity and also eases communication between extremists that are preparing for 'the new revolution'. The only 'problem' is that the competent national authorities also use the Internet to track down, follow and record extremists, which to a great extent eases their control and sanctioning.

Nowadays, the Internet and social media have enormous potential. One of them is the potential to spread information rapidly around the world. It can be a trap for modern man. Because of this, it means that "you should never instantly believe everything you read, and that the same rules of scepticism and analysis need to be applied to digital propaganda as to any other".

4. REFERENCES

B & H World Wide. (n.d.). Home. Retrieved from: https://www.bloodandhonourworldwide.co.uk/bhww (2018, July 22).

Black, D. (2012). Keep Stormfront and SF Media Alive and Growing! Retrieved from: https://www.stormfront.org/forum/t1211646/?postcount=1#post14080008 (2018, July 21).

Bundesamt für Verfassungsschutz. (2013). Right-wing Extremists and their Internet Presence, Bundesamt für Verfassungsschutz, Köln.

Đorić, M. (2014). Ekstremna desnica, Nauka i društvo, Beograd.

Đorić, M. (2016). Ekstremna levica, Nauka i društvo, Beograd.
Lockley, M. (2016). Far right group Combat 18's secret plan to 'recruit teachers' exposed by former member. Retrieved from: https://www.mirror.co.uk/news/uk-news/far-right-group-combat-18s-8339645 (2018, July 18).
Neubacher, H. (1957). Sonderauftrag Suödost 1940-1945 Bericht eies fliegenden Diplomaten, Musterschmit-Verlag, Goöttingen.
Newton, M. (2010). Ku Klux Klan in Mississippi: a history, N.C. : McFarland & Co, Jefferson.
Stormfront.org. (n.d.). Retrieved from: https://www.stormfront.org/forum/index.php (2018, July 21).
https://www.youtube.com/results?search_query=combat+18 (2018, July 23).

UDK [323.283:28]:[32.019.5:004.738.5]
https://doi.org/10.18485/fb_ic4hs.2018.23

ADOPTING THE ISLAMIC STATE'S INTERNET PROPAGANDA METHOD: THE CASE OF BOKO HARAM

Tanja MILOŠEVIĆ*

Abstract: The Internet has provided terrorists with a perfect platform for spreading propaganda, not only through blog posts and social media, but also through posting various videos justifying their cause. The main topic of this research is the Internet propaganda of Boko Haram, the notorious Nigerian version of the Islamic State, and the way it resembles the propaganda of the Islamic State. Given the fact that the manner of spreading propaganda has changed in the era of the Internet, the actions of numerous currently active terrorist organizations have shifted into cyberspace. An analysis of this modern phenomenon is therefore of the greatest importance for combating contemporary terrorism. The Islamic State has provided the currently active terrorist groups with a perfect model for spreading terror on the Internet, which has been adopted by Boko Haram. Since the Islamic State has produced the most technologically advanced propaganda, it was to be expected that this model would be adopted by other terrorist organizations. This paper will thus present the modern means of spreading terrorist propaganda on the Internet, as well as some descriptive examples. The research was formulated as an analysis of information on the propaganda activity of the two most active terrorist organizations on the Internet, the Islamic State and Boko Haram, and an analysis of the propaganda material found on the Internet.

Keywords: Boko Haram, propaganda, terrorism, Islamic State, Internet.

1. INTRODUCTION – TERRORISM AND INTERNET PROPAGANDA

The Internet provides an unrestricted place where terrorist can easily create and spread propaganda through a limitless number of websites and social media platforms. As stated by Rieger, Frischlich and Bente (2013, p. 1), "extremist organisations chiefly use videos and online services on the Internet to win over supporters and to radicalize individuals".

The idea of propaganda is as old as mankind, but the means of spreading propaganda are constantly changing. According to Lieberman (2017, p. 98), propaganda has been documented throughout history. For example, the Greeks used the theatre, and Egyptian

* MA, Military Academy, University of Defense, Belgrade, Serbia, tanja.z.milosevic@gmail.com

pharaohs used carvings on temple walls. These tactics are still present nowadays, but theatres and walls have been replaced by – cyberspace.

The main purpose of propaganda is still "to persuade the recipient into adopting the ideas the propagator tries to convey" (Rieger Frischlich, Bente; 2013, p. 1). Thus, studying the propaganda methods of currently active terrorist organizations is essential for the prevention of recruitment of new members and the spreading of fear in communities.

2. BOKO HARAM

The previous year has turned out to be one of the most violent years, as numerous terror attacks occurred in many countries. It should, however, be stressed that "the vast majority of deaths from terrorism occurred in one of five countries: Afghanistan, Iraq, Nigeria, Pakistan and Syria. And of these deaths, four groups were responsible for 74 % of them: Boko Haram, The Taliban, ISIS and Al Qaeda" (Martin, 2017). Since terrorist organizations such as the Taliban and Al Qaeda need no introduction, as they have been present on the global terrorist map for decades, and ISIS being almost defeated[1], the time has come to dedicate much-needed attention to the world's currently most vicious terrorist organization – Boko Haram.

Boko Haram was founded in 2002 by Mohammed Yusuf. At the beginning of the reign of this terrorist organization, its members were considered to be only "moderate revivalists attempting to implement social change" (Kane, 2007, pp. 64–67). However, when Shekau took over in 2009, Boko Haram gained prominence. It is said that Boko Haram has, since that time, killed tens of thousands and displaced about 2.6 million people from their homes (Onuoha, Oyewole; 2018, p. 2). This terrorist organization "was responsible for 6,644 deaths in 2014, an increase of 317% from the previous year, according to the Global Terrorism Index" (Pisa, Hume, 2015).

The significance of researching Boko Haram lies in the fact that "the jihadi insurgent movement Boko Haram has established itself as one of the relatively few jihadi movements to succeed in the capture, control, and governance of territory in Africa. Over the course of less than two decades, Boko Haram has morphed from a jihadi movement operating within Nigeria to a movement with a regional presence across multiple countries in West Africa and beyond" (Kassim, in: Zenn, 2018, p. 3).

Boko Haram[2] has become notoriously famous worldwide since it started its raids on schools. The most famous case is the kidnapping of Chibok girls, when 276 teenage girls

[1] In December 2017, the Prime Minister of Iraq, Haider al-Abadi, declared victory against the Islamic State. However, in July 2018, reports emerged that the battle had shifted into the central zone of Iraq, as well that ISIS fighters were now using more nefarious tactics, thus spreading more fear among the local population. At this point, it is unclear how the situation will develop in the future (See also: Jay, 2018).

[2] The official name of this group is جماعة أهل السنة للدعوة والجهاد (*Jama'atu Ahlis Sunna Lidda'awati wal-Jihad*), meaning: People of the Sunnah (the practise and examples of Prophet Muhammad's life) for Preaching and Jihad Group. However, the Hausa-speaking residents in the north-eastern city of Maiduguri, where the group had its headquarters, dubbed it Boko Haram, meaning "Western education is a sin".

were snatched from a boarding school in Borno State. Given that this organization has focused on female victims, it was to be expected that it would start using women for carrying out terrorist attacks. Moreover, the kidnapped girls were often used in propaganda materials, appearing in numerous videos. By February 28, 2018, records showed that 469 female suicide bombers had killed more than 1,200 people in Nigeria, Niger, Chad and Cameroon, injuring additional 3,000 people. Using female suicide bombers could also be viewed as ensuring publicity, which definitely has a propaganda effect. (Pearson, in: Zenn, 2018, p. 33–36).

3. BOKO HARAM INTERNET PROPAGANDA

Boko Haram is nowadays present on Facebook, Twitter, and especially Telegram as means of reaching the public with their statements (See also: Zenn, 2018, IV). Moreover, this organization has been publishing videos whose topics range from official statements, propaganda videos explaining the life of a common Boko Haram fighter, to threats and future plans announcements.

According to Mahmoud, (Mahmoud, in: Zenn, 2018, p. 88), messaging and propaganda tactics of Boko Haram can be divided into three phases. The first phase of Boko Haram propaganda was not propagating violence, and it was not spread via the Internet. This phase revolved around the leadership of Muhammad Yusuf, who mainly preached in mosques and appeared in local media. The sermons and interviews were all in Hausa and Kanuri languages, which only proves the fact that the main idea of his movement was the fight against Western influences.

Phase two started when Abubakr Shekau assumed leadership of Boko Haram, after Yusuf's death in 2009. From this point on, Boko Haram officially turned to violent actions. Also, the tactics completely changed under his rule: the main propaganda strategy was carried out through video messages, press statements, and fliers (Mahmoud, in: Zenn, 2018, p. 88). By the end of 2013, the dynamics of Boko Haram's propaganda shifted to being largely based on video messages, while press statements and fliers were used only sporadically. Even though Shekau spoke mostly in the Hausa language, his speeches began including several Qur'anic recitations in Arabic, many of them the same as the ones used by Al-Qaeda.

The third phase started in May 2013, when the Nigerian government declared a state of emergency in Nigeria. During this period Shekau also pledged himself to Al-Baghdadi, the *caliph* of the Islamic State. At this point, Boko Haram's propaganda material started mirroring the material provided by the Islamic State. Also, at the beginning of 2015, Boko Haram set up a public Twitter account العروة الوثقى (*Al- 'Urwa Al-Wutqha*)[3] in coordination with the Islamic State. Shekau's videos started appearing with Arabic subtitles, which suggests that they were meant not only for Nigerians, but for all Arabic-speaking Muslims worldwide. Moreover, as stated by Mahmoud, (Mahmoud, in: Zenn,

[3] The name of this media wing might have been chosen because this phrase means "the firmest bond" in Arabic. The work of this media wing of Boko Haram can be followed on this link: http://jihadintel.meforum.org/identifier/514/boko-haram-al-urwa-al-wuthqa

2018, p. 103), after Shekau's pledge, the Islamic State-coordinated Media Office of the West Africa Province (MOWAP) took over Boko Haram's messaging. By the beginning of 2017, Boko Haram started putting Islamic State logos in the background of their videos, thus confirming that they still are strong supporters of this terrorist organization. Mahmood (2017, p. 21) observes that the 13 videos "produced by MOWAP after Boko Haram's admission into the Islamic State were markedly different from Shekau's previous messages. Short and direct, they exhibited high production values and often involved new members of the group unmasked on camera, diminishing Shekau's position as the public face of the group".

As stated by Mahmood (2017, p. 5), Boko Haram has been spreading its propaganda using the following tools: Twitter/Telegram (12%), YouTube (14%), jihadist forums and websites (6%) and Press interviews and videos (68%). Given that the idea of spreading videos on the ether has been adopted from the Islamic State, it is obvious that the impact of this terrorist organization is definitely strong in the case of Boko Haram.

4. CONCLUSION

Terrorism is a phenomenon that cannot yet be precisely defined because it changes over time. Moreover, it is clear that terrorist organizations are nowadays frequently present in cyberspace. Thus, keeping track of propaganda – and fighting against it, is an essential part of combatting contemporary terrorism.

The world has come a long way, almost defeating the Islamic State, but its influence on other terrorist organizations is still visible. It is obvious that the propaganda tactics of the Islamic State have been adopted by Boko Haram. This cooperation between Boko Haram and the Islamic State is primarily reflected in their adoption of video-making techniques and scenarios, as well as in the official support from the Islamic State public representatives. Even though Boko Haram has put its stamp on propaganda by introducing women into the terrorist battlefield, it is undeniable that the creation of high-tech videos, as well as the introduction of Arabic subtitles, suggests a strong cooperation between these two terrorist organizations. Moreover, the fact that Boko Haram's leader has abandoned the practice of spreading his word in the Hausa language opens up the possibility for the recruitment of not only Islamic State members, but also any other Muslim individuals prone to radicalization.

It is therefore obvious that, if the world wishes to put an end to Boko Haram, it is necessary to analyze the propaganda spread by these two organizations. Given that armed forces cannot exist without soldiers, the first step in combatting terrorism is the prevention of recruitment. Since fear is the sustenance of every terrorist organization, preventing propaganda from reaching the public might be the next step in beheading this African *dragon*.

5. REFERENCES

Jay, M. (2018). Trump's got mother of all migraines coming on; ISIS is back in Iraq. Retrieved from: https://www.rt.com/op-ed/434364-isis-iraq-trump-syria/ (2018, July 27)

Kane, Ousmane. (2007). "Islamic Inroads in Sub-Saharan Africa," Harvard International Review 29:2.

Lieberman, Ariel Victoria. (2017). „NOTES – Terrorism, the Internet, and Propaganda: A deadly Combination". *Journal of National Security, Law and Policy*, Vol. 9:95, 2017.

Mahmood, Omar S. (2017). „More that propaganda: A review of Boko Haram's public messages". *Institute for Security Studies*, *West Africa Report 20*, March 20017.

Martin, Jenna. (2017). *A closer look at 5 of the most dangerous terrorist groups on the planet*. Retrieved from: https://www.sbs.com.au/guide/article/2017/06/13/closer-look-5-most-dangerous-terrorist-groups-planet; (2018, July 11).

Onuoha, Freedom C.; „Oyewole, Samuel. (2018). Anatomy of Boko Haram: The Rise and Decline of a Violent Group in Nigeria". *Al Jazeera Centre for Studies*.

Pisa, Katie; Hume, Tim. (2015). Boko Haram overtakes ISIS as world's deadliest terror group, report says. Retrieved from: https://edition.cnn.com/2015/11/17/world/global-terror-report/; (2018, July 26).

Rieger, Diana; Frischlich, Lena; Bente, Gary. (2013). *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos*. Wolters Kluwer, Luchterhand.

The Middle East Forum. (n.d.). Jihad Intel Presented by the Middle East Forum: Vital Intelligence on Islamic Terrorist Organizations. Retrieved from: http://jihadintel.meforum.org/identifier/514/boko-haram-al-urwa-al-wuthqa; (2018, July 27)

Zenn, Jacob. (2018). „Boko Haram Beyond the Headlines: Analyses of Africa's Endduring Insurgency". *Combatting Terrorism Center at West Point, United*

UDK 061.1EU:314.15
https://doi.org/10.18485/fb_ic4hs.2018.24

SOCIOCULTURAL COMPONENT IN PATTERN OF CROSS-EUROPEAN MIGRANT INTEGRATION POLICIES

Fatima RAMAZANOVA*

Abstract: This paper presents an attempt to consider the integration policy of the European Union within the social and anthropological aspects. This research describes integration policy of several states, namely France, Belgium and Estonia, and it is assumed that their experience could be transferred to the European Union as a whole. Focusing on integration policy as a case study, this paper draws attention to the question whether cultural approach may be included in the global concepts of integration. By uncovering the perception of integration policy by migrants, we set out to contribute to human security conception. The changes in immigration policy will entail the transformation of human security and the safety of migrants.

In order to answer this question, the paper includes an investigation structured by the empirical researches and composed with a comparative perspective in the social and political spheres. This research draws on interviewing different ethnic groups to compare results depending on the cultural environment. To examine the impact of the implemented policies, ongoing programs and activities, the results assessing the effects on migrants are used. Scientific methodology is based on comparative methods and complex analysis of the legislation, literature, materials of mass media and non-profit organizations.

Keywords: immigration, integration policy, European Union

1. INDTRODUCTION

State's requirements of integration for newcomers are based on the nationhood conceptions (such as a liberalism, cosmopolitanism, communitarianism, republicanism) and their respective political system. It is a question whether migration and integration policies of the European Union states might be revised towards a common strategy in the context of human security framework. Furthermore, the diversity of approaches towards integration policy have been noticed. An interdisciplinary approach will allow the subject to be dealt with in a comprehensive manner.

* Postgraduate student, Department of Political Science and Public Management, Central Russian Institute of Management, Branch of Ranepa, fati.ramazanova@gmail.com

The signification of “Europeanization” lies on the cultural and historical background of each state in the European Union. Out of the immigration patterns, it can be defined the different perceptions of membership for each state and succession to unite values within the Union. One of the discussed strategies among theoretical conceptions is an idea of rational liberalism for equal opportunities in multicultural society by Will Kymlicka (Kymlicka 1995). Human security encompasses freedom from discrimination in a new country and inequality in the labour market or in the social life.

However, the liberalism conception fails to take into account the reception of the natives. It is necessary to stress the importance of the tolerance’ significance with increased political radicalization concern about migrant presence. Tolerance as a socio-psychological research tends to focus on perceptions by indigenous and migrants populations. This is why according to Dutch research, the rejection of liberal values by Muslims is stronger when it concerns religion. The ideas of freedoms and rights are supported by Muslims in other fields (Verkuytenn 2007).

According to Paul Vogt, tolerance is a consciously refrainment from disapproved expression between people. This is the basis for civil society (Vogt 1997). However, this kind of tolerance, as a foundation for multinational state, could pose a threat for the future of the multicultural state. Formal realization of integration policy or formal observance of host' term with prospective advantage does not lead to coherence in society. Christian Joppke rightly points out that culture-based principles are used to achieve migrant’s integration in the host state (Joppke 2007). For these reasons, conception of human security becoming necessary in order to realize the integration policy. Human security includes the protection at the State level of local communities and tackling social exclusion.

2. SOCIOCULTURAL APPROACH IN INTEGRATION POILICY

As an example of integration policy toward Muslim migrants, the results of research within Estonian Research Grant “Estophilus” could be considered. Series of interviews were conducted with the representatives of Muslim communities from Dagestan, Azerbaijan and Tatarstan and analysed with the help of the secondary data to reveal the structure of Muslim communities. Also, the interviews was conducted with Azerbaijan diaspora from Finland and Latvia. The Estonian integration policy aims to develop the inter-ethnic dialogue and human rights through culture, education, art and sports. In the case of Estonia, migrants or formerly migrants accept the state’s essential constitutional principles, but in the same time, preserve their own culture, above that, promote it into Estonian environment. The Estonian integration program permits to subsidize organization of culture communities with aim to co-exist peacefully respecting the state values. This project, covering Baltic countries is sponsored for 75% by the EU and 25% by the state and is unique in the eastern part of the EU. The question thus is whether the states’ experience in integration policy might be implied and under which condition. On the basis of conducted researches in France and Belgium with a goal to assess the actual response of migrants to integration policy, it is essential to note the following point. A survey from cultural organizations in France and Belgium showed that the members of

cultural organizations are experiencing a deficit of information about self-organization, financial support and accommodation. As a result, migrant's populations become more closed in-group and search support through religion organizations. Moreover, some social workers and professionals in educational sphere suggested during an interview that tutorial of immigrants as in Estonia, concerning questions of self-organization is illiberal. As a consequence, migrants cannot develop they rights recognized by law due to the lack of awareness, that could be considered as a threat to the basic principle of human security. Therefore, we will recur to "paradox of liberalism" (Orgad 2010).

It would seem that every government, and its citizens, are motivated in a relatively full integration of newcomers. Liav Orgad notes a "Paradox of Liberalism" where European states following their liberal principles, finally address illiberal policies (Orgad 2010). Since the "Sarkozy law" of November 26, 2003 concerning the stay of foreigners in France and their nationality, a migrant must justify his "assimilation to French community" in an individual interview ruled by authorities[1]. A candidate must show knowledge of the French language and "good manners". The good manners may be for example a frequent utilization of "Merci" and deeply knowledge of the French history, but it is doubted whether it is really helpful in socialization. France granted citizenship, but as a condition required complete assimilation and loyalty to the secular values of the French Republic. In France, transformation of the French conception has moved from multiculturisme of the 70's to present-day assimilationist policy. Assimilation is as a convenient way of solving problems, but total cultural uniformity is a utopic idea in a multicultural world. Achieving social equality for migrants as a policy objective needs deep understanding about the willingness of national authorities to recognize the cultural value of diversity and to promote the idea of harmonious cohabitation.

3. INTEGRATION AS A STEP TOWARD NATURALIZATION

Another strategic importance of the EU about human security on the issue of integration is the naturalization process. The issues of naturalization emerge in each country in parallel with flows of migrants, particularly nowadays. For Europe, the legitimacy of naturalization process has been arising in the XX century, when the problem of integration of migrants was not the centre of interest for states.

The introduction of integration policy may have an influence on naturalization law and prerequisites for admission. Whereas Europe challenge of migration is a concern, the issue of naturalization policy became essential. There are, of course, migrants who cannot make a choice for their displacement, but after some time newcomers who have started to migrate within the EU, have to select a state with the wanted conditions that fit the most of their expectations. On this subject, our experience is based on the long-term observations of Chechen community in Europe. Despite of de-escalation in Chechnya, the immigration from Russia has not been ceasing since 1999. The population of Chechens in Europe is

[1] Loi n° 2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité

between 110 000 – 250 000, according to different sources (Kurbanova 2012)[2]. The mains factors of the country selection for Chechens are social welfare benefit, religious rights and residence of compatriots. Chechens, as well as others migrant groups, divides their environment between "we" and "they", that gives rise to rejection of the host society's way of life and closeness of community (it is also the example of some Turkish or Moroccan organizations).

During the series of interviews, which were conducted in different countries, the dual character of the formal naturalization process was observed. The formalization of process is only oriented on real and tangible results, such as the fact that a migrant has to maintain his original way of life or can get a job in the host country. But it ignores the principle values and constitutional arrangements of the host state despite of the fulfilment of criteria for admissions. There is also inverse case when a migrant does not receive the nationality after 15 years on site due to insufficient financial resources even if migrants show respect and full integration to the country. Nevertheless, a migrant could be fully integrated and appreciates that a host country is preserving their traditional culture, as observed during the interviews with Muslim groups in France. It reflects the fact that EU's naturalization policy needs to be revised.

Modification of interior legislation towards common regime and conditions in the EU might resolve the further problems with territorial concentration of migrants. Moreover, the question is, whether the states are disposed for changes in global integration policy, as far as each country accrues benefits from migrants. However, under the current situation due to the disproportion of migrants' flows, Member States could be tackled more constructively. Therefore, it is important to return to the principal foundation of common values and the conception of human security.

4. CONCLUSION

If the family can be considered as a cell or a mini-copy of the state, then the multicultural state is an integral part of the EU, which is also diverse and consists of a multitude of states with different visions of domestic policies. From this perspective, the human security can contribute significantly to development of social, economic and political rights. This paper argues that the creation of a common concept of integration policy for the EU does not limit the rights of a separate state, but allows it to expand and to be improved. A single conception of integration policy in the EU should be coordinated in all departments and at all levels of government.

Each national culture is divided between "we" and "they", which increases rejection of the host society's way of life and closeness of community. This paper argues that cultural approach is the most effective form of integration policy. Moreover, the introduction of integration policy may have an influence on naturalization law and prerequisites for admission. A positive transformation towards the human security and the safety of migrants may be achieved by conceptual changing in immigration policy.

---

[2] Also in the interviews of Chechen communities' heads.

5. REFERENCES

1.Joppke, C. (2007). Do Obligatory Civic Integration Courses for Immigrants in Western Europe further Integration? FOCUS MIGRATION №8.

2.Kurbanova, L.U. (2012). The problems of self-indentification of Chechens. Russia, Krasnodar. 390 p.

3.Kymlicka, W. (1995). Multicultural Citizenship: A Liberal Theory of Minority Rights. 290 p.

4.Loi n° 2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005702743&dateTexte=20090903

5.Orgad, L. (2010) Illiberal Liberalism: Cultural Restrictions on Migration and Access to Citizenship in Europe, American Journal of Comparative Law 58(1). P.53-106

6.Verkuytenn, M. (2007). Social Psychology and Multiculturalism. Social and Personality Psychology Compass, №1. 280 p.

7.Vogt, P. (1997). Tolerance & education : learning to live with diversity and difference, 280 p.

UDK 614.8-055.2
https://doi.org/10.18485/fb_ic4hs.2018.25

DISASTER RISK REDUCTION - GENDER ASPECTS [1]

Zorica MRŠEVIĆ[*], Svetlana JANKOVIĆ[**]

Abstract*:* The subject of this paper is the gender aspect of the disaster risk reduction concept. A natural phenomenon in itself is not a disaster, but it becomes when it strikes a vulnerable community, a group or individuals without proper defence who have no ability to resist or to repair its negative effects. It causes material damage and human losses, possible interruption of the economic and social functioning of the community. The threat of disasters is a matter of overall human security and implies bringing into question the safety of life, housing and economy, food, water, energy, health, and environmental safety. The aim of the paper is to point out that disasters are not a 'natural' inevitability, since they are the result of natural risk factors and human vulnerability, in which gender-based inequalities are a constitutive component. Consequently, disaster risk reduction processes that include prevention, mitigation and preparedness for response in all phases should have a necessary gender perspective, with the aim of increasing disaster resilience. Such an approach is based on the knowledge of the risk management, capacity building and the use of information and communications technology, as well as the analysis of existing gender relations and the need to change unsafe discriminatory practices in the field. Namely, the opportunities available to women and men in fact are not the same even in 'normal' circumstances, not to mention the emergencies. There is a gender division of jobs, unequal access to material and non-material resources, lesser participation of women in decision-making at political and private levels, women's exposure to gender-based violence and various forms of discrimination. The conclusion is that building resistance to disasters, empowering women and community development necessarily represent elements of unique, but not separate, efforts.

Keywords*:* disasters, women, gender relations, poverty, disaster risk reduction

---

[1] This text was created as part of the project of the Institute for Social Sciences in Belgrade: "Social Transformations in the Process of European Integration - Multidisciplinary Approach", funded by the Ministry of Education, Science and Technological Development, no. III 47010.

[*] PhD, Senior Research Fellow, Institute of Social Sciences, Belgrade, zmrsevic@idn.org.rs

[**] MA, Lieutenant Colonel, PhD candidate, University of Belgrade Faculty of Security Studies, svetlana.jankovic.cacak@gmail.com

1. INTRODUCTION

Human and property exposure to catastrophes2 (UNISRDE, 2009) is increasing faster than their vulnerability is being reduced throughout the world. This creates new risks and gradually increases losses caused by catastrophes, with significant economic, social, health, cultural and environmental impacts in the short, medium and long term, especially at the local community level. Disasters can occur suddenly (fast start: typhoons, earthquakes, volcanoes) or gradually (slow start: climate change, drought, desertification, gradual melting of polar glaciers). They affect millions of people (Mršević and Janković, 2018). Over the last decade, they have affected nearly 2 billion people and caused damage estimated at $ 1.7 trillion. In addition, from 2008 to 2012, 144 million people were displaced due to disasters. Disasters, most of which are worsened by climate change and continually increasing in frequency and intensity, substantially inhibit progress towards sustainable development.

Constant rise in disaster risks, including the increased exposure of people and property, combined with previous disaster experiences, points to the need to further strengthen disaster response preparedness, to undertake event prediction actions, to integrate disaster risk reduction in response preparation, and to ensure that there are capacities for effective response and recovery at all levels.

2. IMPACT OF DISASTERS ON WOMEN – KINDS AND EXAMPLES

Only at the end of the twentieth and the beginning of the twenty-first century, did the world become aware of considerably higher number of female victims compared to male victims due to catastrophes. First of all, there is a direct and the most visible consequence of disasters in the form of a disproportionately greater loss of women's lives. Moreover, humanitarian organisations point out that the consequences of the same catastrophic events that occur later on, such as illness, hunger, homelessness, property loss, unemployment, gender-based violence, disability, etc. also affect more often affect women than men.

These mentioned examples are not the only ones, but rather chosen as to paradigmatically illustrate the female disaster vulnerability.

The devastating cyclone, which hit Bangladesh on 2 August 1991, caused the death of 135 to 145 thousand people (History.com Editors, 2009). It was then observed that far more women were killed, not only because they were physically weaker, but because of the religious tradition that supported male domination and restricted mobility of women (Begum, 1993: 35). In the population aged 20 to 44, a total of 71 women and 15 men were killed per thousand people. The example of Bangladesh became paradigmatic for finding that women were the first ones affected by disasters, and that they were hit harder (Oxfam-GB, 2011). In Bangladesh, on 15 November 2007, cyclone Sidr caused, according to the initial estimates, about 4,000 casualties, so that humanitarian organisations later published the information

[2] Disasters are natural phenomena that seriously impair the safety and functioning of society, including widespread human, economic or environmental damage, which exceeds the ability of an endangered society to defend itself by its own forces and remedy the consequences with its own resources.

about 10,000 victims and millions of people left without their homes (Mathbor, 2016), highlighting particularly the vulnerability of female population[3] (UNDP, 2010).

In an earthquake that hit Kashmir in mid-November 2005, 73,318 persons were killed or missing, according to official data, but international estimates were that the victims totalled 87 thousand. Women were the most numerous victims and were killed due to the strict custom of 'purdah', according to which women are confined to moving only within their homes, where most of them died of fear of violating the ban on moving freely in public. In places where the demand for purdah was not so strict, women managed to escape from being overcrowded (Parker, Hamilton and Halvorson, 2007).

In Peru, a warning about the arrival of El Ninja in February 2003 was sent only to fishermen, and as women did not engage in fishing, they did not have this information at all. This directly caused enormous damage that could have been avoided if women had known in advance that existing food supplies should have been saved from storms (UNISDR, UNDP and IUCN, 2009: 24, 44).

The world public faced a brutal fact of the prevailing number of women victims (Jungehülsing, 2012) in the case of the Asian tsunami of 2004, when, in Indonesia and Sri Lanka, the proportion of survivors was one woman per four men, or 75% of women victims, while in some Indian regions women accounted for 80% of victims. The International Humanitarian Relief Agency reported that there were four times more female victims than male victims because of social customs that prevented women from moving freely without men (BBC, 2005).

On 2 May 2008, 138,000 people were victims of Cyclone Nargis according to the official reports. There certainly should be added 55,000 missing as well as an unknown number of victims in the 'second wave' that included subsequent victims of hunger, violence and epidemics as a result of cyclonic destruction. According to UNICEF's first estimates, more than half of the victims of Nargis were women and children, while it was pointed out later that women suffered double more than men (Singh, 2012).

3. CAUSES OF WOMEN'S HIGHER VULNERABILITY

UNDP Disaster Risk Reduction Advisor (Cecilia Aipira), says that women and girls are most affected by natural disasters, but that there is no solid data to show in what way. "As a consequence, they remain largely invisible in assistance and development programmes," she said when presenting the newly opened Centre for Gender and Disaster at the University College in March 2018. (UNDP, 2018). Lack of data on the impact of natural disasters and conflicts on women disables all provisions and plans of assistance and recovery from the negative consequences of such disasters.[4] Unfortunately, the recent

[3] In November 2007, Cyclone Sidr tore through the coast of Bangladesh, killing almost 4,000 people, leaving millions homeless and destroying the livestock, crops, farming equipment and fishing boats essential for people's livelihoods. Bangladesh - Rebuilding Cyclone Sidr Victims.

[4] A survey in Chad carried out within the Building Resilience and Adaptation to Climate Extremes and Disasters (Braced) programme has shown that discrimination and violence prevent women from accessing financial and medical assistance in times of crisis. No statistics are gender disaggregated. In disaster-prone areas, such as Nepal, India or Haiti, women do not have any information about disasters, how they should behave, and whom they should address in case disasters happen.

events have shown that it is similar with other 'developed' areas, for example, during recent disasters in Greece, Japan and California.

Given that the extent of disasters is partly under the influence of political, economic and socio-cultural context, the introduction of a gender component into policies and measures to combat disasters begins with the identification of how women and men are positioned in one society (Centre for Disaster Preparedness, 2010). Limited access to women's economic, social and human resources and their reduced decision-making power both at home and in the political sphere reduce their capacity to implement adaptation and protection measures.

They face different levels of risk and are in various ways vulnerable to risky situations and in various ways deal with the consequences of disasters, which is caused by gender-based political, cultural and socio-economic differences and inequalities that persist throughout the world. Compared to men, women are poorer, have fewer opportunities to gain and develop entrepreneurial skills, weaker access to financial resources such as loans, savings or pensions, fewer opportunities to buy or own land, if they are generally paid less – their earned income is more irregular. When floods occur, only wealthy people are able to move to safer places or send their supplies to safe locations. A typical, low paid rural woman living in a poor community has no opportunity to move to safer housing, and disasters as flood / fire / earthquake usually cause loss of everything, including all her supplies, movable and immovable property (Centre for Disaster Preparedness, 2010.b).

Poverty is the key element that determines vulnerability of individuals and countries. Globally, poverty is largely female, 70% of the world's poor are women[5] (Making Disaster Risk Reduction Gender-Sensitive, 2009: 133), which means that women make up the majority of those who live and work in insecure places and in uncertain conditions. Although both sexes are exposed to physical vulnerabilities during natural disasters, we can claim, based on previous global experiences, that various vulnerabilities are caused by gender roles and gender-based inequalities, such as: lack of opportunities, lack of resources and more limited mobility of women than of men of the same social categories. Even in 141 countries it has been discovered that more women than men lose their lives in natural disasters[6] (Making Disaster Risk Reduction Gender-Sensitive, 2009: 35) and that this phenomenon is associated with unequal socio-economic status of women[7] (Neumayer and Plümper, 2007: 552).

Essentially, women have limited access to information and knowledge, which inevitably increases their vulnerability in risky situations. Poverty and marginalisation are associated

---

[5] We are fully aware that women comprise 70% of the world's poor and that women are more vulnerable to the impacts of disasters due to existing socio-economic, political and cultural disadvantages.

6 A recent study of 141 countries found that more women than men die from natural hazards, and that this disparity is linked most strongly to women's unequal socio-economic status.

[7] Looking at the effects of natural disasters in 141 countries over the period 1981 to 2002, the study shows that in societies where the socio-economic status of women is low, natural disasters kill more women than men, both directly and indirectly via related post-disaster events. The reason for the difference in mortality lies largely in the everyday socio-economic status of women.

with a high degree of vulnerability to the impact of climate change, as well as reduced adaptability capabilities due to limited access to economic and non-economic resources, and information and support networks. Gender is the key variable in this context: unequal gender relations increase female vulnerability to the impact of climate change and reduce their adaptability (Jungehülsing, 2012). Consequently, the policies, instruments, mechanisms and tools used to respond to disasters and climate change cannot be neutral in relation to gender, and should not be formulated and applied without considering specific gender differences.

4. DISASTER RISK REDUCTION: HYOGO AND SENDAI FRAMEWORK DOCUMENTS

Increased appreciation of the need to integrate disaster risk reduction into development policies and activities was formalised in January 2005, when the Hyogo Framework for Action 2005-2015 was adopted by 168 countries and multilateral institutions[8]. The Hyogo Framework for Action states that the gender perspective should be integrated into all disaster risk management policies, planning and decision-making, including those related to risk assessment, early warning, information management, and education and training. The necessity of gender sensitive risk assessment was also noticed. A gender aspect always exists and must be identified: when determining the degree of exposure to natural phenomena, natural disasters or climate change; in the manner of analysing women and men in response to disasters, and the recovery from their consequences, and in building capacities to adapt to changes and create responses to them. This would result in gender sensitive planning of emergency management, which unites individuals in the responsibilities and actions to achieve the goal – a safe, gender equitable and economically developed local community.

Disaster Risk Reduction is a conceptual framework that addresses ways and methods for reducing vulnerability and risk of disasters in societies in order to avoid or hinder adverse impacts and dangers caused by natural phenomena and ensure sustainable development. It is a complex and multidisciplinary process involving the acceptance of international and legal obligations, public understanding, scientific knowledge, careful planning of development, responsible implementation of programme policies and laws, early warning systems, and effective mechanisms for emergency preparedness and response. Reducing disaster risk, also, requires collective involvement and engagement of national policy-makers and government decision-makers, civil society, academic institutions, private sector and the media. Research shows the benefits of preventing or reducing the impact of a disaster – for every dollar invested in reducing disaster risks, two to four dollars can be saved, and they are needed for humanitarian aid, rehabilitation and reconstruction.

One of the key strategies of these efforts is, as foreseen by the Sendai Framework, a successor document to the Hyogo Framework, empowering women and persons with disabilities to publicly promote equitable and universally accessible reactions, recovery,

[8]Serbia is one of the signatory countries.

rehabilitation and reconstruction. Disasters have shown that the recovery, rehabilitation and reconstruction phase is actually a starting point for planning and preparing prevention and response to future disasters. It is then necessary to develop such systems through a participatory process, to adapt them to the needs of users, including social and cultural requirements, especially those based on gender.

5. CONCLUSION

The consequences of the assumption that disaster risk is gender neutral is: incorrect identification and risk assessment, inadequately conceived policy response, policy making and risk financing at the national and community level. The starting point for reducing disaster risk and promoting a culture of disaster relief lies in the knowledge of the dangers of both physical, social, economic and environmental disaster vulnerabilities that most societies face. We should always bear in mind that disasters do not discriminate, but people do (UNISDR, UNDP and IUCN, 2009).

A gender-inclusive, non-discriminatory approach to reducing disaster risk can achieve a beneficial result for families and communities, as women, if given equal opportunities, can perform multiplied functions properly – as participants in all security-building processes, as well as leaders in disaster risk reduction. It is very important that a woman is not always seen as a victim, but in the whole process of disaster risk reduction she has an active role, both during and after the disaster (Centre for Disaster Preparedness, 2010.c). One of the lessons we have learnt from earlier disasters, which is always stated in the context of gender aspects, is that it is very important to involve expert women when recovery interventions are planned (UNISDR, 2007).

For this reason, laws, policies and practices should take into account the fact that, due to different economic, social, reproductive and political roles of men and women, they also have different capacities and needs in responding to the effects of disasters and climate change. Disaster risk reduction must be integrated into all policies, plans and programmes for sustainable development and poverty reduction, and supported through bilateral, regional and international cooperation, as well as through various types of partnership (Oxfam-GB, 2011). It is evident from previous practice that women taking on multiple roles on behalf of their communities are able not only to strengthen the capacity of their community to deal with catastrophes, but also to build active citizenship dealing with development priorities, which are inextricably linked to the reduction vulnerability. In doing so, resilience to disasters, community development and empowerment of women are elements of unique, but not separated, efforts (ISDR, 2007).

6. REFERENCES:

Bangladesh - Rebuilding Cyclone Sidr Victims. Retrieved on 21 September 2018 from http://www.youtube.com/watch?v=QJjACB5k0Vk.

Begum, R. (1993). Women in environmental disasters: the 1991 cyclone in Bangladesh. Focus on Gender 1 (1), 34-39. Retrieved on 20 September 2018 from https://www.gdnonline.org/sourcebook/chapt/doc_view.php?id=7&docid=776.

Building Resilience to Natural Disasters: A Framework for Private Sector Engagement. World Economic Forum The World Bank, United Nations International Strategy for Risk Reduction. (January 2008). Retrieved on 10 June 2018 from http://www.unisdr.org/files/1392_DisastersRepFINCopyright.pdf.

Gender Perspective: Working Together for Disaster Risk Reduction, Good Practices and Lessons Learned. (June 2007). Geneva: United Nations ISDR.

Halvorson S. J. & Hamilton J. P. (2005). The 2005 Kashmir Earthquake: A Perspe-ctive on Women's Experiences, Geography Faculty Publication 27 (4), 296–301.

Retrieved on 26 August 2018 from https://scholarworks.umt.edu/cgi/viewcontent.cgi?article=1001&context=geography_pubs.

Handbook, Women Leadership in Disaster Risk Management. (2011). Bangladesh: Oxfam-GB. Retrieved on 26 June 2018 from http://www.preventionweb.net/files/submissions/19919_makeup2englishfinal.pdf.

History.com Editors, (2009). Bangladesh Cyclone of 1991. New York City: A&E Television Networks. Retrieved on 19 September 2018 from http://www.history.com/topics/bangladesh-cyclone-of-1991.

Hyogo Framework for Action 2005-2015: Building the resilience of nations and communities to disaster, Mid-term Review 2010-2011. (March 2011). Geneva: UNISDR. Retrieved on June 23, 2018 from https://www.unisdr.org/files/18197_midterm.pdf.

Integrating Gender into Community Based Disaster Risk management: Training Manual. CBDRM Training and Learning Circle Philippines (2010). Retrieved on June 15, 2018 from http://library.pcw.gov.ph/sites/default/files/Integrating-Gender-into-CBDRM-Training-Manual.pdf.

Jungehülsing, J. (2012). Gender Relations and Women's Vulnerability to Climate Change, in Climate Change, Mexico City: Heinrich Boell Stiftung. Retrieved on 13 June 2018 from http://www.boell.de/downloads/2012-04-gender-climate-change-tabasco.pdf.

Making Disaster Risk Reduction Gender-Sensitive, Policy and Practical Guidelines. (2009). Geneva: Published by UNISDR, UNDP and IUCN. pp. 24, 35, 44, 46 and 133. Retrieved on 8 June 2018 from https://www.unisdr.org/files/9922_MakingDisasterRiskReductionGenderSe.pdf.

Mathbor, M.G. (2016). Local Capacity Building in Humanitarian Crises: An Effective Dealing Strategy for Bangladesh. Sociology and Anthropology 4(5), 408-415.

Most tsunami dead female – Oxfam. (26. March 2005). BBC NEWS. Retrieved on 22 December 2012 from http://news.bbc.co.uk/2/hi/asia-pacific/4383573.stm.

Mršević Z., Janković S. (2018). Inkluzivna bezbednost kao način smanjenja rizika od katastrofa i pratećeg nasilja. U: Macanović, N. (2018). Ne nasilju, jedinstveni društveni odgovor. (str. 401 – 411). Banja Luka: Centar modernih znanja.

Neumayer E., Plümper, T.(2007). „The Gendered Nature of Natural Disasters: The Impact of Catastrophic Events on the Gender Gap in Life Expectancy", Annals of the

Association of American Geographers 97(3), 551-566. Retrieved on 21 July 2018 from http://gsdrc.org/document-library/the-gendered-nature-of-natural-disasters-the-impact-of-catastrophic-events-on-the-gender-gap-in-life-expectancy/

Singh D. (2012). IDDR 2012 - Putting women and girls on the map, Geneva: Published by UNISDR. Retrieved on 21 September 2018 from http://www.unisdr.org/archive/28886.

Žene i LGBT osobe nevidljive su žrtve katastrofa.(10. mart 2018). Zagreb: Libela portal. Retrieved on 8 July 2018 from https://www.libela.org/prozor-u-svijet/9386-zene-i-lgbt-osobe-nevidljive-su-zrtve-katastrofa/.

The Hyogo Framework for Action 2005-2015: Building the resilience of nations and communities to disaster. (19 April 2008). Strasbourg: Council of Europe. Retrieved on 5 June 2018 from http://www.coe.int/t/dg4/majorhazards/ressources/Apcat2005/APCAT-2005-25-Hyogo-frameworkISDR.pdf.

UDK 342.7-055.2
https://doi.org/10.18485/fb_ic4hs.2018.26

IMPACT OF THE GENDER DIGITAL DIVIDE ON SECURITY AND WOMEN'S HUMAN RIGHTS

Ksenija ĐURIĆ-ATANASIEVSKI[*], Brankica POTKONJAK-LUKIĆ [**]

Abstract: The problem of the gender digital divide is recognized today as a problem of women's human rights, but also as a social, economic and security problem. It involves a number of international actors because it is estimated that, without progress in solving the gender digital divide, the gap between the presence of women and men in Internet communication technologies will increase, causing even greater gender differences, but also the economic, social and security vulnerability of women globally.

Unequal conditions for women and men in the economy and different economic opportunities for one or the other gender have existed for a long time, but digital technologies have made this problem even more visible and acute. Most jobs come from science, technology, engineering and mathematics (the so-called STEM), but it is estimated that in the developed world only 12% of students of technical sciences are female.

The social and economic empowerment of women, i.e. work engagement in digital technologies, diminishes their overall vulnerability. In addition to the positive economic effects, knowledge in the use of ICT increases awareness and the use of positive knowledge in other spheres of life, such as, for example, security, protection of human rights, healthcare, legal issues, environmental protection or culture.

The problem of the gender digital divide requires the consideration of the causes of gender inequality in education, of the possibilities of educating boys and girls and the availability of information literacy, but also of the causes that come from other areas such as education based on religious and ethnic postulates or prejudices about gender roles and the intellectual abilities of boys and girls. These causes may exist in the legal and political sphere, and especially in the sphere of security and protection.

The paper presents the solutions for overcoming the gender digital divide and its impact on women's lives and security. It also presents the situation in Serbia, providing data on the

[*] Associate professor, PhD, Department of Management, National Defence School ksenija.djuric@mod.gov.rs l

[**] PhD, MoD of the Republic of Serbia; brankica.lukic-potkonjak@mod.gov.rs

gender digital divide and comparisons with the situation globally. Possible measures for reducing the existing differences are analyzed from the perspective of the implementation of Serbian documents and strategies for gender equality and the achievement of their goal – to increase women's security in terms of protecting their human rights more effectively.

Keywords: gender digital divide, gender equality, women's human rights, security of women

1. INTRODUCTION

Information and communication technologies (ICTs) have undergone similar development to other communication technologies. These new technologies have benefited those who already had access to other resources at greater rates than people who had fewer resources (de Haan, 2004; van Dijk, 2006). However, the unfolding of the digital evolution is happening at an unprecedented speed (Rogers, 2003).

The benefits of the development of ICT are undeniable in all areas of society and the lives of individuals. Those who do not use ICTs are at a disadvantage economically, socially, politically and educationally (Morahan-Martin, 2000**).** ICTs are seen as necessary ingredients for economic development in the so-called 'knowledge society'. Internet search, online multimedia resources, social media, as well as services such as e-government, e-health, e-banking, e-learning, e-commerce, and e-voting, all create new arrangements of communication, engagement and social and economic behaviour (European Parliament, 2018). Nevertheless, differences have remained in Internet access, Internet use and its impact. The term "digital divide" refers to the gap between individuals, households, businesses and geographic areas at different socioeconomic levels with regard to their opportunities to access ICTs and their use of the Internet for a wide variety of activities (Organization for Economic Cooperation and Development, 2001). In academic papers and research based on different theories, the digital divide is seen as a social issue. At the level of the individual, the digital divide exists as a difference in the use of digital technologies in terms of age, place of residence, indigenous wealth, ethnic origin or belonging to one or the other sex. In that context, the available data disaggregated by sex and their analysis show that the gender digital divide affects women to a much greater extent than men. Women have traditionally been underrepresented in regard to the use and especially development of ICT. This undeniably has a negative impact on all aspects of women's lives, first of all on the protection of their human rights and security, which is an essential precondition for the individual empowerment of women and their social development in every way.

2. WHY IS THE GENDER DIGITAL DIVIDE IMPORTANT?

The unequal use of the Internet by men and women is an inequality that has been identified as one of the most important forms of the digital divide. The "gender digital divide (GDD)" refers to the measurable gap between women and men in their access to, use of and ability to influence, contribute to and benefit from ICTs (Human Right Council UN, 2017). The International Telecommunication Union (ITU) has described the GDD as

a gender-driven imbalance in access to ICTs, general ICT literacy and presence in science, technology, engineering and mathematics studies (ITU, 2012).

The differences between male and female ICT users are of increasing interest worldwide as the digital divide evolves. The GDD is more prominent in the developing world, where 80% of the world's population of women lives, but it still exists in the developed world. According to the International Telecommunication Union (ITU, 2016), "the global Internet user gender gap grew from 11% in 2013 to 12% in 2016".

Gender-based discrimination and disparities in the physical world are being replicated in the digital world (Federal Ministry for Economic Cooperation and Development of Germany, 2017). Barriers such as the cost, network coverage, security and harassment, trust and technical literacy, language barriers and barriers to women speaking freely and privately online all contribute to the fact that women in developing countries are nearly 25% less likely to be online than men (Intel Corporation, 2018).

In a study titled *Gender and Digital Agenda*, the European Institute of Gender Equality (EIGE, 2016) provides an overview of gender inequality issues in digitalization and identifies gender differences not only in access to and use of digital technologies, but also in digital-related education and other fields of study between girls and boys, in women's low participation in the digital labour market and in the impact of cybercrime on women.

The digital divide can be understood as the existence of inequalities in four successive types of *access:* motivation, physical access, digital skills and different usage. It is claimed that the divide has shifted from the first to the last-called type of access in the last ten years (van Dijk, 2012). The offline population is disproportionately poor, rural, older and female, and the gap between them and those who have access to the Internet is widening steadily. Worldwide, it is estimated that approximately 250 million fewer women than men are online (Philbeck, 2017). The development of mobile telephony has made access to the Internet easier. However, there are still 200 million fewer women than men who have access to mobile phones in developing countries. Women's access to ICT is constrained by factors that go beyond issues of technological infrastructure: socially and culturally constructed gender roles shape and limit the capacity of women and men to participate on equal terms.

There is also an inequality in Internet *use* between men and women. Some researchers believe that more men than women use the Internet because of gender differences in socio-economic status, some explain this as gender differences in gender roles and others still as gender-influenced perception of computer technology (Hafkin, 2013). The education of boys and girls is based on the creation of gender roles which are the result of social expectations and stereotypes in many societies. It is believed that boys are more interested in ICT (Faulkner, 2001, Nsibirano, 2009). The research of Livingstone and Helsper (2007) confirms that there are no gender differences in computer usage among younger children (7–11 years) but that the gender gaps expand significantly in their mid-teens (16–17) – by then, boys use the Internet more frequently and perform a wider range of activities than girls. Women need to have the knowledge and resources to translate access into effective use (Human Rights, Big Data and Technology Project, 2016). It is necessary to have digital literacy and digital competence. Men use the Internet more than women for a wide range of activities, particularly those that require greater technological skills such as job

searching, e-banking, and posting or uploading material, while women like it for the human connections it promotes (Fallows, 2005). Other reasons for the gender inequality in the use of ICT are *socio-cultural barriers* such as the patriarchal system in many developing countries that only allows women (unpaid) household work and impedes schooling. In developed countries, women can also be unemployed or burdened with the "triple burden" – work, home and community.

ICTs are increasingly being recognized for their potential to carry the new global knowledge-based economy. The ICT market itself presents many opportunities for growth through the development of software products for a variety of purposes, the expansion of social media and other large corporate platforms, the development of news goods and services, the evolution of artificial intelligence and the Internet of Things, or 'green growth' and the increasing demand for smart applications (ITU, 2012). ICTs also enable work from home, which is extremely important for women and their families.

The delay of women in digital education has led to an increase in the gender gap even in developed countries. In the world of information technology and computer science, men dominate not only numerically, but also in regard to their positions. Women in ICTs occupy low-level jobs and represent only 19.2% of managers in the ICT sector, compared to a much better share of 42.5% in the non-ICT service sector (European Parliament, 2018). The study Women in ICT explains this low representation of women in terms of stereotypes about women lacking relevant skills (including leadership skills and aptitude for STEM studies and careers); work-life balance complexities; male stereotypes and networking culture; and lack of role models.

While the use of ICTs has contributed to the empowerment of women and to a fuller realization of their human rights, it has also facilitated the development of *online violence against women*. The General Assembly of the UN acknowledged in its Resolution 68/181 that information technology-related violations, abuses and violence against women were a growing concern and could be a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights. Online violence against women encompasses acts of gender-based violence that are committed, facilitated or aggravated by the use of ICTs, including online threats and harassment and gross and demeaning breaches of privacy, such as "revenge pornography" (Women's Rights Online, 2015). Online violence has risen sharply over the past few years and can result in women limiting their participation on online platforms.

Such a situation should not lead to the conclusion that women should use ICT less. It is the responsibility of administrators, sites and platforms whose content could be classified as cybercrime to fight against online violence. Also, every empowerment of women and their increasing percentage in ICT proportionally empower their human rights.

3. HOW TO OVERCOME THE GENDER DIGITAL DIVIDE

Measures, activities and proposals for the solution of the gender digital gap are offered by numerous governmental and non-governmental organizations. Realization is largely left to national states. Solutions to the GDD problem are based on the fact that the gender gap goes beyond the nature of technology. Policies that only attempt to improve women's access to and more frequent use of digital technologies cannot solve the problem of the

gender split. They have to respect the political, economic or sociocultural factors that create the inequality of women in societies and improve their human rights. The technology and the Internet are not agents of change by themselves, but they encompass gendered characteristics and interact with social circumstances in complex ways. The aim of policy and practice is that the outcomes of such interactions work toward greater gender equality. Nonetheless, the settings in which ICTs are often placed might reproduce such inequalities or recast them in new forms as well (European Parliament, 2017).

Most of the proposals stem from the fact that overcoming or at least reducing the gender digital gap would have economically quantitative effects. The European Commission Report (2013) concludes that if as many women as men held jobs in the digital economy, this could boost the annual EU GDP with roughly EUR 9 billion. In addition to the economic advantages, numerous other benefits are also derived from greater and better involvement of women in ICT. The GDD is both a consequence and cause of violations of women's human rights. It is a consequence in that disparities in ICT access and use reflect the discrimination of women in society. The GDD is also a cause of violations of women's human rights: women without meaningful ICT access are less equipped to exercise their human rights and to participate in public life, the economy and society (United Nations High Commissioner for Human Rights, 2017).

A systematic approach to embedding human rights in efforts to tackle the GDD requires addressing the full range of women's human rights that are affected by ICTs. Inequalities in access to and use of the Internet and associated technologies have the potential to undermine the opportunities for realising human rights and attaining the Sustainable Development Goals (SDGs) as ICTs may function as a gateway to the realisation of human rights (Human Rights, Big Data and Technology Project, 2016)**.** Women who have access to ICT equipment and who are confident, skilled and capable of using it efficiently have been given an extremely valuable opportunity to contribute to their economic, social and political empowerment. Thereby, they can also be better aware of their legal rights and have a significant impact on improving the quality of their lives and increasing their personal safety and security. Today, communication through social media, mobile phone applications and websites is a powerful means of enabling women, *inter alia,* to raise their awareness of gender equality, different types of gender-based violence, and penalties for non-compliant behaviour. It also enables women to exchange experiences through networking, to report security risks and get in touch with adequate services that can support and help them in cases of any kind of abuse and violations of their human rights. On the other hand, it is more and more evident that using ICT has the potential to encourage new online risks and forms of violence against women and this is something women must be fully aware of.

There are several documents from international organizations that propose activities for closing the GDD. Some of them are: the Sustainable Development Goals (UN, 2015), the Action Plan in the ITU Report of the United Nations High Commissioner for Human Rights. The UN Sustainable Development Goals list the major goals that a country needs to achieve in order to overcome the GDD. UN Member States are required to: achieve universal affordable internet access by 2020 (SDG target 9.c); ensure equal access to basic services [and] appropriate new technology for all women and men (SDG target 1.d); implement policies to empower women through technology (SDG target 5.b). Beyond

these important targets, access to ICT is also critical to achieving other SDGs, such as: achieving quality education (Goal 4), creating decent work and economic growth (Goal 8) and reducing inequalities (Goal 10).

In 2014, the International Telecommunication Union (ITU) adopted an action plan to accelerate inclusive and sustainable development by closing the digital gender gap and harnessing the transformative potential of ICTs for women's empowerment. It can be understood as potentially challenging and changing the power relations between men and women and as enabling women to take greater control over their resources and lives in general. The broad aims of the Action Plan are: 1. Develop gender-responsive strategies and policies 2. Ensure access to ICTs by women and mitigate the online risks that hinder women's access to and use of technology 3. Build digital capacities and support development of content, applications and services that meet women's needs 4. Promote women in the technology sector, including in positions of decision-making 5. Establish multi-stakeholder partnerships.

4. THE GENDER DIGITAL DIVIDE IN SERBIA

Bearing in mind that the GDD is an inequality between men and women in the access, use and impacts of ICTs, statistical data in Serbia suggest that there is no gender digital gap for two of the three factors – access to and use of ICTs. According to data from 2016, the majority of users are women, and in most age groups more women than men are information literate.

However, when it comes to education, employment and the IT sector, statistics reveal that men have an advantage. In information technology, 74% of graduates in Serbia are men, compared with 88% of male students in some developed countries. A smaller percentage of women in ICT will determine a smaller number of women in all innovative economic branches that will develop from IT in the future.

In recent years, the Serbian government and relevant ministries have recognized the importance of increasing women's digital competencies and their participation in ICT considering that these jobs will be the most promising and well paid in the future. The importance placed on overcoming the GDD is also reflected in the fact that the celebration of the ICT Girls Day started in April 2010 at the initiative of Serbia.

The 2017–2020 Strategy for the Development of Information Technologies Industry, as well as the 2018 action plans for the implementation of the strategy envision many activities related to the GDD, such as: introducing information science in elementary schools; projects and programmes for the re-education of women that would enable them to be employed in the ICT sector or start their own business through start-up companies.

6. CONCLUSION

The GDD is recognized in politics, science and practice as one of the major problems in respecting women's human rights, but also as a developmental problem affecting all segments of society. Therefore, reducing the gender digital gap will positively contribute to economic, political and security development. In Serbia, the percentage of women who use ICT and are digitally literate is more favourable than in some developed countries. Although the percentage of women employed in the information industry is also higher

compared to some other countries, the situation is not favourable. It is necessary to undertake measures for empowering women in ICT as the technology of the future.

7. REFERENCES

Akcioni plan za 2018 za sprovodjenje Strategije razvoja industrije informacionih tehnologija 2017-2020 (in Serbian): Retrieved from http://www.srbija.gov.rs/vesti/dokumenti_sekcija.php?id=4567

Amy,A, Tuffley D.(2014). The Gender Digital Divide in Developing Countries, Future Internet. 6(4), 673-68.doi10.3390/fi6040673

Broadband Commission (2013). Doubling Digital Opportunities: Enhancing the Inclusion of Women and girls in the Information Society. Retrieved from http://www.broadbandcommission.org/documents/working-groups/bb-doubling-digital 2013.pdf

de Haan, J. (2004). A multifacte dynamic model of the digital divide. IT&Society. 1(7), p 66-88

Digging into Data on the Gender Digital Divide (2016) Web Foundation, Retrieve from https://webfoundation.org/2016/10/digging-into-data-on-the-gender-digital-divide/

Dighe, A and U. Reddi (2006) Women's Literacy and Information and Communication Technologies: Lessons that Experience has Tought us. Commonwealth Educational Media Centre for Asia, p.4.

European Parliament's Policy Department for Citizens` Right and Constitutional Affairs, Directorate General for Internal Policies (2018). The Underlying causes of the digital gender gap and possible solutions for enhanced digital inclusion for women and girls. PE 640.940

European Parliament (2012) Women in ICT. Brussels: Policy Department C - Citizens' Rights and Constitutional Affairs Brussels: European Parliament.

European Commission (2013) Women Active in the ICT Sector. Brussels: European Commission.

Fallows, D. (2005) How Women and Men Use the Internet. Pew Research Center. Internet and Technology. Retrieved from http://www.pewinternet.org/2005/12/28/how-women-and-men-use-the-internet/

Faulkner, W.(2001). The technology question in feminism: A view from feminist technology studies. Women's Studies International Forum.24(1)

Gender and Digital Agenda.(2016) Luxemburg: European Institute for Gender Equality.

Hafkin, N. (2013) Stocktaking and Assessment on Measuring ICT and Gender for the Partnership on Measuring ICT for Development. Task Group on Gender of the Partnership on Measuring ICT for Development, p.11.)

Hilbert, M. (2011). Digital gender divide or technologically empowered women in developing countries? A typical case of lies, damned lies, and statistics. Women's Studies International Forum, 34(6), 479-489. http://dx.doi.org/10.1016/j.wsif.2011.07.001

Human Rights Big Data and Technology Project (2016). Ways to bridge the Gender Digital Divide from a Human Rights Perspective, Human Rights Center of the University of Essex

International Telecommunication Union (2012). A Bright Future in ICT: Opportunities for a New Generation of Women. Geneva: International Telecommunications Union. Retrieved from https://www.itu.int/en/ITU-D/Digital-Inclusion/Women-and-Girls/Documents/ReportsModules/ITUBrightFutureforWomeninICT-English.pdf.)

International Telecommunication Union & UN Women (2015). Action Plan to Close the Digital Gender Gap. Retrieved from https://www.itu.int/en/action/gender-equality/Documents/ActionPlan.pdf

International Telecommunication Union "The gender digital inclusion map: research methodology" Retrieved from https://www.itu.int/en/action/gender-equality/PublishingImages/Pages/EQUALS/The%20Gender%20Digital%20Inclusion%20Map%20-%20Research%20Methodology.pdf

Livingstone, S, Helsper, E. (2007). Gradations in digital inclusion: children, young people and the digital divide. New media & society, 9 (4). pp. 671-696. DOI: 10.1177/1461444807080335

Morahan-Martin, J. (2000) Women and the Internet: Promise and Perils. Cyber Psychology and behaviour, Volume 3 No 5: 683-691

Nsibirano, R. (2009). "Him and Her" - Gender differentials in ICT uptake: A critical literature review and research agenda. International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2009, Vol. 5, Issue 5, pp.33-42.

Philbeck, I- (2017). Connecting the unconnected: working together to achieve Connect 2020 Agenda targets, background paper to the special session of the Broadband Commission and the World Economic Forum at the Davos Annual Meeting 2017, p. 7

Rogers, E. M. (2003). Diffusion of Innovations, 5th Edition (5th ed.). Free Press.

Understanding the Digital Divide, Organization for Economic Cooperation and Development, (2001)

van Dijk, J.A. (2005) The Deepening Divide: Inequality in the Information Society (1st ed) Sage Publication, Inc.

van Dijk, J.A. (2012) The Evolution of the Digital Divide. Digital Enlightenment Yearbook 201 2J. Bus et al. (Eds.) IOS Press, 2012 doi:10.3233/978-1-61499-057-4-57

Women and the Web. (2018). Intel Corporation & Dalberg Global Development. Retrieve on 23. June 2018 from https://www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf

Women's Pathways to the Digital Sector: Stories of Opportunities and Challenges (2017), Federal Ministry for Economic Cooperation and Development of Germany. Retrieved from https://www.itu.int/en/ITU-D/Digital-Inclusion/Women-and-Girls/Girls-in-ICT-Portal/Pages/Publications.aspx

Women`s Right Online: Translating Access into Empowerment (2015). Webfounation. Retrieved from http://webfoundation.org/docs/2015/10/womens-rights-online21102015.pdf

UDK 351.758(497.11)
https://doi.org/10.18485/fb_ic4hs.2018.27

THE LOCAL PERCEPTION OF URBAN SAFETY IN OPEN PUBLIC SPACES AS A PARAMETER FOR TOURIST ATTRACTIVENESS IN THE HISTORIC CORE OF SMEDEREVO, SERBIA

Aleksandra ĐUKIĆ[*], Milica RISTOVIĆ[**], Branislav ANTONIĆ[***]

Abstract: The concept of urban safety has been developed on the contemporary/broad feeling of human safety in open urban spaces. It is connected with ordinary people's fear of crime and crime perception. In this constellation, lack of urban safety is directly confronted with the always desired aspirations to make open urban spaces liveable, attractive and socially mixed. Indirectly, it can negatively influence other socio-economic conditions, which consequently downgrades extended urban areas. Therefore, urban safety is a demanding task for qualitative open public spaces in modern cities.

In the case of cities that are rich in cultural heritage, these aspirations are not just related to local residents, but to prospective visitors from the cultural tourism sector as well. Therefore, urban places with abundant cultural heritage and a high level of safety have better prospects to boost cultural tourism.

The aim of this paper is to examine the personal perception of urban safety in open public spaces in Smederevo, Serbia, and its role in upgrading the city's attractiveness for cultural tourism. This sector is underdeveloped in the city today despite the abundant cultural heritage of its historic core, with the exceptionally valuable medieval Smederevo Fortress, and the position of the city on the Danube, a major tourist route in Europe. It is assumed that the lack of urban safety in open public spaces located close to cultural heritage sites in Smederevo's historic core contributes to their underuse by local people, which further minimises their tourist attractiveness. Hence, a survey based on the actions of crime prevention through urban design and planning was conducted to examine the personal feelings of safety in open public spaces among local people from Smederevo. The results

[*] Associate professor, PhD, University of Belgrade – Faculty of Architecture, Belgrade, Serbia, adjukic@afrodita.rcub.bg.ac.rs

[**] MA Student, University of Belgrade – Faculty of Architecture, Belgrade, Serbia, ristovic.milica0906@gmail.com

[***] PhD Candidate and Teaching Assistant, University of Belgrade – Faculty of Architecture, Belgrade, Serbia, antonic83@gmail.com

of this survey imply that these spaces should be redesigned to be safe and more attractive for tourists.

Keywords: Urban Safety, cultural heritage, cultural tourism, survey, open public space, Smederevo, Serbia

1. INTRODUCTION – URBAN SECURITY

Since ancient time, cities have been major sites to advance human security and development. One of the UN's 2016–2030 Sustainable Development Goals, which should become the new global agenda for future urban development, has proposed that we should 'build cities and human settlements inclusive, safe, resilient and sustainable'. One of the proposed targets within that goal is: "by 2030, provide universal access to safe, inclusive and accessible, green and public spaces, particularly for women and children, older persons and persons with disabilities" (UN-SDSN, 2012). The European Urban Charter asserts "a secure and safe town free, as far as possible, from crime, delinquency and aggression" (CE, 1992) as the basic right for the citizens of European towns. Furthermore, urban planning, design and management of open public spaces influence people's feelings of safety. However, good governance supports safe cities.

Open public spaces in cities, as the main vibrant places for the everyday life of their citizens and visitors, should fulfil the criteria for successful functioning and social cohesion. The safety and security of an open public space, besides its accessibility, identity, comfort and liveability, is considered as one of the main factors for the validation of its quality. Currently, the perceived insecurity of open public spaces has become one of the main problems in cities (Valera & Guardia, 2014; Gehl, 2004; Gronlund, 2012), with important psychological and psycho-social consequences (Amerio & Roccato, 2005). Open public spaces which are perceived as safe and secure are often more occupied by users. A sense of safety influences people's behaviour and leads to gathering and social contact in open public spaces. People's sense of safety can affect their everyday routines and activities, and affect the way they choose their walking routes and places for rest and leisure (Barni et al, 2016).

The perceived safety of open public spaces is based on several factors, such as: perceived security, accessibility, maintenance, visibility in the area, the presence of greenery and water, streetlights, the concentration of users, the shape and size of the place (Fennelly & Crowe, 2013; Gronlund, 2012; Ellaway et al, 2005; Gehl, 2004; Borst et al, 2008; Schroeder & Anderson, 1984; Mehta, 2014). However, an open public space that has visible CCTV or police patrols is perceived to be safer. Comfort is another important criterion that influences the behaviour of people and their sense of safety (Gronlund, 2012; Gehl, 2004; Fennelly & Crowe, 2013).

Three factors are used in literature to describe perceived insecurity (Fernández & Corraliza, 1997). The first factor corresponds with personal competences to cope with crime, and is related to age, gender, behaviour patterns, physical fitness and self-confidence. The second one is related to previous personal and social, direct and indirect experiences of the place. The third is related to the environmental characteristics of the place, including:

- its physical aspects (street lightening, visibility, maintenance, vandalism) and
- its social aspects (concentration of users, gathering, and level of interactions between different groups).

The main goal of this research is to explore the perceived security and insecurity among the users of the main open public spaces in the city of Smederevo by analyzing and describing key environmental variables, and to provide suggestions for improving their safety.

2. METHODS AND RESULTS

This research uses a survey as a core method. Surveys are a suitable method for research that deals with thoughts, opinions, and feelings (Shaughnessy et al, 2011). As previously mentioned, they are very common in urban security. Personal perception of fear and discomfort in an open public space can be significantly different from actual trends and figures relating to it.

This survey was developed into a supplementary questionnaire with 12 questions (plus 3 demographic variables), organised in 4 thematic groups. The questions also differ by type: rating scale, yes-no questions, multiple choice, and semi-open questions.

The survey was conducted in the summer of 2018. The results of the survey were based on 100 completed questionnaires. At the beginning, it is important to give some information in brief regarding the structure of the survey respondents, based on the aforementioned demographic variables:

- The gender ratio was almost identical as the general ratio in Smederevo – 51% of the respondents were women and 49% were men; the general ratio is 50.7% to 49.3% in favour of women;
- The age structure was based on three main statistical groups (<18, 18-65, and >65 years of age). The ratio between the respondent groups was 13%/69%/18%, respectively. Compared to the general age structure in Smederevo (18%/65%/17%, respectively), the situation is also very similar, although the youngest group had a slightly higher representation.
- The third variable was about education. Among the respondents, there were 1% without elementary education, 4% with elementary education, 41% with a high school degree, and most of them, 51%, with a college or university degree; 3% had a specialisation, a magister or doctoral degree.

3. SURVEY RESULTS

3.1. SMEDEREVO AS A RESEARCH ZONE

The questionnaire was administered in the City of Smederevo, a medium-size city in central Serbia, 41 km east of Belgrade. The city is located on the Danube and represents the seat of the Podunavlje (Danube) District.

Smederevo has a rich cultural heritage dating back to the Roman period, through medieval to modern and industrial heritage sites. The most famous is the Smederevo Fortress, the seat of medieval Serbia in the fifteenth century (Fig. 1), and the Golden Hill (*Zlatni breg*), the royal summerhouse of the Obrenović dynasty. There are also several locations with well-preserved industrial heritage sites from the early twentieth century.

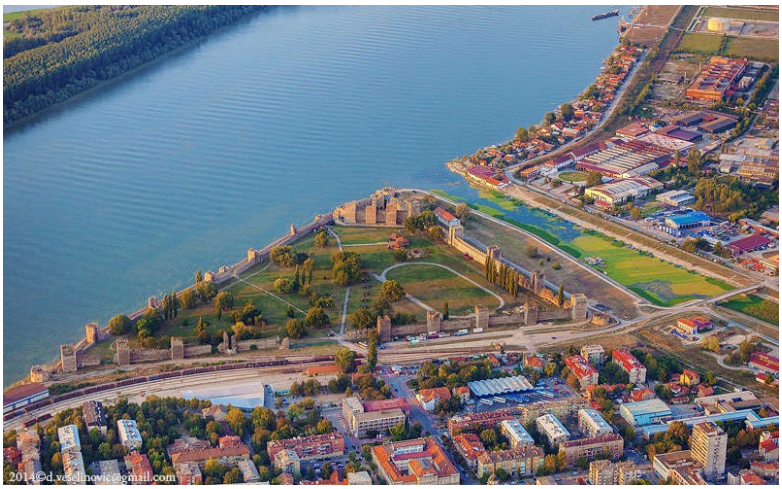


Fig. 1: Panorama of the Smederevo Fortress on the confluence of the Danube and the Jezava (Source: http://srbijauslici.blogspot.com/2015/03/smederevo-iz-vazduha.html)

The historic core of Smederevo is also a concentration of cultural heritage (Fig. 2). However, all these heritage locations are divided by the old railway as a barrier; it disables the physical connection and visual overview of the historic core, the Danube riverside and the fortress as a coherent urban and tourist zone.

Fig. 2: Aerial view of the city's central zone (Source: http://srbijauslici.blogspot.com/2015/03/smederevo-iz-vazduha.html)

The results of the survey were based on all completed questionnaires. As was already mentioned, the questionnaire was designed based on four groups of questions. The first group was related to the PERSONAL SENSE OF SAFETY, and included four questions, with separate responses for day and night.

In the first question, the respondents were asked to evaluate the safety of different places and areas in the central zone of Smederevo (Fig. 3). Cumulatively, there were nine places and areas evaluated in the first question:

Table 1: Comparative analysis of the personal perception of safety of places and areas in the central zone of Smederevo for day and night

NO.	PLACE / AREA	AVERAGE OF RATE SAFETY		THE MOST COMMON MARK	
		DAY	NIGHT	DAY	NIGHT
1.	Smederevo Fortress	3.86	2.03	4	2
2.	Danube quay and riverside	4.31	3.34	5	4
3.	Despot Đurađ Street	4.37	3.46	5	3
4.	Railway area	2.46	1.69	2	1
5.	Jezava Riverside	3.20	2.13	4	2
6.	City port area	3.05	2.23	3	1
7.	Karađorđeva-Goranska Street	4.24	3.29	5	3
8	Majdan Hill	2.78	1.77	3	1
1.	(Main) industrial zone	3.35	2.22	3	2
Note: 5 is the highest mark for the safety of a place/area, and 1 is the lowest mark.					

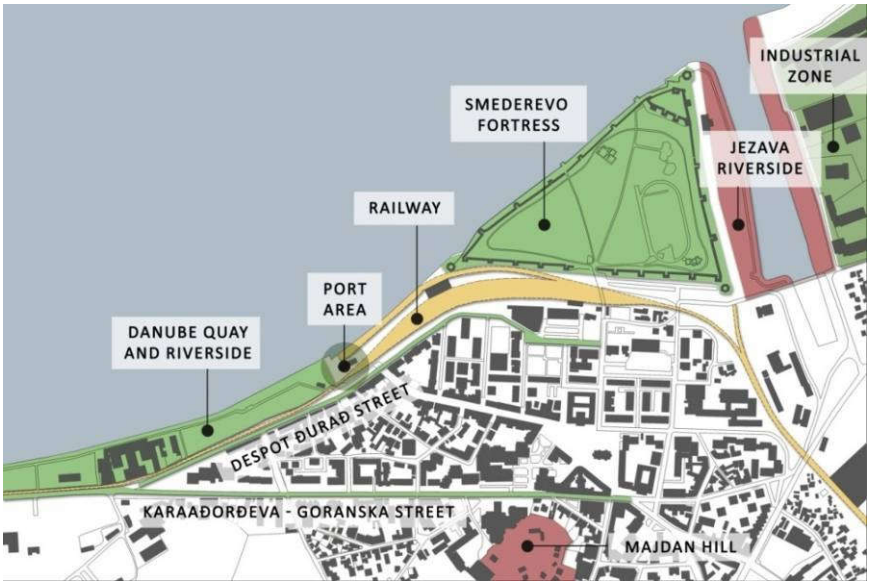


Fig. 3: Spatial disposition of listed places (Author: M. Ristović)

All selected places in central Smederevo are separately presented in the form of column charts (Fig. 4-6). In these charts, the evaluation of safety for each place is shown for day and night.

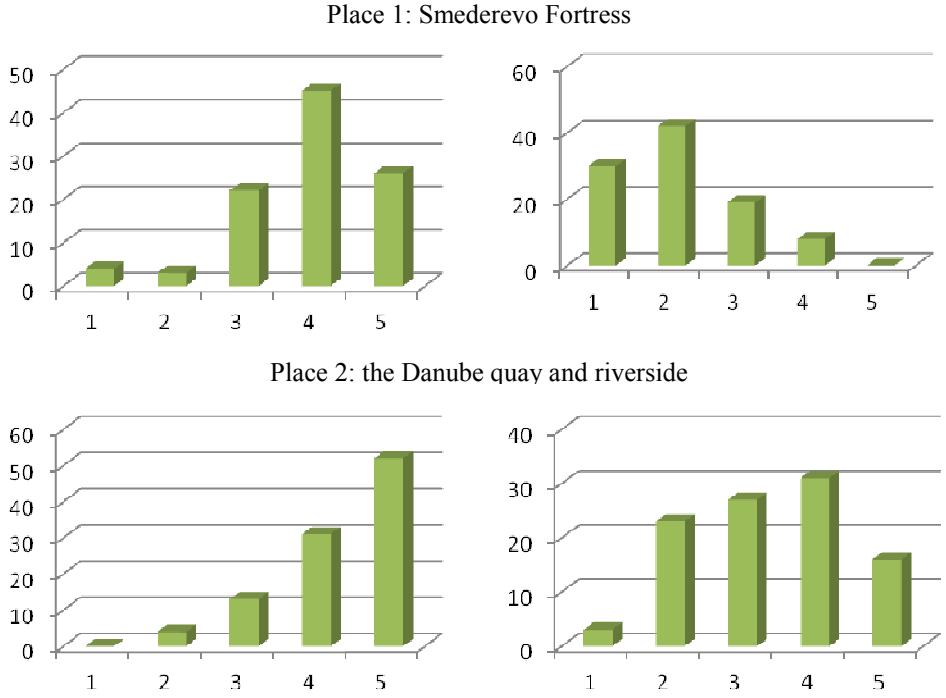
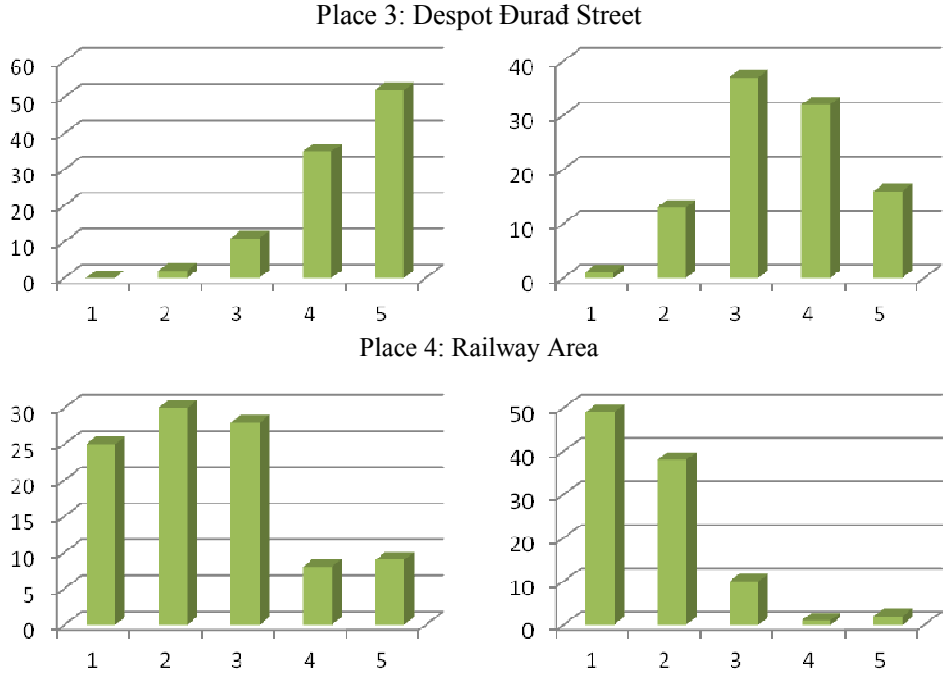


Fig. 4: The evaluation of the safety of selected places in central Smederevo – part 1 (Left chart - daytime; Right chart - night-time) (Author: M. Ristović)



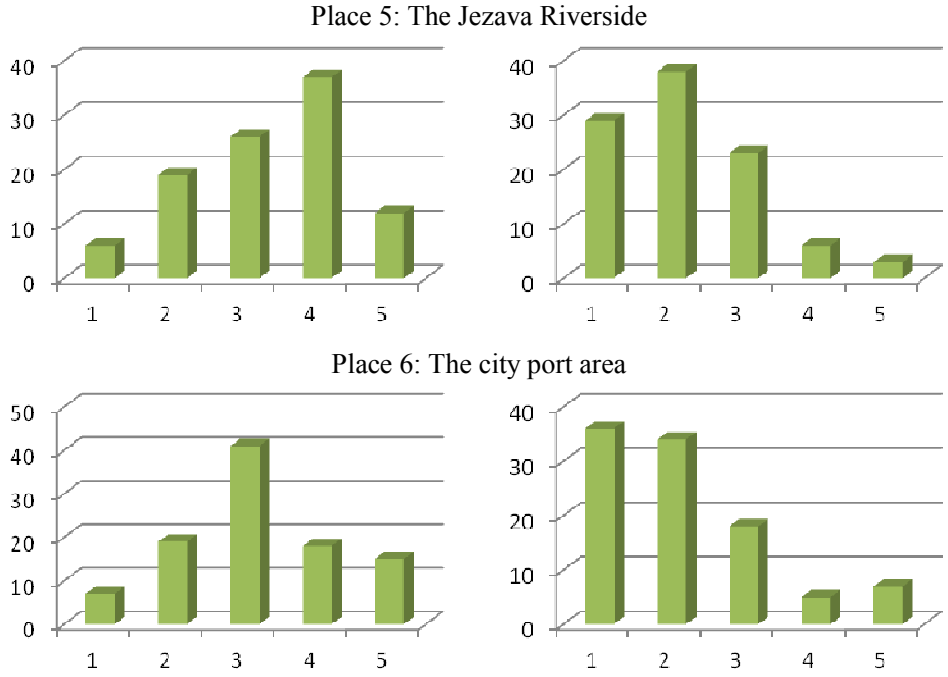
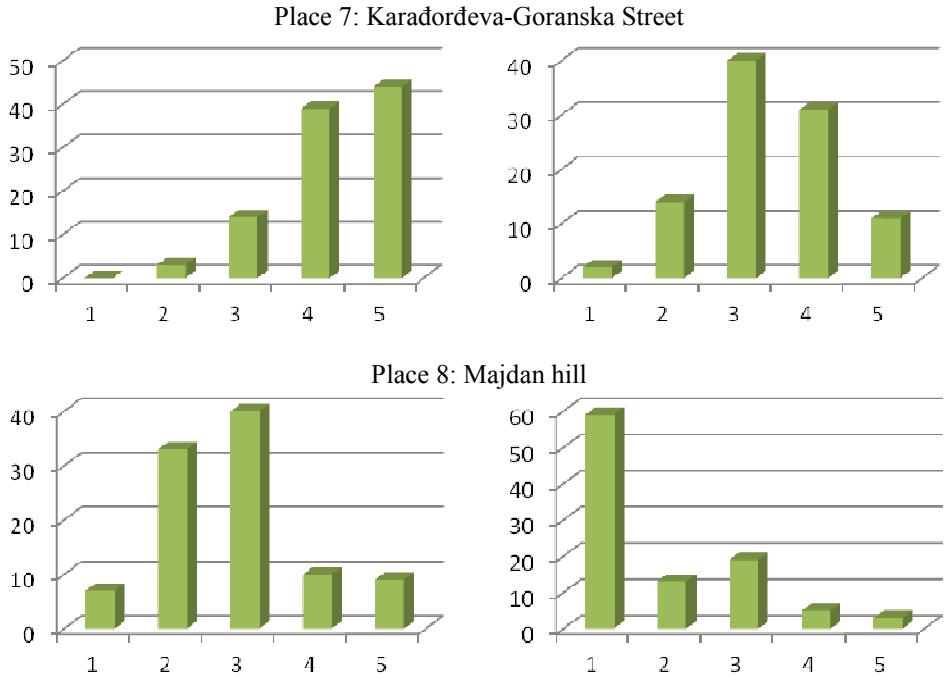


Fig. 5: The evaluation of the safety of selected places in central Smederevo – part 2 (Left chart daytime; Right chart - night-time) (Author: M. Ristović)



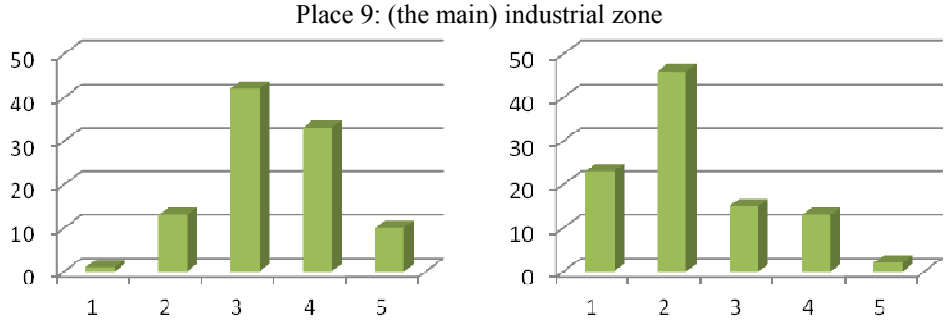


Fig. 6: The evaluation of the safety of selected places in central Smederevo – part 3 (Left chart -daytime; Right chart- night-time) (Author: M. Ristović)

In the second question (Fig. 7), the respondents were asked if they avoided any places in the city for safety reasons. During the day, 41% of the respondents kept away from some places because they considered them unsafe. During the night that percentage was expectedly higher – 79%.

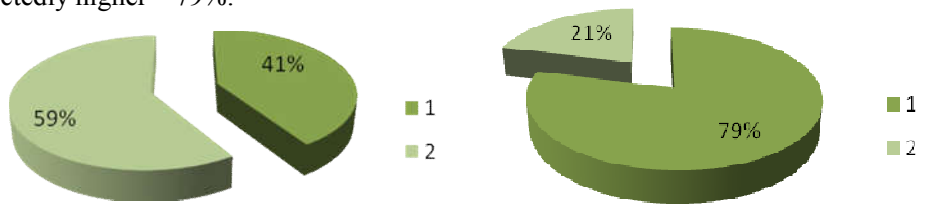
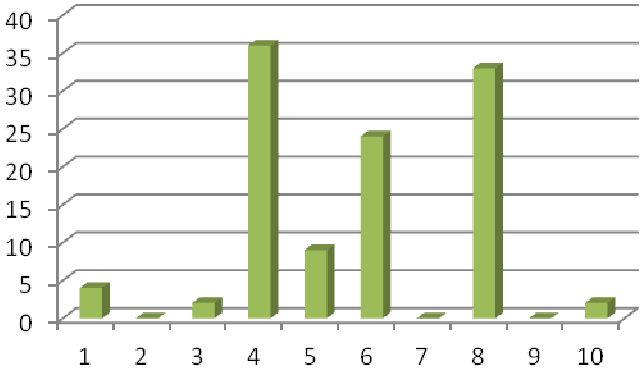


Fig. 7: The question "Are there places in the city that you avoid for safety reasons?" for day (left) and night (night) (Author: M. Ristović)

The next few questions were related to this one. The respondents were asked if they avoided some places for security reasons and which places they kept away from. All the sites whose safety they evaluated in the first question were listed, and there was a possibility to name a place which was not listed. The respondents were able to provide more than one response, but they were also asked to name the least safe place. As in the previous question, the responses for day and night were also separated.



1) Smederevo Fortress
2) Danube quay and riverside
3) Despot Đurađ Street
4) **Railway area**
5) Riverside of the Jezava
6) **The area around the Port**
7) Karađorđeva - Goranska Street
8) **Majdan Hill**
9) Industrial zone
10) Other

Fig. 8: The question “Which places do you avoid for safety reasons during the day?” (Author: M. Ristović)

During the day (Fig. 8), when 41% of respondents avoided some places, they mostly avoided the Railway area, but the area around the city port, which is located on the railway trace, and Majdan Hill were also really close in terms of the number of marks

Most people designated the Railway area as the least safe (42%), but Majdan Hill with 32% and the area around the port with 16% were also mostly designated as the least safe during the day (Fig. 9).

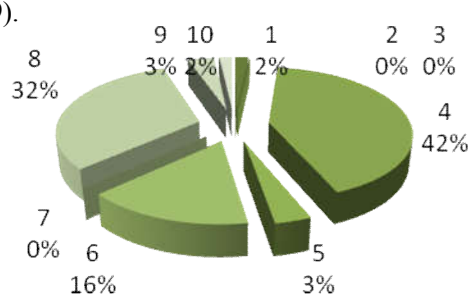


Fig. 9: The question "Which place do you consider the least safe during the day?" - Number of the listed responses is the same as in the previous question (Author: M. Ristović)

The respondents were also asked what made the place marked in the previous answer the least safe unsafe by day (Fig. 10), and the most common answer for this period was disrepair and lack of maintenance (36%), but there were also the large number of feral dogs and the usage of traffic intersections with 21%; the third reason was mostly provided for the railway or the port area as the least safe sites.

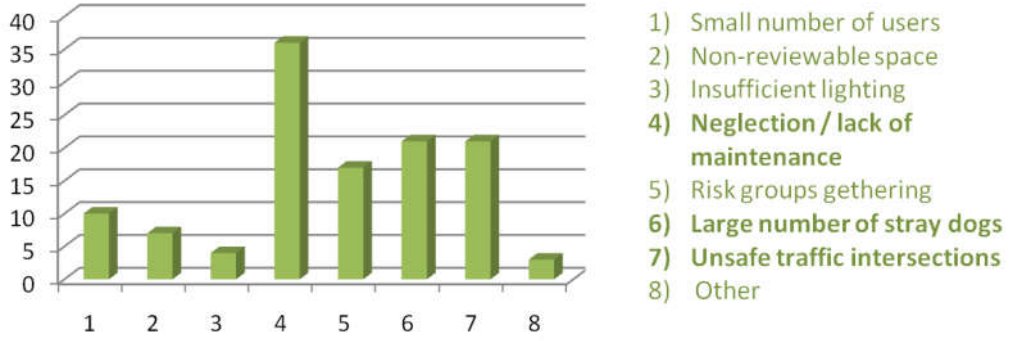


Fig. 10: The question "What makes the place marked as the least safe unsafe during the day?" (Author: M. Ristović)

During the night (Fig. 11), when 79% of respondents avoided some places, they mostly avoided the same places as in the daytime: the Railway area, the area around the port and Majdan Hill, but also the Smederevo Fortress, which was not a frequent answer for the daytime.

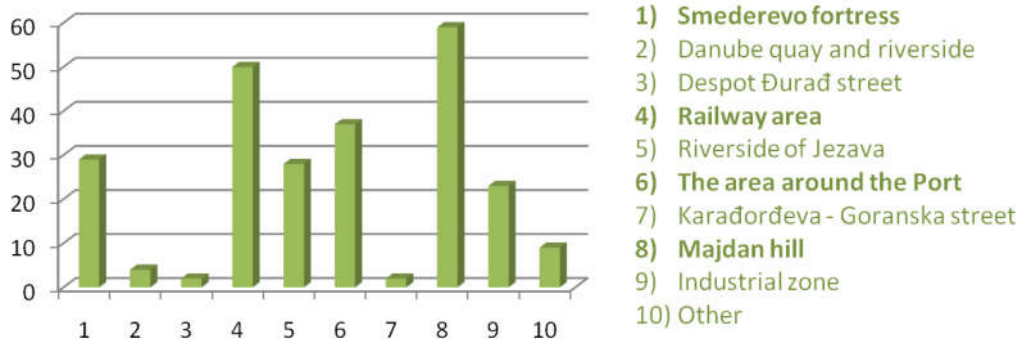


Fig. 11: The question "Which places do you avoid for safety reasons during the night?" (Author: M. Ristović)

Half of the respondents (Fig. 12) designated Majdan Hill as the least safe during the night (50%), which was one of the most frequent answers for the daytime as well. The area around the city port, with 12%, and the Smederevo Fortress, with 11%, were also frequent answers. Once again, it is noticeable that the results match, so the Smederevo Fortress appears as an answer in both questions.

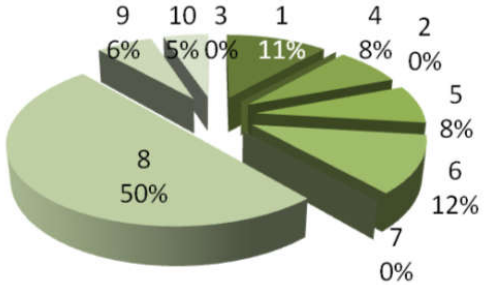


Fig. 12: The question "Which place do you consider the least safe during the night?" - number of the listed responses is the same as in the previous question? (Author: M. Ristović)

As the answer to the question about what made the least safe places unsafe during the night (Fig. 13), the respondents provided slightly different responses, so it is evident that they are mostly afraid of encountering dangerous groups of people, which was not the case in the daytime. Insufficient lighting also logically appears as a problem only during the night-time.

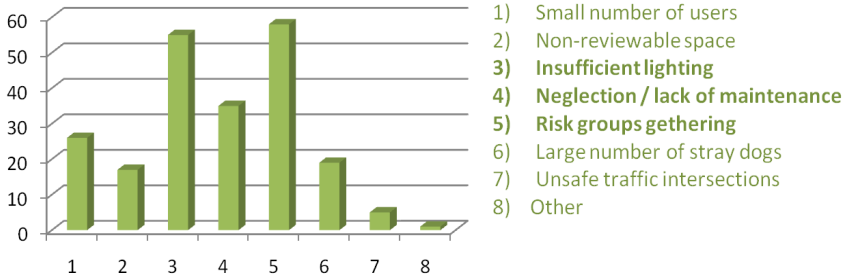


Fig. 13: The question "What makes the place marked as the least safe unsafe during the day?" (Author: M. Ristović)

The second group of questions was related to REAL DANGERS. The respondents were asked if they or someone close to them had ever experienced an accident in the public area of the central zone of the City of Smederevo, and 14% of them responded that they did.

The next two questions were related to the type of accident and the place where they experienced it. From 18 accidents that people experienced (Fig. 14), ten were verbal violence (51%), four were physical attack (11%), and two were pickpocketing and mugging. Nobody experienced sexual abuse or murder as an eyewitness.

The places in the central zone of the city were the accidents occurred were the Smederevo Fortress (2), the Danube quay and riverside (2), Despot Đurađ Street (2), Karađorđeva-Goranska Street (1), and other places such as the Republic Square, or some sites in the peripheral zones of the city.

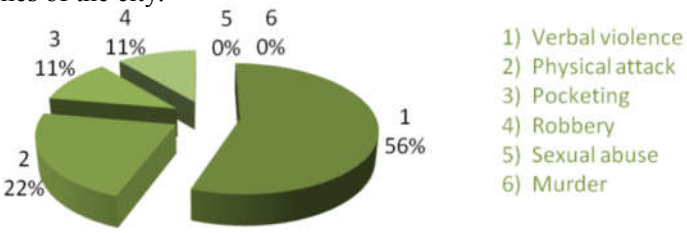


Fig. 14: The question "If you, or someone close to you, have ever experienced an accident in the public area of the central zone of the City of Smederevo, what kind of accident was it?" (Author: M. Ristović)

The third group of questions was related to VIDEO SURVEILLANCE, where people were asked if they knew which public spaces were covered by video surveillance, how it influenced their sense of safety, and if they thought that video surveillance of public spaces violated personal privacy.

The results showed that 30% of the respondents knew which parts of public spaces were covered by cameras (Fig. 15). An equal percentage thought that it violated privacy (Fig. 16), but not the same respondents, because most of those who responded that they knew which places were covered also responded that it did not violate their privacy.

When it comes to the sense of security (Fig. 17), the same percentage of respondents (49%) responded that video surveillance made them feel more secure, and that it did not affect their sense of security, while only 2% of the respondents responded that they felt less secure.

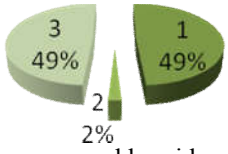


Fig. 15: Left pie chart – the question "Do you know which public spaces are covered by video surveillance?" (1-yes, 2-no)

Fig. 16: Middle pie chart – the question "Do you think that video surveillance of public spaces violates your privacy?" (1-yes, 2-no)

Fig. 17: Right pie chart – the question "Do you feel safer when a public space is covered by video surveillance?" (1-I feel safer, 2-I feel less safe, 3- It does not affect my sense of security) (Author: M. Ristović)

The fourth and last group of questions referred to the POLICE. The first question in this group required the respondents to indicate if they had confidence in the police force or not (Fig. 18). The second/the last question was related to the way an increased police presence in public spaces affected the respondents (Fig. 19). Out of 100 respondents, 60% declared that they had confidence in the police and law enforcement; an almost identical number of respondents (58%) felt more secure with an increased number of police officers in public spaces; it did not affect the sense of security for 36%, and 6% of the respondents felt uncomfortable in that situation.

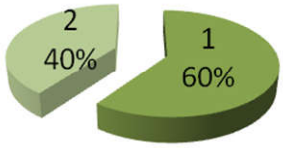


Fig. 18: The confidence of respondents in the police force (1 - yes, 2 - no) (Author: M. Ristović)

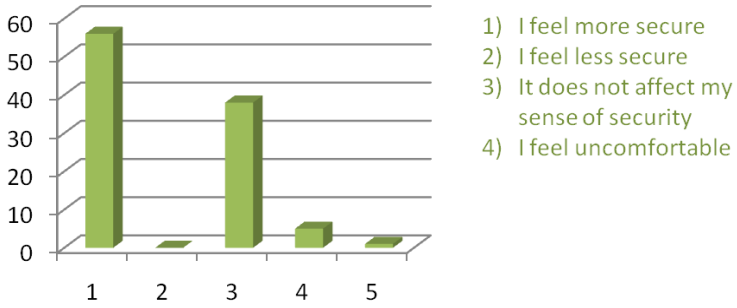


Fig. 19: The column chart for the question "How does an increased presence of the police in public spaces affect you?" (Author: M. Ristović)

4. DISCUSSION

After the overall examination of the results, it is obvious that most of the results match our theoretical presumptions. For example, the respondents gave the highest score to the safety of the areas that are intensively used by pedestrians, mostly in retail, residential and recreational zones with a high concentration of facilities. This was evident even if there was heavy traffic, such as in Karađorđeva-Goranska Street or Despot Đurađ Street.

Places with the highest scores (Despot Đurađ Street, Karađorđeva-Goranska Street and the city quay) are interconnected, but also connected with other urban facilities and functions in the city core. Places with the lowest ratings are mostly isolated (without any content that causes people to gather), not visited often, badly designed and inappropriately maintained. Those places where the railway represents a barrier for their access to the city centre (e.g. the fortress) are mostly marked as unsafe. This is evident for the railway itself, too.

When we take into account the responses about the characteristics which make places unsafe, the reasons for the respondents' insecurity are indicative:

1) Traffic insecurity – rail traffic in the pedestrian zone (railway) – there is no 'natural' way of intersection for these two types of traffic. The railway is a completely inflexible system with zero tolerance for pedestrian traffic;
2) Non-attractiveness and substandard maintenance – typical places are Majdan Hill or the area around the city port. They are characterised by physical and functional isolation from other public spaces, a lack of equipment, even unmaintained one, and a lack of content. Therefore, they visited infrequently despite their essential attractiveness (closeness to water/greenery, nice panoramas, etc.).

The real danger is actually very low – only 14% of the respondents have been in any real danger. Most of the accidents that people experienced were verbal violence (56%). Extreme forms of violence in public areas were not observed by the respondents. The most serious forms of accidents, such as physical attacks, pickpocketing or robbery, were reported in only 6% of cases.

There is not enough information about the existence of video surveillance, and 30% of the respondents think that it does not violate their privacy. The respondents are almost completely divided regarding their stance about their confidence in video surveillance in terms of their security in urban spaces. Nevertheless, the majority of the respondents have confidence in the police (60%), while mistrust and discomfort due to its increased presence are negligible.

5. CONCLUSIONS

The presented survey generally confirms that the safety and security of an urban space are an important factor of its quality. Those spaces with a higher level of security are considered to be of higher quality, regardless of their real value and importance in the network of urban spaces. Hence, they are visited much more frequently.

The results of the survey show the connection of security perceptions and three factors:

1) Personal competitiveness related to gender, age, the education structure, behaviour patterns, self-confidence;
2) Personal and public experience of space; and
3) Characteristics of space considering physical and social aspects. Different requirements and attitudes are recognized towards security in different categories of users of open public spaces.

Security and, consequently, the perceived quality of open public spaces affect the habits of people regarding their use. Safer spaces are often more attractive for users than similar spaces with a higher degree of insecurity.

Considering that Smederevo is located on the Danube, a major European tourism route, and that the city is planning new facilities in order to developed into a new tourist destination along this international river, several issues relating to the safety in open public spaces in the city should be improved by urban planning and design, to support these intentions:

- Removing unacceptable content from open public spaces (e.g. railways) - currently in progress;
- The functional revival and increase of attractiveness of neglected public spaces, in accordance with their importance and function in the network of public urban spaces. This is especially true for the interior of the fortress as the most prominent cultural heritage site in Smederevo;

Networking/interconnection of open public spaces, which should be implemented both physically (through arranged corridors) and functionally (distribution of urban facilities and activities);

Urban furniture, pavement and other urban equipment in open public spaces has to be of higher quality and contribute to urban safety. Using this approach is important in multiple ways, because it also increases urban values and enhances the local identity, which is crucial for tourism development.

6. ACKNOWLEDGMENTS

This paper is part of the national research projects No 36034 and No 36035, financed by the Ministry of Education and Science of the Republic of Serbia for the purposes of the project "DANube Urban Brand - a regional network building through tourism and education to strengthen the "Danube" cultural identity and solidarity", selected by the INTERREG Danube Transnational Programme.

7. REFERENCES

Amerio, P. & Roccato, M. (2005). A predictive model for psychological reactions to crime in Italy: an analysis of fear of crime and concern about crime as a social problem. *Journal of Community & Applied Social Psychology, 15*(1), 100-110. DOI 10.1002/casp.806.

Barni, D., Vieno A., Roccato M. & Russo, S. (2016). Basic Personal Values, the Country`s Crime Rate and the Fear of Crime. *Social Indicators Research, 129*(3), 1057–1074. DOI 10.1007/s11205-015-1161-9.

Borst H.C., Miedama, H.M.E., de Vries, S.I., Graham, J.M.A. & van Dongen, J.E.F. (2008). Relationship between street characteristics and perceived attractiveness for walking reported by elderly people. *Journal of Environmental Psychology 28*, 353-361. DOI 10.1016/j.jenvp.2008.02.010.

Council of Europe – CE (1992). *European Urban Charter*. Retrieved from https://rm.coe.int/168071923d.

Ellaway, A., Macintyre, S. & Bonnefoy, X. (2005). Graffiti, greenery and obesity in adults: secondary analysis on European cross-sectional survey. *British Medical Journal, 331*(7517), 611-612. DOI 10.1136/bmj.38575.664549.F7.

Fennelly, L. & Crowe T. (Eds.) (2013). *Crime Prevention through Environmental Design (3rd edition)*. Amsterdam: Elsevier.

Fernández, B. & Corraliza, J.A. (1997). Hacia una tipología de lugarespeligrosos, enrelación con el miedo aldelito. *Intervención Psicosocial 6*(2), 237–248. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=2012648.

Gehl, J. (2004). *Towards a fine city for people: Public Spaces for Public Life – London*. Copenhagen: Gehl Architects.

Grönlund, B. (2012). *Building safe living environments*. Retrieved from http://www.rikoksentorjunta.fi/material/attachments/rtn/rtn/jseminaarit/tampereenseminaarin2012alustukset/6CdYHbwzG/Bo_Gronlund_-_Turvallisen_kaupungin_rakentaminen.pdf.Amerio 1999.

Mehta, V. (2014). Evaluating Public Space. *Journal of Urban Design, 19*(1), 53-88. DOI 10.1080/13574809.2013.854698. Retrieved from https://www.fs.usda.gov/treesearch/pubs/14855.

Schroeder, H.W. & L.M. Anderson (1984). Perception of Personal Safety in Urban Recreation Sites. *Journal of Leisure Research, 16*(2), 178-194.

Shaughnessy, J., Zechmeister, E. & Jeanne, Z. (2011). *Research methods in psychology (9th edition)*. New York, NY: McGraw Hill.

United Nations - Sustainable Development Solutions Network – UN-SDSN (2012). *Indicators and a Monitoring Framework: Launching a data revolution for the Sustainable Development Goals*. Retrieved from http://indicators.report/targets/11-7/.

Valera, S., Guardia, J. (2014). Perceived insecurity and fear of crime in a city with low-crimes rates. Journal of Environmental Psychology, 38, 195.

UDK 004:351.78
https://doi.org/10.18485/fb_ic4hs.2018.28

SMART CITY ICT SOLUTIONS FOR ENHANCING HUMAN SECURITY

Ana PARAUŠIĆ*

Abstract: Over the past two decades there has been a considerable shift toward information and communication technology (ICT) solutions that try to solve urban problems and provide services more efficiently. Such efforts are expressed through the idea of smart cities, an initiative that seeks to transform urban governance, management and way of living with the use of modern digital technology. Smart city technologies are promoted as an advanced way to counter and manage urban insecurities and risks through the effective and efficient delivery of services. The main objective of this paper, therefore, is to review some existing ICT solutions that citizens could apply in improving their own security. Based on the existing academic literature and research data, a deeper analysis of ICT solutions for improving human security in the urban environment will be conducted. The basic criterion for choosing technological solutions for enhancing security is that citizens are involved in formulating and/or that they participate in how security services are conceived and delivered. Potential security consequences and vulnerabilities regarding ICT solutions for human security in the city will also be tackled. New ICT solutions create new vulnerabilities and threats, which could make city infrastructure, services and residents insecure and open to diverse forms of criminal activity.

Technology contributes to the improvement of urban security in various ways, for example in emergency telecommunication, surveillance and wireless video streaming, predictive policing with the help of ICT, social media monitoring, etc. The use of these technologies has been critiqued for being technocratic and top-down, enacting forms of governance that control and discipline citizens. They are also seen as tools for producing and reinforcing the neoliberal logics of urban management, which serve the interests of states and corporations more than they do those of citizens. However, the core idea in smart city security initiatives is how citizens themselves could contribute to their personal safety and the safety of other citizens in distress, i.e. how to create a 'citizen-centric' smart city.

* MA, Research Trainee and PhD student, University of Belgrade Faculty of Security Studies, parausicana@gmail.com

ICT solutions in smart cities that will be discussed here have a stronger citizens' perspective in addressing security issues. Cities can simultaneously host all kinds of smart initiatives designed to interact with and serve citizens in different ways and produce a diverse range of citizen participation. The involvement of citizens in these ICT solutions can help in creating long-term effectiveness rather than short-term efficiency. However, researchers and practitioners should bear in mind that smart city technologies entail a number of security threats and risks that are prone to exploitation, and could amplify potential human security vulnerabilities.

Keywords: smart city, ICT solutions, human security, citizens' participation, urban insecurities

1. INTRODUCTION

Contemporary urban settlements are places of unprecedented complexity and diversity, with growing numbers of residents. The challenges for contemporary cities are therefore very diverse and range from crime and violence, poverty and inequality and natural hazards to the inadequate provision of services, critical infrastructure and unemployment. Attempts at solving these problems and preventing them are quite different but almost all of them encompass an advanced technological component.

Over the past two decades there has been a considerable shift toward information and communication technology (ICT) solutions that try to solve urban problems and provide services more efficiently. Such efforts are expressed through the idea of smart cities, an initiative that seeks to transform urban governance, management and way of living with the use of modern digital technology (Kitchin & Dodgge, 2017: 1). Smart city technologies are promoted as an advanced way to counter and manage urban insecurities and risks through the effective and efficient delivery of services.

One of the important issues regarding smart city initiatives is citizen participation in city management and governance. There are several levels of citizens' involvement in formulating and participating in how services are conceived and delivered (most notably presented in Arnstein's ladder of citizen participation (Arnstein, 1969)). The significance of citizen participation has motivated promoters and planners to develop initiatives that are citizen- or community-focused (Cardullo & Kitchin, 2017: 4).

The main objective of this paper is to review some existing ICT solutions that citizens could apply in improving their own security. Based on the existing academic literature and research data, a deeper analysis of ICT solutions for improving human security in the urban environment will be conducted. The basic criterion for choosing technological solutions for enhancing security is that citizens are involved in formulating and/or that they participate in how security services are conceived and delivered. Potential security consequences and vulnerabilities regarding ICT solutions for human security in the city will also be tackled.

2. REVIEW OF SOME ITC SOLUTIONS FOR ENHANCING HUMAN SECURITY

Technology contributes to the improvement of security in the city in various ways, for example in emergency telecommunication, surveillance and wireless video streaming, predictive policing with the help of ICT, social media monitoring etc. The use of these technologies has been critiqued for being technocratic and top-down, enacting forms of governance that control and discipline citizens. They are also seen as tools for producing and reinforcing the neoliberal logics of urban management, which serve the interests of states and corporations more than they do those of citizens (Kitchin 2014; Vanolo 2014; Datta 2015; Luque-Ayala & Marvin 2016; Kitchin et al., 2017). However, the core idea in smart city security initiatives is how citizens themselves could contribute to their personal safety and the safety of other citizens in distress, i.e. how to create a 'citizen-centric' smart city.

There are a growing number of applications available that could be helpful in citizen reporting, social platforms to discuss urban security problems and emergency applications for alerting family and friends (Habeeb Rahman, 2013). The main advantage of these ICT tools is that they are easily accessible and user-friendly for everyone who has a smart device.

Sexual violence and harassment are major security challenges for women and girls in many cities around the world. The prevalence of this serious threat to human security has resulted in the launching of several very useful ICT solutions for addressing and preventing gender-based sexual harassment and violence. **Safecity**[1] is a web platform that crowdsources personal stories of sexual harassment and abuse in public spaces. The idea is to make this data useful for individuals, local communities and local administration by helping to identify the factors that cause the behavior that leads to violence and work on strategies for solutions. To tackle the serious issue of sexual violence against women, **Harassmap**[2] was developed as a web service with a digital map to address the harassment and abuses against women and change attitudes towards such abuses. It is a social platform for women to report harassment incidents via text messages and social media to increase awareness about sexual harassment and the necessity to report such crime. Inspired by Harassmap, the **FightBack** smartphone application enables women in Delhi to send SOS alerts via email, Twitter and Facebook to their friends and family any time they are in danger. The **Circleof6**[3] application allows users to choose six of their friends and alert them when they want immediate help or want to be interrupted when in an uncomfortable situation. Originally designed to prevent sexual violence among college students, the application is designed for everyone who needs help in distress. **Hollaback**[4]

[1] The collected data is aggregated as hotspots on a map indicating trends at the local level. It currently contains around 10,000 stories from over 50 cities in India, Kenya, Cameroon and Nepal. http://safecity.in/

[2] https://harassmap.org/en/

[3] https://www.circleof6app.com/

[4] https://www.ihollaback.org/

is an application designed to help women, the LGBT population and other marginalized groups to share their stories of harassment and its main aim is to initiate public conversations and to develop innovative strategies to ensure equal access to public spaces.

ICT solutions for improving human security in the city are developed for more general problems in urban areas like crime, vandalism, congested traffic or signs of physical or social disorder. **Retio**[5], an iOS application available for cities in Mexico, allows citizens to report and have real time information about what is happening in their city. Users are allowed to warn fellow citizens and keep them informed by tweeting about shootings, risky situations and traffic. In Dublin, there is **Fix-Your-Street**[6], where citizens can use an online tool to report the location of issues that need to be addressed (such as potholes, graffiti, broken streetlights, illegal dumping) (Cardullo & Kitchin, 2017).

As far as different problems faced by urban dwellers are concerned, the **Sentinel** smartphone application was developed to help users to inform family and friends about their location during medical emergencies, accidents or in critical situations when they are being robbed or stalked. The advantage of this application, which differentiates it from similar applications, is that it encompasses a range of different urban security problems but can also send alerts even when there is fear that the phone will be destroyed or when the phone is out of the network coverage area. Based on social activism, citizen journalism and geospatial information, **Ushahidi**[7] is one of the most ambitious projects that use crowdsourcing and enable local observers to submit reports on different incidents using their mobile phones or the Internet.

Apart from mobile applications, there are also initiatives to install interactive screens in different centers in cities where people could share useful information about security issues in their urban environment. The screens would provide details about safe and unsafe locations in the city, such as risk areas, or the nearest police stations or health services. To complement the interactive screens, there could also be community reporting centers where citizens could anonymously send reports to the police (Habeeb Rahman, 2013). In Dublin, **Dublinked**[8] is the city's open data store, sharing a mix of administrative and operational data, including some real-time datasets related to transport and the environment. Much of these data, along with statistical and administrative data published by other government agencies, are made available to the public through the Dublin Dashboard in the form of interactive maps, graphs and apps (Kitchin *et al*., 2016).

In several European cities, a number of Living Lab projects have been implemented. Living Lab is an open innovation environment in real-life settings in which user-driven innovation drives the co-creation process for new services, products, and societal infrastructures (Bergvall-Kareborn & Stahlbrost, 2009:357). As a part of smart city initiatives for enhancing human security, Living Labs have served for measuring air or

[5] https://ret.io/r/mx/DF/

[6] http://www.fixyourstreet.ie/

[7] https://www.ushahidi.com/

[8] http://www.dublinked.ie

noise pollution[9], or for more general issues such as raising the quality of life in a city, as in the Dublin Beta project.[10]

One of the main reasons for implementing ICT solutions for enhancing human security in the city is that research shows that, when faced with an emergency or a stressful situation, people will rather call a friend or a family member than report the incident to the police (Habeeb Rahman, 2013). People sometimes perceive the police as corrupt and insufficiently transparent and believe that reporting a crime is not going to solve their problem. This could be a useful way to change a grim statistic.

3. POTENTIAL CHALLENGES AND RISKS OF CITIZEN-CENTRIC ICT SOLUTIONS

While the advantages of ICT solutions for enhancing human security are undeniable, they are accompanied by unintended consequences and a variety of traditional problems (Datta, 2015; Townsend, 2013). New ICT solutions create new vulnerabilities and threats, which could make city infrastructure, services and residents insecure and open to diverse forms of criminal activity.

There are several preconditions for the successful implementation of citizen-centric ICT solutions (Habeeb Rahman, 2013). First is accessibility – in order to use the applications citizens need to have smart devices (Android or iOS). This precondition is not hard to meet in most developed cities around the world. But in other cities not all citizens have smartphones that could be used in emergency situations. Even in developed cities, there are marginalized or poor citizens that cannot afford a mobile phone. Second, there is the problem of connectivity, since proposed ICT solutions should work even when there is no possibility to connect online. Third, the time it takes to access an application needs to be reduced to a minimum because a citizen's primary concern in a life-threatening situation is to alert family and friends as soon as possible. Fourth, it is desirable for the proposed ICT solutions to be cost-free so that even the poorest and the most marginalized people could have access to them.

One of the major challenges for implementing ICT solutions is the safety of the stored data and user privacy. Reported incidents are publicly available and could be subject to serious misuse. Citizens use their phones when alerting family and friends or anonymously posting an experience of a crime, so skilled hackers could jeopardize their privacy (data on a person's movement and the places he/she visits or data on browsing habits). When using smart city ICT solutions, citizens create data that companies can then extract value from by mining them for the purposes of social sorting, predictive profiling, micro-marketing, and anticipatory governance (Kitchin 2014). Making cities "smart" by introducing modern ICT solutions has made systems exposed to software bugs, data errors, network viruses, hacks and criminal and terrorist attacks (Little, 2010; Kitchin & Dodge, 2011; Townsend, 2013). With interactive screens and community reporting centers, there is the possibility of

[9] https://fablabbcn.org/0000/01/06/smart-citizen.html; http://www.sensornet.nl/english

[10] http://dccbeta.ie/

duplicating reports or of false reporting of incidents, so there needs to be a strict procedure for monitoring and analyzing the data.

In practice, bottom-up, inclusive and empowering citizen involvement in key decision-making processes in cities is difficult to achieve. In the case of smart cities, there are few successful examples of co-produced and citizen-led initiatives to date (Cardullo & Kitchin, 2017). Sharing or crowdsourcing apps have largely been co-opted within an economic frame and are owned by companies rather than communally (McLaren & Agyeman, 2015).

4. CONCLUSION

ICT solutions in smart cities discussed here have a strong citizens' perspective in addressing security issues. Cities can simultaneously host all kinds of smart initiatives designed to interact with and serve citizens in different ways and produce a diverse range of citizen participation (Cardullo & Kitchin, 2017: 18). The involvement of citizens in these ICT solutions can help in creating long-term effectiveness rather than short-term efficiency. They could strengthen citizens' responsibility for their own safety as well the safety of their fellow citizens and contribute to the quality of life in the city.

Smart city technologies are promoted as an effective way to counter and manage uncertainty and risk in contemporary cities. However, researchers and practitioners should bear in mind that smart city technologies entail a number of security threats and risks that are prone to exploitation and could amplify potential human security vulnerabilities.

In smart cities, there are as yet relatively few cases where citizens have single-handedly developed, created and implemented ICT solutions. Usually, examples are drawn from community development initiatives undertaken through partnerships between community organizations and the state, but such initiatives have not yet been created with regards to the smart city.

5. REFERENCES

Arnstein, S. R. (1969). A ladder of citizen participation. *Journal of the American Institute of planners*, *35*(4), 216-224.

Bergvall-Kareborn, B., & Stahlbrost, A. (2009). Living Lab: an open and citizen-centric approach for innovation. *International Journal of Innovation and Regional Development*, *1*(4), 356-370.

Cardullo, P., & Kitchin, R. (2017). *Being a 'citizen'in the smart city: Up and down the scaffold of smart citizen participation: The Programmable City Working Paper 30.* Maynooth: National University of Ireland Maynooth.

Datta, A. (2015). New urban utopias of postcolonial India: 'Entrepreneurial urbanization' in Dholera smart city, Gujarat. *Dialogues in Human Geography*, *5*(1), 3-22.

Habeeb Rahman, D. (2013). *Megacity Challenges: Public Safety and Possible ICT Solutions.* Uppsala: Uppsala University.

Kitchin, R. & Dodge, M. (2011). *Code/Space: Software and Everyday Life.* Cambridge: MIT Press.

Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences.* London: Sage.

Kitchin, R., & Dodge, M. (2017). The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, 1-19.

Kitchin, R., Coletta, C., Evans, L., Heaphy, L., & Mac Donncha, D. (2017). *Smart cities, urban technocrats, epistemic communities and advocacy coalitions: The Programmable City Working Paper 26.* Maynooth: National University of Ireland Maynooth.

Kitchin, R., Maalsen, S., & McArdle, G. (2016). The praxis and politics of building urban dashboards. *Geoforum*, *77*, 93-101.

Little, R.G. (2010). Managing the Risk of Cascading Failure in Complex Urban Infrastructures In: S. Graham (Ed). *Disrupted Cities: When Infrastructure Fails,* pp. 27–39. London: Routledge.

Luque-Ayala, A., & Marvin, S. (2016). The maintenance of urban circulation: An operational logic of infrastructural control. *Environment and Planning D: Society and Space*, *34*(2), 191-208.

McLaren, D., & Agyeman, J. (2015). *Sharing cities: a case for truly smart and sustainable cities*. Cambridge: MIT Press.

Townsend, A.M. (2013). *Smart Cities: Big Data, Civic Hackers and the Quest for a New Utopia.* New York: WW Norton and Company.

Vanolo, A. (2014). Smartmentality: The smart city as disciplinary strategy. *Urban Studies*, *51*(5), 883-898.

UDK 351.78
https://doi.org/10.18485/fb_ic4hs.2018.29

HUMAN SECURITY – DEFINING AND APPLYING THE CONCEPT

Emil Sloth PEDERSEN*

Abstract:Since the conception of the concept of human security it has been the center of great debate. A part of this debate concerns what the human security concept points to in the world. I outline three positions on the ontology of human security. Human security as (1) a subject matter than can be universally defined, (2) as defined by headlines of political programs (3) as a discipline with norms, standards and methods. I analyze how these definitions of human security make for quite diverse interpretations of the role of human security in the world. This is part of an important assessment of the role of human security in dealing with a long list of challenges to the wellbeing of people all over the globe. I contribute to this assessment by discussing the role of human security in tackling challenges related to the environment and natural resources. These challenges are numerous and include global climate change in its totality, which pose a threat to the human lifeform, but also a variety of smaller and larger challenges some of which are related to climate change, some of which are not. I argue that the position from which human security best guide academic study and policy-making is as a discipline. I show the relevance of this argument in a case of natural resource management in Ghana. Analyzing this case, I show how the methodologies of the discipline contribute to a socially and environmentally sustainable management of natural resources. I discuss whether the experiences from the case-work can be extrapolated to other work dealing with sub-global challenges to human well-being and dignity. Finally, I discuss the transformative potential of the human security discipline in mitigating global climate change specifically and global challenges to human well-being more generally.

Kewords: human security, environment, climate change

1. INTRODUCTION

Human security - it sounds like something everyone would agree upon but this is not so. Since the conception of the concept it has been the center of great debate. A part of this debate is ontological, concerning what the human security concept points to in the world. In this paper, I outline three positions on the ontology of human security. That of human

* MA Student, Aarhus University, Denmark, emil497@hotmail.com

security as (1) a subject matter than can be universally defined, as (2) defined by headlines of political programs; or as (3) a discipline with norms, standards and methods. These three definitions of human security, make for three quite diverse interpretations of the role of human security in the world, which I will delve into in the first part of this paper.

This discussion is not merely a theoretical exercise. It is part of an important assessment of the role of human security in dealing with a long list of challenges to the wellbeing of people all over the globe. I contribute to this more general assessment by discussing the role of human security in tackling challenges related to the environment and natural resources. These challenges are numerous and include global climate change in its totality, which pose a threat to the human lifeform, but also a variety of smaller and larger challenges some of which are related to climate change, some of which are not. Against the backdrop of this discussion, I present insights into the potential of human security in tackling challenges to human rights, human well-being and human dignity at the global level as well as at the sub-global levels.

I begin by analyzing the three positions and argue that the position from which human security best guide academic study and policy-making is by thinking of human security as a discipline. I then show the relevance of these arguments in a case on challenges related to natural resource management in Ghana. Analzying this case of foreign-company encroachment on the land on which indigenous community depends, I show how the methodologies of the discipline contribute to a socially and environmentally sustainable management of natural resources. Subsequently I discuss whether the experiences from the case-work can be extrapolated to other work dealing with challenges related to the environment and natural resources specifically and other non-global challenges to human well-being in general. Finally, I will discuss the transformative potential of the human security discipline in mitigating global climate change, the elephant in the room when assessing any environmental and natural resource related challenge. This will offer insights into general challenges for the success of the human security endeavors at the global level.

2. HUMAN SECURITY AS (1) SUBJECT MATTER, (2) POLITICAL USE OR (3) DISCIPLINE

2.1. HUMAN SECURITY AS A SUBJECT MATTER

"Existing definitions of human security tend to be extraordinarily expansive and vague, encompassing everything from physical security to psychological well-being, which provides policymakers with little guidance in the prioritization of competing policy goals and academics little sense of what, exactly, is to be studied" (Paris, 2001, p. 88).

This quote by Roland Paris exemplifies the first position that I want to draw forth; human security as a subject matter. Paris does not believe human security is defined by what policy-makers do under the heading of human security. Rather, human security are phenomena that academics could study and that policy-makers could then seek to reach e.g. like economic growth. This idea was first propelled, at the end of the Cold War, by

scholars who wanted to break with the narrow focus on the political and military sector as the 'referent object' of study within classical security complex theory of International Relations (Buzan, Wæver & de Wilde, 1998, p. 15). The focus was sought widened to draw attention to the urgency of non-military threats (Buzan, Wæver & de Wilde, 1998, p. 2). Although the positions were many, one trend that emerged was that under the heading 'human security' the scope of threats to be regarded were the negative counterparts to 'the seven pillars of human security' as they were formulated by the UNDP in the 1994 Human Development Report. Namely threats to personal-, political-, economic-, health-, environmental-, community- and food-security.

For Paris, this list is so broad as to mean everything and thus nothing: "if human security is all these things, what is it not?" (Paris, 2001, p. 92). If we assume Paris' premise, that human security refers to a subject matter, then I agree that it is very hard to discern the boundaries of this subject matter in the debates on human security. This is not to say that the concept could not be narrowed down in specific application. Certainly, we could say that in a concrete case of water-shortage, striving towards human security would first and foremost be about securing a water-supply. But as Paris points out, it will be hard to reach any consensus on what the concept should be narrowed down to. As a subject matter, human security cannot in any coherent way guide academic study and policy-making. This is suboptimal, and looking at the third position, I will show that not accepting Paris' premise holds a greater promise for guiding academics, development practitioners, businesses and policy-makers alike in a coherent fashion. Before doing so, I will turn to the position that human security is defined by its political use.

2.2. HUMAN SECURITY AS POLITICAL USE

"14 years after human security was first taken up by the United Nations, its integration into the policymaking and policy practices of leading Western states and international institutions has revealed that talk of two different 'paradigms' – the radical counter-position of 'individual' and 'state-based' approaches, or between 'critical theory' and 'problem-solving' frameworks – has been much exaggerated" (Chandler, 2008, p. 427f)

This statement made by David Chandler exemplifies the second position that I want to draw forth from the debate on human security: that the meaning of the concept of human security is derived from its use in policy-making of leading Western states and international institutions. From this position, the evaluation of the novelty and accomplishments of human security is based on these policy practices. For Chandler, unlike proponents of other positions, human security is not defined by the framework of human security from the 1994 UNDP publication. This is also the premise of his critique; that human security is not the transformative concept that others claim it to be: "Human security is 'the dog that didn't bark', in that its integration into the mainstream of policymaking has reinforced, rather than challenged, existing policy frameworks" (Chandler, 2008, p. 428).

This criticism needs nuance as the state and international organizations policies under the heading of human security are diverse. In some cases, the language of human security has been transformative like UN operations on police-reform, disarmament, peace in relation

to vulnerable groups, and women and peacebuilding (Krause, 2014, p. 83). Despite this, Chandler is right that most of the policies undertaken in the name of human security have centered on securing individuals from threats of violence. These policies then resemble a security focus somewhere in between the narrow focus of traditional security policies and the much wider focus of the 'seven pillars' promoted in the 1994 UNDP Human Development Report (Krause, 2014, p. 84). Although Chandler might be right in his critique of the policies under the banner of human security, I do not accept his premise that human security is defined solely by its use in these policies. If we accept other definitions of human security, like for example the definition in the 1994 UNDP report, we may instead claim that there is a great gap between the human security concept, and the practices of many states and international organizations in the name of human security (Krause, 2014, p. 76).

2.3. HUMAN SECURITY AS A DISCIPLINE

The third position that I want to draw forth is the position that human security refers more to a way of working, than to a subject matter to be worked with or to the policy-practice under the human security heading. We find this position expressed by scholars like Des Gasper who argue that human security is a 'language' or a way of 'thinking' that is defined less by what it thinks about and much more by how it does so and how these thoughts are expressed in stories (Gasper, 2013, p. 69). We also find the position expressed in the United Nations Trust Fund for Human Security (UNTFHS) publication 'Human Security in Theory and Practice' (2009). Although this publication also cites the seven pillars of human security as avenues of study the recurrent theme of the publication is the 'operationalization' of human security, and the focus on human security as an 'approach' rather than the demarcation of subject matter onto which this approach should be applied.

This proposition is not merely an afterthought to gloss over the failures of human security as subject matter or policy-practice. Already when the concept was first promoted by the UNDP in 1994 it was expressed as an attempt to "redefine humanity's development agenda" (UNDP, 1994) this meant changing the way development was practiced. This must be seen in light of the post-Cold War context where the UN sought to reconcile the two generations of human rights, namely, the first generation of civil and political rights and the second generation of economic and social rights. The two had previously been separated along the Cold War divides. In line with reconciliation the UNDP effort presented a conceptual triangle in which the rethinking of *development* through the concept of *human security* was seen as the "condition for *human rights* [of all generations] to be fulfilled" (Tadjbakhsh, 2014).

I want to make the case that this position of human security is that the concept of human security refers to a *discipline*. I define discipline as a practice about instruction on-, the shaping of-, and communication of- a field of knowledge, with certain norms and standards but with a, possibly, wide variety of approaches (Schanz, 2012). Thus, a discipline is not as much characterized by what is studied, as by how it is studied.

In the 1994 UNDP report and in the 2009 UN Trust Fund for Human Security publication 'Human Security in Theory and Practice' we find a range of norms that shape the

discipline of human security. First and foremost, there is the norm of protecting human rights and ascribing equal value to the economic, social, cultural, civil and political rights including the right to food. Further, it is non-discriminatory when it comes to gender, religion, race or ethnicity. It is **'multi-sectoral'** in the challenge-analysis and the planning, coordination, and evaluation of solutions with regards to what challenges and solutions are considered, moving beyond a mere concern with military or other violent threats; with regards to where challenges and solutions are considered, moving across and beyond institutional divides like state boundaries; and with regards to how challenges and solutions are considered, moving across academic boundaries. It is **'prevention-oriented'**; challenges are to be tackled at their root causes, in their earliest stages and be long term sustainable both socially and environmentally. Within human security there is a norm of working towards the two mutually reinforcing goals of **protection** and **empowerment**. Protection is a top-down perspective recognizing that threats are at times beyond the control of people and that national and international institutions and organizations then have a responsibility to protect these people, rather than focusing on e.g. protecting economic assets. Empowerment is a bottom-up focus on enabling people to develop resilience to difficult situations including preventive local-capacity building (UNDP, 1994 & UNTFHS, 2009). As a discipline, human security is also characteristic because of its normative nature. With an explicit norm of being transformative in improving the livelihood of others, human security resembles newer disciplines like development studies.

I contend that another aspect worth noting about human security as a discipline, is its methodological characteristics. These are different from traditional security studies in combining the quantitative, distanced methodology of this older field with a more integrative, consultative, qualitative methodology (Martin & Kostovicova, p. 298) usually found within the humanities in e.g. sociology and anthropology. The UNTFHS publication calls this **context-specific**, and **people-centered** (2009), emphasizing that the analyst must acknowledge differences across different settings, seek contextualized inclusive analyses and solutions that are based on local assets for coping. Further, she must be complimenting this with quantitative indicators. Thus, human security is at its methodological core interdisciplinary.

We find these norms and methodologies institutionalized since 1994 under the heading of human security in university courses and research projects at prestigious universities (Paris, 2001, p. 87; Krause, 2014, p. 81), in handbooks (UNTFHS, 2009), and in publications like the Human Security Report (Krause, 2014, p. 81). Despite this, I have not been able to find any use of the term "discipline" about human security. Thus, in a reversal of the old fairy-tale (Andersen, 1991) it seems that a lot of people are aware of the 'clothes' - the norms, methodologies and institutionalization - of human security but no one shouts that it is 'well-dressed' - that it is a discipline. It does however seem obvious once declared.

It is worth noting that human security as a discipline is not merely an academic practice confined to universities and scientific journals. As mentioned the concept was first promoted by the UNDP in 1994 in an attempt to "redefine humanity's development agenda" (UNDP, 1994) this meant changing the way development was practiced across 'humanity' including in academia, in ministries, NGO's and in international institutions.

The extent to which this change of practice has materialized at different levels is beyond the scope of this paper. Instead, I investigate the potential for change that this practice holds. Thus, I will turn again to Paris' critique that human security cannot guide the study of academics or the action of policy-makers, and look at how this may not be the case if we think of human security as a discipline.

3. THE PROBLEM OF DEFINITION

As mentioned, Paris argued that the scope of the subject matter of human security makes it impossible to prioritize goals for politicians and to discern what is to be studied by academics (Paris, 2001, p. 88). This resembles a point made by David A. Baldwin, who argues that "conceptual clarification logically precedes the search for the necessary conditions of security, because the identification of such conditions presupposes a concept of security" (Baldwin, 1997, p. 8). In other words, what constitutes security needs to be specified before we can promote security (Paris, 2001). I believe this clarification is necessary, but only problematic, when thinking about human security as a subject matter. I do not believe these problems are necessarily present if we think about human security as a discipline. With the disciplinary norm of participation in mind this conceptual clarification of security need to be done *in situ,* with the people affected. Inspired by Nils Bubandt we may say that the security concept of human security is *vernacular,* meaning site specific (Bubandt, 2005, p. 276). This is not working from a pre-established universal concept of human security as the *what*, the subject matter of human security, as Paris demands. Rather it is working from the notion that what constitutes security is always socially and discursively situated (Bubandt, 2005, p. 275). Thus, the analyst should allow for ideas about security that may not reflect "the dominant political agenda", which is why the approach has been called emancipatory (Tadjbakhsh, 2014, p. 46). Being attentive to this, the human security analyst investigating site-specific meanings of security can find help clarifying priorities and objects of study by asking seven questions put forth by Baldwin. (1) Security for whom (2) securing what (3) security from what (4) security to what degree (5) security at what time scale (6) security with which means (7) security at what costs (Baldwin, 1997). Answering these seven questions will bring forth a very clear concept of vernacular security, useful in the assessment of threats, and useful in guiding the action of potential policy-makers. This work is possible, despite being developed within a very broad discipline of human security.

In sum, academics, NGO's, businesses, governments and international institutions working within the discipline can work with a multitude of cases, but their work will not be random, or without useful conclusions. Instead, the work within this discipline, due to the norms and methods, will help policy-makers gain knowledge about vulnerable individuals and communities and will help them make qualified decisions to improve the vernacular human security of these individuals and communities. In the following, I present a case example to show the discipline in practice.

4. SITUATING HUMAN SECURITY

Before presenting the case, I want to note that the work done in the case was not done *explicitly* within the 'discipline' of human security. The term 'discipline' is not used for

the human security approach although as I have argued it lives up to the criteria for a discipline. Through my analysis of the case it will be clear that the work meets the norms and methodologies of the discipline of human security especially the standards of using a participatory, prevention-oriented, and human rights centred approach.

In Ghana, as in many other countries, large-scale land acquisition detrimental to local communities is a great challenge. This challenge is in part constituted by a national legal system within which community land is in fact state owned and power asymmetries between the affected communities and the foreign-based companies trying to acquire land (Akologo & Guri, 2016). The Centre of Indigenous Knowledge and Organizational Development (CIKOD) worked with the local community of Tanchara to deal with the challenge of large-scale land-acquisition. In 2000 the Ghanaian government granted an Australian gold mining company the right to prospect for gold within the community area without informing or involving the community in the decision (Guri Yangmaadome et al., 2012, p. 124).

The approach that CIKOD applied falls within the norms and methodologies characteristic of human security as a discipline. With regards to norms, CIKOD sought to protect the human rights of the villagers, namely the human rights of indigenous communities to free, prior, informed consent regarding changes that affect their means of subsistence, cultural practices and traditional sites (UNDRIP, 2008). It did so, in what is a good example of the norm of top-down **protection** based on the acknowledgement, that local people may not hold all the means to tackle threats. Protection was sought top-down as CIKOD mediated support to the community from the Ghanaian Commission on Human Rights And Administrative Justice (GCHRAJ) (Akologo & Guri, 2016). External protection was sought in acknowledgment that the government decision also needed to be fought through legal expertise which the local community did not hold. The GCHRAJ provided the protection of legal frameworks by mapping the rights of the community according to customary, national and international laws and conventions (Guri Yangmaadome et al., 2012, p. 127).

The work of CIKOD also followed the human security disciplinary norm of **empowerment** working bottom up to develop resilience to difficult situations among the affected. This was done in a **people-centered, context-specific** manner as CIKOD sought to "understand and work within the communities' own worldview" (Guri Yangmaadome et al., 2012, p. 122). Thus, the assessment of threats to the community; the assessment of the community assets that could be used; and the planning of how to reach a more secure future; was all made by the community itself. The tools for doing so were provided by CIKOD. Made by the community itself, the assessment of threats and strategies for action was **multi-sectoral** including aspects from arenas, that are sometimes separated by disciplinary standards such as the threat to community coherence, the need for political attention, and the potential health and economic threat of prospected mining (Guri Yangmaadome et al., 2012). In other words, a vernacular, emancipatory concept of security and security-threats was developed.

Additionally, the work done by CIKOD was **prevention-oriented.** Root-causes of the challenges were taken on at the early stages before mining was underway and this gave enough

time to start processes towards socially and environmentally sustainable long-term solutions, based on vision-statements of where the community wanted to be 10 years ahead (Akologo & Guri, 2016). There is a clear testimony to the empowerment of the community through increased awareness of local assets, and through the awareness of being protected by national and international legal frameworks in the processes and changes adopted by the community. To name a few: since 2004 biannual meetings have been organized to review activities and present projects to external actors on how to secure the community livelihood and its rights. The community has improved environmental sustainability of the sacred groves by implementing organic, zero tillage land-use with traditional crop varieties. In turn, this has strengthened the community authorities that depend on these groves. The women of the community are now better organized and increasingly do farming as an economic activity which increases their voice in the community. This is an example that the human security approach is not merely conserving indigenous communities, but is transformative while respecting community practices (Guri Yangmaadome et al., 2012, p. 123). The perhaps greatest example of community strengthening is the fact that local workshops on the impact of gold-mining lead to regional forums in which a joint-statement of strategies were made to deal with the problems associated with goldmining. At these forums goldmining company representatives also participated and for the first time engaged with the local communities (Guri Yangmaadome et al., 2012, p. 126). At the forum, the government and the mining company was informed about how to engage with the community in order to ensure free, prior and informed consent, this included the statement that the community had the right to say no to any dispossession. In the end goldmining was postponed indefinitely in the area and the community reached its vernacular goals for security (Akologo & Guri, 2016, p. 39).

This case shows that within the discipline of human security, it is indeed possible to narrow down, apply and prioritize ideas of human security. We see that in this concrete case, we can easily answer Baldwins seven questions (1) the Tanchara community consisting of 3800 members were the ones for whom security was at stake, what needed to be secured (2) was their land on which they heavily depended for their livelihood and which held great spiritual significance for the village as well. (3) The community access to land needed to be secured from the encroachment of mining companies that were active in the region. (4) This needed to be done to the degree that access to the land was not lost at all and natural resources were not degraded (5) in the following 10 years. (6 & 7) This was to be ensured using the resources within the community; through regional forums and via the existing community, national and international legal frameworks.

If we accept this as an example of work within human security as a discipline then this case shows that by following the norms and methodologies of the discipline, fruitful work can be done to tackle environmental and natural resource challenges. Further, nothing in the case indicates that the success of the human security practice was conditioned by the fact that this was a natural resource challenge. The case analysis also shows the clear advantages of considering human security as a discipline rather than a subject matter or defined by the use of policy-makers. As a discipline, the subject matter of human security was not predetermined in the Tanchara case, rather it was context-specific and this guaranteed the relevance of the work done. Also, the political efforts were not defined by

an existing political human security agenda, directly opposite the political efforts were guided by the work done according to the norms and standards of case analysis within the human security discipline. The case shows that strategic priorities were made both in the analysis of the challenges, and in guiding the relevant actors in taking action. In this quite small-scale case, the actors were the affected community. But CIKOD has also used the case to provide guidance to policy-makers at the national level on how to improve the process of reaching free, prior, informed consent of local communities in cases of large-scale land deals.

In the following, I discuss how the insights from this case analysis apply in general to the analysis and policy-guidance within the human security discipline, when considering the wider scope of challenges to human rights, human dignity and human well-being.

5. HUMAN SECURITY CHALLENGES

The variety of human security challenges is unfathomable. The amount of people affected by these challenges range from a single individual as the case of a lone person's isolated house catching fire from a lightning to potentially everybody on the planet as the case may be with global warming in its totality and the connected avalanche of negative snowballing side-effects that are still being realized. Some issues are confined within local, national or regional political boundaries, others are constituted partially by these boundaries themselves as is the case with trans-boundary crime (see e.g. Van Schendel, 2005), and yet others simply override any such boundary. Some are confined to a short span of time, others have effects that potentially outlast the next many generations to come. I will deal with this great span of challenges and the potential of the human security discipline in two sections. First by considering challenges that are less than global. Secondly, considering global climate change in its totality as a potential threat to the human life form and discussing the great methodological challenges that global issues in general present to the discipline of human security. I will argue that despite these challenges human security analysis may be an important life rope away from climate disaster and other global challenges to human well-being.

6. HUMAN SECURITY AND LESS THAN GLOBAL CHALLENGES

The discipline of human security can contribute to many of the challenges to human well-being and upholding of human rights if these challenges are narrowed down to concrete instances e.g. the problem of smog in Beijing or the dangers involved in irregular migration from Cheran in Southern Mexico. The human security analyst will be able to engage with more localized challenges of protection, adaptation, and prevention: protection from e.g. disease outbreaks or ethnic violence; adapting livelihood practices to e.g. mitigate the effects of changing weather patterns by e.g. changing the type of crop grown; preventing further contribution to the deterioration of livelihoods by altering key practices of e.g. decision-making, consumption, production or interaction. In order to meet the standard of promoting sustainable solutions, these three elements should all be included in the analysis and policy-guidance. Across the spectrum challenges, the case analysed earlier is instructive, in deciding the subject matter on which the discipline holds

the greatest potential. The participatory approach demands an inclusion of the affected parties in the assessment of what constitutes a threat, and what constitutes security. If this is possible, then human security as a discipline will benefit from not being constrained to look only within certain sectors like the political or the military. Rather the human security analysts can follow linkages seamlessly across sectors as they are developed by study subjects. This context-specific, people-centred, multi-sector perspective aimed at empowerment avoids proposing policies merely because they fit institutional frameworks but insists on a bottom-up approach, rather than one-size-fits-all solutions. Human security with its emphasis on both empowerment and protection is theoretically useful in tackling any challenge to the upholding of human rights, well-being and dignity. But it is worth noting, that as protection relies on the 'goodwill' of the relevant external protectors, this may be hard to attain, and poses a difficulty within the discipline. An example of this is the prospecting of new coal plants in China by the Chinese government, despite people protesting the lethal smog of Northern China that annually leads to one million premature deaths (Carney, 2017). In this case the protector is clearly not taking the needed responsibility. Despite this difficulty, even in cases where the immediately relevant institutions do not adhere to their responsibility to protect vulnerable people threatened by things outside their control, the work within human security as a discipline increase the chance that protection will manifest. It does so because it empowers the people affected and gives these people a voice via the human security analysis. The policy-guideline that arise from this analysis makes it clearer what protective action is needed and thus makes it easier for the relevant external actors to engage in. This lesson can also be drawn from the case example from Ghana. Here the government initially failed to meet its responsibility to protect the local community rights, as prospection rights were given to the foreign company. Only later, after the empowerment of the local community, is the government starting to take responsibility to protect. The government has also praised the involved organizations for emphasising the government responsibility and drawing up the needed action (Danso & Donkor, 2017). Further, the mining company after the empowerment has delayed action in what can be interpreted as an acknowledgement of community rights and of the company's role as the principal agent of threat.

7. HUMAN SECURITY AND GLOBAL CHALLENGES

A range of threats to humans are of a nature that cannot meaningfully be called merely transnational or regional but are rather international or global. Among them are the proliferation of nuclear technology, the development of multiresistant diseases, global financial downturns and global climate change. Other threats in this category do not necessarily affect people worldwide, but need strong global decision-making organs to protect the rights, well-being and dignity of specific populations. These threats include the conflict in Syria and dangers involved in international irregular migration. To analyse the potential of human security in dealing with these global challenges I focus on global climate change, and draw wider lessons from this.

The threat of global climate change is imminent. By the most negative estimates, global carbon emissions have already exceeded the level below which we could expect that the

environment would not be so significantly altered as to render our societies unsafe (Gasper, 2013, p. 63f). The level of disruption is however relative to the continued emissions, and so preventive action is still meaningful.

Taking on global challenges, human security as a discipline faces two perhaps insurmountable methodological challenges. The first challenge is that at a global level the analyst cannot realistically hope to work in a 'people-centered' fashion. Establishing a vernacular concept of security is close to meaningless when considering the enormous differences in the assessment of what constitutes threats and what constitutes security, when discussing global challenges in each their, often interrelated, totality. As Naomi Klein has described in the article "Disaster Capitalism", some people are making a living selling security products in high-threat situations (Klein, 2007). These people, along with all the people and states whose immediate prosperity depends on disaster propelling businesses like fossil fuels, offensive weaponry, human trafficking or high-risk financial transactions are not likely to express threat assessments that can be easily conflated with those who are the most at risk from global challenges, those who depend the most on disaster preventive efforts, or those who know the most about implications of these global challenges. In that case, asking Baldwins seven questions will only provide answers that serve particular interests, and not the interest of the whole affected populace. In other words, within human security there is no meaningful analytical scale at which the totality of issues like global climate change can be gauged, no scale at which the 'world society' can be gauged as a coherent whole. Thus, as a proxy, the human security analyst would have to make do with an institution that could speak on behalf of the world community on these issues. But as Ulrich Beck has pointed out in his 2009 book 'World at Risk', international climate politics are still the politics of nation-states, although perhaps nation-states with a cosmopolitan outlook influenced by a range of international organizations (Beck, 2009, p. 103f). This is so despite a myriad of actors coming together in collaboration to counter global warming. I would argue that Beck's analysis is also valid for the other global threats, although in some instances with an even smaller degree of a cosmopolitanism because the negative consequences of other global issues, like the conflict in Syria are more unevenly distributed than the case is for climate change. In any case supranational institutions of cooperation and consensus building that effectively can deal with global threats to human rights, well-being and dignity are yet to emerge (Beck, 2009, p. 92). This makes the people-centred and vernacular approach within human security impossible to follow even when 'the people' are substituted by a proxy institution.

If Ulrich Beck is right in his analysis, there is also a second methodological challenge for human security that applies to all the global scale issues: Without the supranational institutions that Beck talk of, there is no proper organ that holds the responsibility to protect the global population, and no single nation can lift such challenges on their own. Thus, human security can only hope to empower since there is no one to call forth to protect. This becomes especially problematic regarding the specific threat of global climate change with due to its inbuilt mechanism of negative feedback loops and its spill over consequences into other challenges like poverty, irregular migration, and widespread conflicts like the one in Syria. As the forecasts for climate change steadily grow darker,

with the 2-degrees goal from the Paris climate accords still more unlikely to be met (Wallace-Wells, 2017), the people of the planet can increasingly be said to be at a threat beyond their control. As stated, in these contexts human security cannot call upon a global guarantor of democratic oversight, but can only seek to empower at non-global levels

Empowerment in itself is not insignificant. Des Gasper, has argued that human security holds a transformative potential for the needed global climate action. According to Gasper such action is premised on three 'value transitions':

"from a preoccupation with the acquisition and consumption of commodities towards a broader and deeper picture of what gives quality of life; from an overwhelming individualism towards human solidarity, based on respect for all individuals; and from an attitude of mastery and domination of nature towards an attitude of stewardship for 'Mother Earth'" (Gasper, 2013, p. 71)

Gasper believes that such transitions, although far from being realized, are possible because the 'language' of human security connects to 'human subjectivity' and the 'texture of everyday life' and thus holds an 'explanatory force and motivational power' that is not present in other 'languages' like economic development or human rights (Gasper, 2013, p. 68f). Gaspers claim is that the empowerment of the human security method, giving a voice to those who are the most affected by global CO2 emissions, can create the needed subjective connectivity to the greatest emitters that trigger the needed value transition among these emitters. This may lead to protective action, although one that is uncoordinated from above. Combined with the small-scale contributions to protection, adaptation and prevention made by the individual human security projects, this contribution through storytelling may be an important life rope out of climate disaster.

Gaspers point about the power of the human security language is not only relevant regarding climate change. It resonates Johan Galtung's points about international efforts towards a more peaceful society. He argues that the lack of a democratic global guarantor of peace can only be compensated for by working at all levels to increase democratic governance, human rights and fairer trade deals:

> "The hypothesis would be that once the system has attained a certain level of diversity, then diversity will, through symbiosis, generate more diversity. Diversity will feed on itself, so to speak. The result will be an increasingly resilient system, able to withstand injury from within and without" (Galtung, 1996)

Thus, a circular logic is at play in which the only way to move forward is to move forward, the increasing benefits of the small steps at local promotion of human rights and democratic governance will increase the ability to take further steps toward peaceful global governance (Galtung 1996). Based on my presentation of the human security as a discipline and my case-analysis of its merits I argue that human security is a practice that holds the potential to increase the length and stability of these steps both small and large.

8. CONCLUSION

I've made the case that a lot of the criticisms that are raised against human security, do not apply if we think of human security as a discipline institutionalized in university courses, research projects and handbooks, and having certain norms and standards useful in the work of NGO's, businesses, governments and international institutions. Instead of working from a pre-established concept of security, the disciplinary approach is about defining threats and what constitutes security in participation with the people studied.

As a discipline, human security seeks to empower the people at threat. Based on a case analysis I showed an example of how this has been done. A vernacular definition of threats and what constituted security was established by the affected community. By letting these people identify their own assets and how they could be used, these people were given a voice and were enabled to better use their own assets. The case analysis also showed how the human security discipline can contribute to guiding the action of those who have a responsibility to protect vulnerable people. This protective aspect is enhanced by giving a voice to those who need protection, and by drawing up a clear path of action that the protectors can follow to meet their responsibility.

The lessons drawn from the case, can be used in analysis and policy guidance for a broad spectrum of challenges related to all the pillars of human security. The criteria for this is that the concrete cases have identifiable people at threat who can voice their vernacular ideas of security and its threats. This is the primary measure for the applicability of the human security methodology. I have argued that in these cases the methodology would contribute to solutions to all challenges to security.

Finally, I pointed out that global threats to human rights, human well-being and human dignity, poses methodological challenges to human security as a discipline as no vernacular concept of security or of the threats can be established neither directly nor through proxy representative organs. Despite this, the smaller scale case-work within the discipline contributes to the mitigation of such global challenges in two ways. By facilitating protection, adaptation, and prevention in local settings, meaning that this setting becomes more resilient and contribute less to threatening practices such as carbon emissions, poor governance, economic exploitation and offensive arms trade. And secondly, by mediating stories of threat and insecurity that facilitate a subjective connectivity between the most affected and the most contributing. Inspired by Gasper and Galtung, I argued that this could provoke the needed value change among the greatest instigators of global issues. Complimenting Galtung I further argued that the discipline of human security can facilitate the small and diverse steps towards a more democratic global order that promotes human rights, human dignity and human well-being.

9. BIBLIOGRAPHY

Akologo, S. Z. & Guri, B. Y. (2016). *Unmasking Land Grabbing in Ghana.* Accra: Caritas-Ghana. Pp. 32-43

Andersen, H.C. (1991). 'Keiserens nye Klæder' in Andersen, H.C. *Samlede Eventyr og Historier,* 7th edt., pp. 74-76, Odense: Hans Reitzels Forlag

Baldwin, D. A. (1997). The Concept of Security. *Review of International Studies*, *23*(1), 2-26

Beck, U. (2009). *World at Risk.* Cambridge: Polity Press

Bubandt, N. (2005). Vernacular Security: The Politics of Feeling Safe in Global, National and Local Worlds. *Security Dialogue*, *36*(3), 275-296

Buzan, B., Wæver, O. & de Wilde, J. (1998) *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers

Carney, M. (2017). China's air pollution crisis shows no sign of ending as nation fails to lower coal use. Retrieved from: http://www.abc.net.au/news/2017-01-08/chinese-air-pollution-crisis-caused-by-ongoing-coal-use/8168702

Chandler, D. (2008). Human Security: The Dog That Didn't Bark. *Security Dialogue, 39*(4), 427–438

Danso, J. & Donkor, E. K. (2017). Caritas Ghana holds two-day dialogue on Land Grabbing. Retrieved from: http://www.ghananewsagency.org/social/caritas-ghana-holds-two-day-dialogue-on-land-grabbing-126608

Galtung, J. (1996). Peace By Peaceful Means - Peace and Conflict, Development and Civilization, London: Sage Publications

Gasper, D. (2013) Climate Change and the Language of Human Security. *Ethics, Policy & Environment, 16*(1), 56-78

Guri Yangmaadome, B., Banuoko F., Daniel, K. Derbile, E., Hiemstra, W. and Verschuuren, B. (2012).'Sacred groves versus gold mines: biocultural community protocols in Ghana' in A. Holly, N. Kenton, and A. Milligan (eds) *Biodiversity and culture: exploring community protocols, rights and consent*, pp. 121-130, London: The International Institute for Environment and Development

Klein, N. (2007). October) Disaster Capitalism - The New Economy of Catastrophe. *Harpers Magazine*, 47-58

Krause, K. (2014). 'Critical Perspectives on Human Security' in M. Martin and T. Owen (eds) *Routledge Handbook of Human Security*, pp. 297-307, London: Routledge

Martin, M. and Kostovicova. D. (2014). 'From Concept To Method: The Challenge of a Human Security Methodology' in M. Martin and T. Owen (eds) *Routledge Handbook of Human Security*, pp. 297-307, London: Routledge

Paris, R. (2001). Human Security: Paradigm Shift or Hot Air? *International Security, 26*(2), 87-102

Schanz, H. (2012). Hvorfor er idéhistorie vigtig?. Retrieved from: http://baggrund.com/idehistorie/

Tadjbakhsh, S. (2014). 'In Defense of The Broad View of Human Security' in M. Martin and T. Owen (eds) *Routledge Handbook of Human Security*, pp. 43-57, London: Routledge

UNDP (1994) *Human Development Report 1994*. New York: Oxford University Press. Pp. 22-40

UNDRIP (2008). United Nations Declaration on the Rights of Indigenous. Retrieved from: http://www.un.org/esa/socdev/unpfii/documents/DRIPS_en.pdf

UNTFHS (2009). Human Security In Theory And Practice. Retrieved from: http://www.un.org/humansecurity/sites/www.un.org.humansecurity/files/human_security_in_theory_and_practice_english.pdf

Van Schendel, W. (2005). 'Spaces of engagement: How borderlands, illicit flows, and territorial states interlock'. In W. Van Schendel and I. Abrahams (eds.) *Illicit flows and criminal things: States, borders, and the other side of globalization,* pp. 38-68. Bloomington and Indianapolis: Indiana University Press.

Wallace-Wells, D. (2017). The Uninhabitable Earth. Retrieved from: http://nymag.com/daily/intelligencer/2017/07/climate-change-earth-too-hot-for-humans.html

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

341.231.14(082)
351.86:005.5991.6(082)

INTERNATIONAL Conference on Human Security (4 ; 2018 ; Beograd)
4th International Conference on Human Security : the Proceedings of Human Security and New Technologies / editors Svetlana Stanarević, Goran J. Mandić, Ljubinka Katić. – Belgrade : Faculty of Security Studies, Human Research Center, 2018 (Beograd : Čigoja štampa). – 263 str. : graf. prikazi. ; 24 cm

Tiraž 200. – Str. 9-10: Editorial / Svetlana Stanarević, Goran J. Mandić, Ljubinka Katić. – Napomene i bibliografske reference uz svaki rad. – Bibliografija uz svaki rad.

ISBN 978-86-80144-30-6

a) Права човека – Зборници b) Људска безбедност – Зборници c) Безбедносни сектор – Технолошки развој – Зборници
COBISS.SR-ID 269449740