

INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

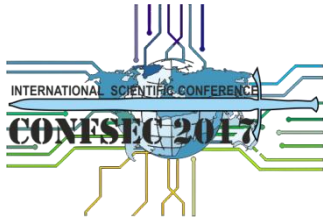
ISSN: (PRINT) 2535-0668

ISSN: (ONLINE) 2535-082X

YEAR II ISSUE 3/2018



PUBLISHER SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING - INDUSTRY 4.0
BULGARIA



INTERNATIONAL SCIENTIFIC JOURNAL SECURITY & FUTURE

PUBLISHER:

**SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING
INDUSTRY-4.0**

108, Rakovski Str., 1000 Sofia, Bulgaria
tel. (+359 2) 987 72 90, tel./fax (+359 2) 986 22 40,
office@stumejournals.com,
www.stumejournals.com

ISSN (PRINT) 2535-0668

ISSN (Online) 2535-082X

YEAR II, ISSUE 3 / 2018

EDITORIAL BOARD

CHIEF EDITOR

Prof. Nikolay Radulov
New Bulgarian University, Sofia, BG

Members:

Alexander Baranov, Prof.	Higher School of Economics	RU
Alexander Kurbatski, Prof.	Belarusian State University	BY
Alexander Troyanskiy, Assoc. Prof.	Odessa State Polytechnic University	UA
Andrzej Misiuk, Prof.	Warsaw University	PL
Ariana Bejleri, Assoc. Prof.	Polytechnic University of Tirana	AL
Galina Zhavoronkova, Prof.	National Aviation University, Kyiv	UA
Gudrun Biffel, Prof.	Donau University	AT
Dimitar Dimitrov, Prof.	Shumen University	BG
Evgeni Manev, Prof.	University of Library Studies and Information Technologies	BG
Hanáček Petr, Assoc. Prof.	Technical University of Brno	CZ
Iliyan Lilov, Prof., Col.	“Vasil Levski” National Military University	BG
Jaroslav Tureček, Assoc. Prof., Col.	Police Academy of the Czech Republic	CZ
Josef Reitšpís, Prof.	The University of Security Management in Kosice	SK
Juris Borzovs, Prof.	University of Latvia	LV
Kristiina Hakk, Assoc. Prof.	Estonian Information Technology College	EE
Kiril Stoychev, Prof.	Institute of Metal Science – BAS, Sofia	BG
Lev Elisov, Prof.	Moscow State Technical University of Civil Aviation	RU
Milan Popović, Prof.	University of Montenegro	ME
Muhammed Ali Aydin, Assoc. Prof.	Istanbul University	TR
Nebojša Bojanić, Assoc. Prof.	University of Sarajevo	BA
Nikifor Stefanof, Prof.	University of Security and Economics - Plovdiv	BG
Ninoslav Marina, Prof.	University of Information Science and Technology - Ohrid	MK
Nurgali Zaurbekov, Prof.	Almaty Technological University	KZ
Oliver Bacanovic, Prof.	University "St. Kliment Ohridski" - Bitola	MK
Ognyan Ivanov, Assoc. Prof.	Institute of Solid State Physics, BAS - Sofia	BG
Piotr Majer, Prof.	University of Warmia and Mazury	PL
Razvan Rughinis, Prof.	Polytechnical University of Bucharest	RO
Siniša Tatalović, Prof.	University of Zagreb	HR
Stoyan Denchev, Prof.	University of Library Studies and Information Technologies	BG
Tatyana Ejevskay, Prof.	Transbaikal State University	RU
Valentin Todorov, Assoc. Prof.	Varna Free University „Chernorizets Hrabar“	BG
Vesselin Demirev, Assoc. Prof.	Technical University Sofia	BG
Vladimir Zakhmatov, Prof.	Academy of Ecological Safety, Kiev	UA
Zelimir Kesetovic, Prof.	University of Belgrade	RS

CONTENTS

THEORETICAL FOUNDATIONS OF SECURITY

INTERNET OF THE THINGS. SECURITY 4.0

Prof. Radulov N., PhD 99

REMOTELY CONTROLLED NON-LETHAL WEAPON SYSTEMS IN THE CONTEXT OF LAW ENFORCEMENT

Assist.-Prof. Dr. Eng. Tumbarska A. 102

NATIONAL AND INTERNATIONAL SECURITY

MIGRATION, TERRORISM AND POSSIBLE ARMED CONFLICTS IN THE WESTERN BALKANS

Prof. dr. Saša Mijalković. PhD, Ass. Prof. Dr. Dragana Cvorovic. PhD 106

THE IMPACT OF THE SECURITY SITUATION ON TOURISM IN THE COUNTRIES OF THE FORMER YUGOSLAVIA

Ing. Iveta Hamarneh, Ph.D., Mgr. Petr Jeřábek 111

THE ROLE OF HUMAN RESOURCES DEPARTMENTS IN CREATING THE SECURITY SYSTEM – THE OUTLINE OF THE PROBLEM

M. Dąbrowska-Świder. Msc. 116

ANALYSIS OF THE SYRIAN CRISIS AND ITS ROLE IN INTERNATIONAL RELATIONS

Chief Assistant Professor PhD eng. Dolchinkov N. T. 119

NUCLEAR WEAPONS IN RUSSIA

Chief Assistant Professor PhD eng. Dolchinkov N. T. 123

ANALYSIS OF THE RELATIONSHIP BETWEEN ENERGY DEPENDENCE AND NATIONAL SECURITY

Chief. Assist. Prof. N. I. Padarev PhD 127

BEST PRACTICES IN CBRN WASTE MANAGEMENT IN MILITARY OPERATIONS

Chief. Assist. Prof. Nikolay I. Padarev PhD 130

INFORMATION SECURITY

INFORMATION SECURITY AWARENESS IN CONTEMPORARY ORGANIZATIONS – CHALLENGES AND SOLUTIONS

Assoc. Prof. Popescu D. PhD 134

DEVELOPMENT AND IMPLEMENTATION A PLATFORM TO SECURE CYBER INFRASTRUCTURE AND OPERATION

PhD. Eng. Mircheska S. 138

TECHNICAL FACILITIES FOR ENSURING SECURITY

MATERIAL MODEL PARAMETERS IDENTIFICATION OF BLAST ENVIRONMENT

M.Sc. Dubec B., M.Sc. Stonis P. 142

FAST PROTOTYPING IN THE MANUFACTURING OF COMPLEX ARMAMENT PARTS

Assoc. Prof. Ing. Ganev V. PhD., M.Sc. Ing. Dimitrova Ya., M.Sc. Ing. Antonov S. 146

EXPERIMENTAL DEVELOPMENT OF A SMART FUZE DETONATION ALGORITHM

Cad. Dimitrov M., Assoc. Prof. Ing. Ganev V. PhD., M.Sc. Ing. Dimitrova Ya. 149

INTERNET OF THE THINGS. SECURITY 4.0

Prof. Radulov N., PhD, New Bulgarian University, Sofia, Bulgaria
 nradulov@nbu.bg

Abstract: *The Fourth Industrial Revolution implies a total change in our way of life. To be adequate to the new security threats stemming from high technology, we need to analyze and evaluate them from the point of view of people's security.*

KEYWORDS: SECURITY, IOT, SMART SENSORS, INTELLIGENCE AND COUNTERINTELLIGENCE

1. Introduction

1.1. Security and industrial revolutions

The development of public order and security systems undoubtedly follows the development of the economy and social relations. Technology development often occurs first in military organizations and those of security and later they appear as products for civilian use. The crime is directed at the illegal acquisition of goods by organized and disorganized criminal groups. With the development of industry, the wealth - capital, movable and immovable property, storage in banks, also increase and all of these are the object of interest and desire for illicit acquisition by the criminal world. Since it is dissolved in the normal world, it is also subject to development and uses the benefits of the technical progress. Criminals are becoming more and more creative, educated, pretentious and greedy. Well-educated and well-equipped criminals are developing ever more innovative ways of criminal enrichment. This causes normal people to demand from the governing people adequate protection due to the fact of citizenship and paying taxes. Much of the criminal interests are focused on big capital. This makes the interests of poor and rich converge to higher security synchronous. Therefore, resources are allocated, specialists are trained, and research and development is being carried out to tackle crime and, of course, espionage. There is no way for innovative industrial development without resource-intensive development. From the point of view of opposing countries, intelligence should be a productive force that, for example, spending a total of EUR 100 million, gives its producers an advantage worth billions.

There is no technical breakthrough without impact on the need of security – rail transport, in addition to its economic importance, allows for easy transport of people over long distances, whether military formations, criminals or police forces; construction of aircraft, photography, beyond their exceptional economic significance, have great value since their emergence for intelligence, counterintelligence, military and special operations. Cybercrime, cyber-intelligence, cyber-security are interconnected industrial and social phenomena demonstrating the possibility of modern crimes and the creation of modern products for civil and national security.

A stage of development of the security system corresponds to each stage of industrial development. So when we consider the security in the mean of Industry 4.0, we take into account innovative security paradigms, technologies and techniques that match high technology. We can unite them under the common name Security 4.0.

1.2. Forth industrial revolution

In practice, this is predictable with a high probability near future, which is already at the start. Massive cyber-physical systems in manufacturing, serving human needs will develop. The changes will affect the most widely all aspects of life. There are, of course, risks - increased instability and the possibility of collapse of the global system due to a change in basic paradigms of coexistence. The technologies that are already being developed and will cover everything are: Big Data; the Internet of Things (IoT); virtual, complementary and mixed reality; 3D printing; printed electronics; quantum computing; blockchain technology; artificial intelligence; neurotechnologies; new materials; space and geotechnology.

Security 4.0 is unthinkable without huge masses of data accumulated using millions of sensors and devices connected to each other, end devices in a modern internet environment that we call the Internet of Things.

2.0. Results and discussion

2.1. Internet of Things (IoT)

The Internet of Things (IoT), also known as the Internet of Objects (from Russian: Интернет вещей), is a concept of a computer network of physical objects (devices, vehicles, buildings and other objects) having built-in electronic devices to interact with each other or with the external environment. This concept considers the organization of such networks as a phenomenon capable of rebuilding economic and social processes so as to exclude the need of human participation in some of the actions and operations. IoT consists of networked intellectual sensors collecting information and transmitting it over the Internet to other devices or people for further use. IoT will increase people's interaction with machines, and economic relationships between machines will grow faster than between people. In the next 10 years, over 10 billion devices will be added to IoT, and their industrial use could bring the world economy up to \$ 14 trillion until 2030. Security systems use a wide range of sensors – volume sensors, motion sensors, infrared, noise, fire, etc., resulting in increased security, rapid response to alerts, and overall improved security for citizens. The presence of security alarm systems (SAS) based on sensor systems, which is usually disclosed, has an additional prophylactic effect against criminal offenses. So far, much of the SAS's networks are connected to private security companies, but there are innovated internet-based systems, hidden video recordings, cloud-protected information cameras, use of reaction scenarios based on modern software. In recent years, security systems have been built with hundreds of thousands of sensors and video cameras to ensure the security of important events, communicating between each other and with the network management, reacting immediately through artificial intellect-aided computer systems – the Sochi Olympics, the football championship in Moscow.

The exponential distribution of sensors and devices and the traffic generated by them will lead to complications in interstate transmission of data, including confidentiality issues, property ownership, copyright, accessibility, etc. One of the important tasks of Industry 4.0 will be the creation of regulatory measures with regard to global information flows in the Internet of Things.

IoT is much more than intellectual devices connected to the Internet and services on their basis. The real value lies in the fact that it allows data collection, analyzes and manages them, finds unexpected correlations and opportunities for action, anticipating destructive changes or crises. For years in the security sector, there has been talk about insufficient information, the lack of information sensors allowing for truly interactive crime maps and for immediate counter-scenarios.

The use of real-time data-processing sensors will likely help to create a developing economy with positive results thanks to the optimization and stimulation of consumer and citizen behavior. This means that IoT can serve as a tool for solving systemic problems such as energy efficiency, traffic management, and environmental pollution. In fact, it is a tool to reach security either in the broad or in the narrow sense of the term.

Serious concern, however, is the impact of IoT at the level of labor and working habits, joining IoT with AI and robots, reducing the demand for routine and manual work for low-skilled workers. But the main risks of IoT systems are most often considered cybersecurity threats, related to low security of devices, lack of standards and legal frameworks for interstate data transfers. This poses new challenges for both the society as a whole and the individual qualification of the individual – the devices will displace the person from the low-skilled, routine work but will unleash the potential for hundreds of activities related to creativity, imagination, erudition, analytical and mental activity. However, this may be a positive trend if the system of life and education provides opportunities and stimulates conscious and uninterrupted training and retraining of people, in line with the exponential development of technology. In the field of security, this will be even more visible and necessary. Actually, the confrontation between crime and the systems of human rights protection will be an opposition between the high technology and the experts using them as a tool in the criminal and security services. Security and public order services are required to be proactive, and this means highly specialized training, a continuous cycle of training, practice and retraining, a special innovative and uncompromising system for selection, recruitment and employee development.

2.2. *Special services and IoT. Security and IoT*

There is a clear contradiction between the ability of the special services to use innovations and the preservation of individual information, personal data, the confidentiality of every person's life. What is certain is that special services need access to information, but it must be secured against abuse, legally framed and technologically secure. The danger of using the information collected by millions of sensors for the needs of criminal organizations and criminal activities is enormous, so safety must be ensured by the delegated bodies.

The revolution in data collection, which is already happening online, is ready to be repeated in the physical world thanks to the Internet of Things. The idea for IoT is that everyday objects (things) secured with sensitive sensors can now collect and transfer data over a wireless network. The variety of items that can be connected through internet is almost endless: from pavement slabs and concrete to walls to our shoes and clothes, and even toothbrushes. All of them get connected and in the near future they will start adding information to the cloud.

The potential use of IoT for surveillance is recognized by the intelligence services. Former US intelligence chief James Clapper said last year to the Guardian that the agencies would probably use the Internet of Things to "[identify, monitor, track, locate, and access the network or identification data of user]". This approach shows that the intelligence community takes into account this technology and the new extraordinary capabilities to collect and analyze data. All of this must undoubtedly change the current paradigm of intelligence and create a new one.

2.3. *The emergence of a new security paradigm*

In most special services, there are several paradigms that define the meaning and content of intelligence: radio-electronic intelligence; visual intelligence; intelligence by measuring signature and parameter of goals and objects; agency intelligence; intelligence analysis based on public sources and geospatial intelligence.

The emergence of the Internet of Things shows that intelligence services take into consideration, this new technology, new data collection and analysis potential. The introduction of the Internet of Things generates a new paradigm: temporal intelligence (TII). It is not a narrow methodology for collecting intelligence data that focuses on certain sources but a comprehensive approach to collecting and analyzing data. It implies that most people and infrastructures will be monitored and that some of the data can be collected, analyzed and stored, generated for intelligence and new ones will be created.

Such an approach allows us to explore new hypotheses on old data that have been collected and stored without any real purpose. In the past, intelligence services have collected data selectively due to the difficulties of the process and the high cost of storing a large amount of information. But now, when based on the connected sensors, the presence of devices that transmit data almost non-stop, the intelligence agencies only need to take care of data collection and storage. As a result, they have a powerful tool at their disposal, because if there are any changes, analysts can actually apply the "backward time" to the saved data to see what's behind these events. The final time intelligence platform, consisting of what's happening everywhere, allows the event to be expanded, stopped, rewind (like a video) – with a full comment on the physical and mental health of each person, details for which are obtained using portable devices.

There are two major technological issues related to temporal intelligence.

The first problem is the accumulation of data. Applying TII means that we need to store large amounts of data for later consideration. By 2019, the Internet of Things is expected to collect more than 500 zettabytes data – that's 500 trillion gigabytes. Irrespective of the huge volume, the resulting data can be divided into the following main groups: sound recordings, location and activity monitoring, and images taken from connected surveillance cameras. In addition, the mass storage capabilities over the last few decades have expanded and there are no limits to improving and increasing the volume.

The second technological issue is to filter a huge amount of data to find the necessary information. This problem is resolved by the rapid improvement of artificial intelligence, which, with the help of a neural network, acquires the ability to recognize faces, subjects, and even abstract concepts in pictures and videos.

Should security agencies have all the capabilities of TII? In fact, secret services already have such powers today and collect the most available information. The Internet of Things will only increase the amount of collected and processed information. Citizens are, of course, seriously concerned about the growing ability of governments to control mass people in general. Special services should not ignore these fears; they should try to reduce them. For example, authorities can use artificial intellect to identify potential terrorists without the need for a particular employee to personally view the data of millions of citizens. These institutions could provide some of the algorithms for public control. Such transparency will help to prevent misuse of information as well as to detect errors.

Special services are often accused of not being prepared to solve future problems. Once the trends of Internet of things have been identified and a new intelligence paradigm has been created, these institutions now have the opportunity to act proactively. This, of course, is the most important advantage they can have against their opponents. And this is one of the compromises citizens of the democratic states will have to accept.

2.4. *Crime and Internet of Things*

Internet of Things has some particularities according to Marc Goodman¹, namely:

By plugging in new and new devices, people forget that everything accessible through the network sooner or later can be penetrated. No existing security technologies and agencies are enough to counteract the growing threat. The Internet evolves at times faster than the means to protect it.

¹ The book "Crimes of the Future" is one of the popular science bestselling books in the US in 2015. In it, a former Los Angeles police officer with experience in Interpol, the CIA and Secret Service, advising the police services of dozens of nations, reflects on the subject of unprecedented crimes that await us in the 21st century.

The crimes become so high-tech that they astound law enforcement experts. Particularly serious threats result from the realization of the "Internet of Things" concept, within which more and more devices get access to the network. Medical equipment and power stations, implanted devices and security systems – the easier and more convenient to use, the easier it is for criminals to access.

4.0. Conclusion

It is necessary to initiate a new project to bring together the best scientists and researchers, universities, governmental and non-governmental organizations, corporations, civil society. Security experts, entrepreneurs, politicians, lawyers, and military have to be involved – in order to create comprehensive, overall protection, including safer equipment, operating systems and software as a minimum on nationwide, and even better on a global level.

In this connection, some neuralgic points can be defined, allowing the study, analysis and influence of the values embodied in the technologies that guarantee security.

Educational programs – specialists using and developing new security technologies are particular specialists, they work on the edge of modern theoretical knowledge of security, binding it with high technology. However, they can only occur and develop with consciously created and followed specialized training programs and practical training.

Funding and investing in security resources – security money is never enough, but new technologies and the necessary preparation for their operation require a certain resource – financial, human, moral, ethical, and so on.

Organizational culture in security – knowledge of ways, methods, forms of use of new technologies, their use in a complex way to achieve a synergic effect.

Decision-making and ranking of priorities – priorities are tailored to the needs of security, resources, technological capabilities.

Creation and use of operational methodologies – possible, desirable, secured by resources.

Economic incentives – resources are directed to structures and specialists operating with modern technologies in the interest of the society and civil security.

Design of high-tech security products – technologies in intelligence, counterintelligence, special intelligence means. Historically, the latest technology has been deployed and developed in defense and security.

Effective technical architecture – networks, information systems, expert systems, modern security communications covered by a unified architecture, resulting in a synergic technological effect.

Overcoming the resistance of society. Disputes over the use and misuse of services by new technologies, incited by ongoing scandals, lead to doubts as to the appropriateness of the use, the legality and the illegality, the competence and the incompetence. Here again, the well-known contradiction – "Freedom or Security" – is emerging. However, the facts gathered over the past 30 years have shown that even denial of certain civil liberties clearly does not lead to more security, but to abuses, anti-constitutional laws, activities and actions, and ultimately the result is defective security. Obviously Benjamin Franklin appears to be right, saying, "[Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.]" Proven necessary use of new technologies to counter crime and assure civil security can lead to overcoming this natural resistance.

5.0. References:

- Attali, J. A Brief History of the Future: A Brave and Controversial Look at the Twenty-First Century, Arcade Publishing, 2009, 291 p.
- Burrows, M., The Future, Declassified Megatrends That Will Undo the World Unless We Take Action. St. Martin's Press, 2014, 288 p.
- Goodman, M. Future Crimes. Inside the Digital Underground and the Battle for Our Connected World. Penguin Random House, 2016, 608 p.
- Labaree, L. W. (ed.). The Papers of Benjamin Franklin, vol. 6, 1963, p. 242

REMOTELY CONTROLLED NON-LETHAL WEAPON SYSTEMS IN THE CONTEXT OF LAW ENFORCEMENT

Assist.-Prof. Dr. Eng. Tumbarska A.

Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamic Centre "Acad. Angel Balevski"
at the Bulgarian Academy of Sciences (IMSETHAC-BAS), Sofia, Bulgaria

E-mail: y.toumbarski@ims.bas.bg

Abstract: *Unmanned weapon systems with one or another degree of autonomy are widely discussed in the last years. The increasing use of drones in the law enforcement of some countries attracts considerable attention with regard of potential human rights violations. Although both non-lethal weapons and remotely controlled systems can save lives and provide indisputable tactical advantages, the introduction of non-lethal armed robotic systems into law enforcement is being viewed with skepticism and concerns. The purpose of this article is to explore why society is concerned about these systems and to what extent such concerns are grounded.*

Keywords: NON-LETHAL WEAPONS (NLWs), REMOTELY CONTROLLED WEAPON SYSTEMS, UNMANNED VEHICLES, LAW ENFORCEMENT, DRONES, AUTONOMOUS WEAPON SYSTEMS (AWSs)

Introduction

Non-lethal weapons¹ (NLWs) are intended to avoid or at least minimize undesired deaths, injuries and destruction in situations where force is applied. In other words, NLW should cause short-term and reversible effects on people, equipment and environment. NLWs represent a wide range of weapons, munitions and devices, operating on various physical principles (kinetic, chemical, biochemical, electrical, directed energy, acoustical, mechanical).

Non-lethal weapons have been used in law enforcement since the 1960s. Initially utilized as an alternative or an addition to police firearms in controlling public disorders, at present NLWs play an important role throughout the spectrum of law enforcement functions – from arresting suspects and control of civil or prisoners rioting to border and infrastructure protection, counter-narcotics, anti-piracy, counter-terrorist and other operations to protect the order and security. Since the 1990s military forces are also taking advantage of the NLWs (though to a limited extent), mostly in so called 'operations other than war'.

Robotic weapon systems have been widely discussed lately. The progress of technology has brought us closer to the moment when the stories of science fiction films in which robots make decisions about killing people is about to become a reality. Semi-autonomous weapon systems already exist and the appearance of fully autonomous weapon systems (AWS) can be expected in the near future. While the idea of robots replacing people on the battlefield is inspirational for some, most people do not accept the use of fully autonomous weapons enabling strikes to be carried out without meaningful human intervention. Outstanding scientists, non-governmental organizations and institutions, including the European Parliament, call for a ban on development, production and use of fully autonomous weapon systems.

The rapid development and expanded use of systems with one or another degree of autonomy, whether equipped with non-lethal or lethal weapons, raises a number of questions. "The legal, ethical, and moral quandaries of using these systems in warfare are rightly beginning to receive the attention they deserve. But what's still being widely overlooked is the likelihood that they will also be used in police operations, and it is urgent that this is addressed now". [1] If left unchecked, rapid advances in technology, as well existing sophisticated semiautonomous lethal and NLWs systems make the development and deployment of fully AWSs virtually inevitable, both in conflicts and law enforcement operations. [2]

Although both non-lethal weapons and remotely controlled systems (RCSs) can save lives and provide indisputable tactical advantages, the potential introduction of non-lethal armed robotic systems into law enforcement is being viewed with skepticism and concerns, some of which seem well-founded.

Remotely controlled systems for non-lethal weapons delivery

The systems that deliver non-lethal effects to the targets (known as 'delivery systems') are critical to the effectiveness of non-lethal weapons. Along with ensuring safety of targeted objects, these systems should prevent from undesired collateral damage, providing proper 'dosing' of the effect and increased accuracy of delivery. These systems should also allow for engagement from as biggest as possible distances to the targets (out of the enemy weapons range) with the view of the weapons users' safety. In this respect, remotely controlled systems, having significant potential for reducing the risk to officers during their duties execution, are very attractive both for law enforcement and military services.

Robotic weapons can be classified in three groups: human-controlled ('human-in-the-loop') systems; human-supervised ('human-on-the-loop') systems; autonomous ('human-out-of-the-loop') systems. Remotely controlled ('human-in-the-loop') systems represent weapons which are controlled by a human operator from some distance. While such robots may be able to independently perform selected tasks delegated to them (e.g. navigation, systems control, target detection, and weapons guidance), they cannot attack without the real-time command of their human operator. [3]

Worldwide there is an expanding industry ready to produce robotic systems designed specifically for domestic law enforcement. Possible scenarios collected from the marketing literature of some of these companies include the use of such systems in the context of crowd control.[4] Companies in the USA, UK, Jordan, Israel, Spain and elsewhere are developing non-lethal robotic weapons for policing that are remotely operated or which fire automatically when touched. These include unmanned aerial vehicles (drones) and ground vehicles that can apparently shoot electric-shock darts, tear gas and other less-lethal projectiles. [1]

During the last decades a great variety of extended range non-lethal munitions has been developed intended for delivery from existing or especially designed platforms, including remotely controlled or mounted on unmanned land, surface, underwater or aerial vehicles. Non-lethal munitions intended for riot control and area denial that can be fired from such platforms include kinetic (soft trauma) projectiles, riot control agents (RCAs), smoke, sound, flash-bang, electro-shock projectiles, etc.

A range of grenade launchers, designed for riot control or area denial, incorporate a remote control capability. Many of them are intended for mounting on land vehicles or naval vessels and can

¹ Non-lethal weapons are defined by the US Department of Defense as weapons, devices and munitions that are explicitly designed and primary employed to incapacitate targeted personnel or materiel immediately, while minimizing fatalities, permanent injury to personnel, and undesired damage to property in the target area or environment.

utilize various non-lethal, as well as lethal, munitions. Automatic launchers can fire single shots, however when employed in continuous firing mode, and given their potential high rate of fire, they can rapidly discharge numerous non-lethal projectiles. Also, there is variety of 'multi-launchers', depending on the number of projectiles launched, the payload, the speed and mode of firing, range and area coverage, caliber, weight, etc. Unlike the automatic grenade launchers which are fed by belt or box, the multiple launchers are normally manually reloaded, however, using multiple barrels, they can rapidly fire large number of projectiles simultaneously. Both types of launchers are capable of covering wide areas and affecting large numbers of people, therefore have potential for causing significant collateral damage. [5]

Devices for RCAs² dispersion have been developed for indoor installation, for use in buildings and area protection, alternatively in prisons or other places of detention. The range of products include: systems to prevent burglar or terrorist penetrating a secured area or a building, utilizing CS or OC; wall-mounted systems for small rooms; systems for larger rooms, ceiling mounted systems with hosepipes for teargas supply; large systems for military use to protect supply infrastructures; for protecting security vehicles; for use in police vehicle protection; for preventing demonstrations; for prisoners control, etc. Part of these systems are remotely controlled, others are activated by the targeted person and automatically release doses of the agent, practically without a real-time control by operator. The use of such devices in confined spaces or poorly ventilated rooms, or in situations where prisoners, detainees, or other targets cannot leave the contaminated area rapidly, could pose a risk of accumulating toxic chemicals in the human body, leading to serious injury or death. The employment of such devices in larger enclosed areas such as prison halls also has the potential to cause injuries resulting from panic and stampedes. [5, 6]

Some traditional law enforcement tools used for decades, such as water cannons, as well as newer systems like these based on 'Taser' technology, are also designed to be controlled from safe distances. Concepts for the use of advanced systems such as Long Range Acoustic Devices (LRAD) and Active Denial System (ADS), whose implementation is still limited or forthcoming, also provide for remote control functioning or integration with unmanned vehicles.

Remotely controlled water cannons are available for riot control, as well as outdoor stationary systems for area denial and clearing mounted on rooftops and towers of prisons. In addition to the standard kinetic effects of high pressure water jets, chemicals (OC, CS, marking dyes) may be injected into the jet. Some sophisticated anti-riot vehicles are capable along with water cannons, to deliver a range of remotely controlled non-lethal measures for controlling aggressive crowds. [5, 7] Most of the anti-piracy water cannon systems also can be remotely controlled from safe positions on ships.

Devices based on 'Taser' technology have been developed to protect military facilities and other key facilities such as airports, embassies, TV- and radio-stations, through delivering electro-shock to individual intruders or during major demonstrations or riots. Such devices are intended to be attached to the protected building or equipment and remotely controlled via video from a hardened security room within the facility or from the vehicle cabin. [8] However, information for real utilization of such systems was not found. One of the possible reasons for this may be the public attitude to police-favored 'Taser'-type devices associated with a number of incidents.

² Riot control agents (RCAs) are chemical substances which rapidly produce sensory irritation or disabling physical effects in humans which disappear within a short time following termination or exposure. The most commonly used RCAs at present are 2-chlorobenzalmalononitrile (CS, known as 'tear gas'), oleoresin capsicum (OC, known 'pepper spray') and its synthetic analogue PAVA. In some countries malodorants (malodorous 'skunk' substances) are often applied recently in crowd control.

LRAD which can deliver intelligible messages, warnings, notifications, instructions and commands within a range of up to 3 km to individuals or large crowds through focused acoustic beam are systems with potential application in a wide range of law enforcement situations. When integrated with remote-controlled vessels, these systems can be used to ensure the security of ports and ships; LRADs mounted on a helicopter provide vital communication capabilities for a variety of missions, including search and rescue, command and control, humanitarian aid and disaster response. [9, 10]

Active Denial System (ADS) is an advanced directed energy system capable to project a beam of millimeter waves at a distance of up to 1000 m. Unlike the powerful military version, a smaller range compact version is under development for the law enforcement. Some ADS application concepts plan the installation of such systems in US prisons ceiling where everyone in the room can be remotely affected with one joystick movement or pushing a button. [11] A modular ADS system had been intended for testing in the Los Angeles County jail, coordinated by the National Institute of Justice, but the system had been withdrawn before being operational, on the grounds that its use could be considered torture, [12] given the intensive pain caused to targeted persons.

Unmanned ground vehicles (UGVs) are developed to perform various functions, including in policing, military and security operations. Many of them are capable to deliver various kinds of non-lethal /lethal munitions at significant distances. Some UGVs are designed to utilize pepper spray or dazzling lasers that cause temporary blindness [5, 13], others can deliver electro-chock effect [14]. Such robots are usually intended for intervention, without direct contact, in civil riots, prison disturbances or other disorders, where neutralization of particular individuals and eliminating potential threats is required, without the escalation which is usually caused by police use of force.

Non-lethally armed drones

Since armed drones have been subject of discussions and criticism over the last 15 years during the 'war on terror', their use, especially in law enforcement, deserves special attention.

An unmanned aerial vehicle (UAV), commonly known as a 'drone', is an aircraft without a human pilot aboard. UAV is a component of an unmanned aircraft system (UAS) which include a UAV, a ground-based controller, and a system of communications between the two. The flight of UAVs may operate with various degrees of autonomy: either under remote control by a human operator or autonomously by onboard computers. [15]

Unmanned aerial vehicles are not unprecedented - in World War II, radio-controlled B-24s have been sent on bombing missions over Germany; remotely controlled aircraft have carried cameras over battlefields in Vietnam. [16] Initially intended mostly for military applications, now UAVs are widely used for scientific, commercial, agricultural, and other applications, such as surveillance, policing and peacekeeping.

Law enforcement agencies in many countries use drones for surveillance of land and infrastructure; border and road patrol; detection, identification and surveillance of individuals; finding lost persons; crime investigation; search and rescue operations; etc. For example, according the media, in the USA at least 347 police and fire departments in 43 states are using drones for similar purposes.

Drones can perform operations in much less time than ground-based teams and provide enhanced situational awareness during dangerous operations. Despite these tactical benefits, there are strong and valid concerns from human rights advocates and citizens regarding privacy and safety, including the potential of spying, unwanted surveillance, misuse of data collected, etc. [17]

While many people can support targeted attacks on extremist leaders and groups thousands of miles away, at the same time they are very sensitive to the possibility of armed drones flying over their homes. According to a Gallup Poll [18], 65% of Americans think the U.S. government should use drones to launch airstrikes in

other countries against suspected terrorists; 41% support airstrikes in other countries against U.S. citizens living abroad who are suspected terrorists; only 25% - airstrikes in the U.S. against suspected terrorists living here and 13% - in the U.S. against U.S. citizens who are suspected terrorists.

Public debates induced by increased use of UAVs by law enforcement authorities in some countries, particularly in the USA, have deepened when equipping drones with NLWs have begun to be considered. While some states are still debating how these systems should be regulated, North Dakota became the first state in the USA which allowed police to equip drones with NLWs in 2015, setting a precedent for other states to follow. At the end of 2016, Tennessee and South Carolina introduced laws to their legislatures that gave police the option for arming drones. [19] In 2017 the Connecticut lawmakers were considering whether to legalize police drones outfitted with deadly weapons however this proposal was immediately encountered by civil rights and liberties concerns. [20] So far, there has been no known use of armed drones in the context of domestic law enforcement and border protection, although the United States appear to have contemplated using them in support of counter-narcotics operations in Mexico. [21] Given the rapid growth of drone industry, probably more and more countries will soon take legislative measures to regulate the law enforcement use of UAVs. And perhaps legalizing armed drones in law enforcement will face public opposition, given that the term 'drone' has become usually associated with military-style drones like the US 'Predator' used in the 'war on terror'.

For equipping law enforcement drones several kinds of non-lethal weapons have been considered, such as blunt trauma projectiles, RCAs, marking dyes, and electro-shock. According to some, such drones are still not feasible, due to the technical challenges connected with the short range of these NLWs, because of which the drones will have to fly at a small height where it is not difficult to be neutralized. [22] However, as practice shows, these obstacles are not irresistible – the short range 'Taser' type devices can be replaced by wireless electro-shock projectiles, rubber bullets – by extended range non-lethal kinetic grenades, RCAs can be easily placed into capsules or nylon bags to be delivered from drones.

Companies in USA, Israel, China, Germany, Austria, France, South Africa (and probably in other countries) have developed UAVs for law enforcement application [5]. Some of these drones are already in use. For example, drones specializes in non-lethal riot control, crowd management, anti-terror equipment and police gear produced in Israel [mmm] are utilized for delivery of payloads with 'skunk water' bags. [23] In India, a law enforcement agency have purchased and tested several drones built in South Africa, intended to disperse unruly mobs, which are capable of firing large number of paintballs, pepper spray balls or solid plastic balls. [24, 25]

Public concerns about the use of non-lethal remotely controlled in law enforcement

When discussing public concerns about the remotely controlled non-lethal systems, including UAVs, equipped with non-lethal weapons, the two components - NLWs and RCSs - should be considered both separately and in combination, since each of them causes different objections based on real examples of misuse, and more often - on hypothetical concerns about potential misuse.

The existing negative public attitude towards particular NLWs and the NLWs in general is due to several reasons. In the context of law enforcement NLWs are intended to reduce the violence and prevent the use of lethal force. Some people, however, perceive any use of police force as violation of human rights even in situations when it is inevitable and this force is applied by non-lethal means. Along with this, in some countries there are proven cases of NLWs abuse against suspects, prisoners or ethnical groups, as well as cases where they have been unjustifiably used in peaceful civil protests. Although designed for avoidance of fatalities and injuries, NLWs have caused significant number of casualties in the past. Regardless of the experience gained and the continuous improvement of these

weapons, their use is still associated with certain risk since their effects are determined by several factors (to emphasize the fact that NLWs are not 100 % risk free, in some countries' law enforcement they are called 'less lethal weapons'). At present, the incidents due to the use of NLWs are rare and rather result from improper use than from technology itself. An important cause of the NLW's poor image is their use in military conflicts as a complement to conventional weapons (a historic example is the massive use of tear gas by US forces in Vietnam in the 1960s-1970s for removing the enemies from their hiding places to facilitate their killing).

The biggest concern associated with remote-controlled weapon systems, including drones, is that they would make the use of force more easily, since the physical distance between the person who controls such a system and his target would break the psychological barrier that prevents from killing another human being. This theory, known as 'PlayStation mentality/phenomenon', sounds convincing since for most people probably it is much harder to kill a man standing a few meters away, than shooting a figure depicted on the screen by pushing a button. However, some [26] reasonably notice that such statements are either overstated or unproven.

Eliminating relation between the opponents through distance that makes killings, abuses and atrocities to resemble virtual reality can be extrapolated also to law enforcement situations. According to [19], applying this theory is even more aptly in law enforcement because of the lack of lethal force: if police officers think that they can only temporarily harm a suspect, they may have greater incentive to use NLWs. Remotely controlled NLWs, including drones, are intended to limit exposing police officers to risk in dangerous situations, giving them more time for assessing the situation and reaction. However, the question that is raised most often in this connection is whether the officers would use the opportunity to deescalate the situation, or the distance rather will make it easier for them to decide on shooting NLWs.

Furthermore, there are fears that physical distance may result in inaccurate assessment of a situation, thus creating potential for affecting non-targeted people. Even officers present on the scene may sometimes fail to properly estimate when and how much force to apply and that could be more difficult if they do not have a direct view on the situation. For example, in a riot control operation an officer flying a CS-armed drone may not be able to properly judge what quantity of the agent to discharge over a crowd.

Proponents of robotized weapons believe that the accuracy of these systems will drastically reduce collateral damages, however so far the facts rather support the opposite - while such weapons are increasingly deployed the rate of innocent casualties is rising. The use of armed drones in the 'war on terror' for 'targeted killing' terrorist leaders in Iraq, Afghanistan, Yemen, Pakistan and Somalia as a response to terrorist attacks of 9/11/2001 is an eloquent example in this respect. According to statistical data collected by an Israeli scientist, in April 2009, 687 civilians have been killed along with 14 Al Qaeda leaders – over 50 civilians killed for every Al Qaeda target; for each Al Qaeda and Taliban terrorist killed by US drones, 140 Pakistanis also had to die. "Over 90 percent of those killed in the deadly missile strikes were innocent civilians". [27] Against this background, public fears of using armed drones, even equipped with non-lethal weapons, are understandable. However, unlike drones which may be sometimes unpredictable due to meteorological conditions, many others remotely controlled NLWs can be delivered with considerable accuracy.

Undoubtedly, any technology can be used for good or bad purposes and remotely controlled non-lethal systems are not exception. In addition to possible abuse in law enforcement for human rights violations, such systems may be acquired and used by non-state actors such as criminals and terrorists to commit murders and other crimes. While this is quite likely, it does not sound like a convincing argument against the use of such systems in law enforcement. There are also some other arguments that seem less important than those listed and therefore not addressed here.

Finally, a serious concern is that the introduction of non-lethal armed drones in law enforcement could lead to increasing

weaponization, opening the door to deadly weapon systems. While prohibitions of robots armed with deadly force can find police support in countries where most police officers are unarmed, as are most civilians, in others countries, when such robots start being used in committing crimes, they may become just another tools that the police will want to use. [28] And the next step in this direction could be the employment of fully autonomous weapon systems which are inherently incompatible with human rights laws.

Conclusion

Contemporary non-lethal technologies, combined with remote control, have big potential to increase the safety in law enforcement, both of officers and public. Such systems are becoming more accessible and will be increasingly used to disperse forcible crowds and to accurately fire non-lethal munitions to prevent using weapons against the police or other citizens. Probably in the near future their use will cover more life threatening situations as clearing buildings from armed criminals and incapacitating barricaded hostage-keepers. These systems are not perfect, as are the people who control them, so the possibilities for accidents can not be totally excluded. Since the potential negative consequences are known, effective ways of their prevention should be found, without limiting the ability of law enforcement to protect society. The public must be properly informed about the new technologies and convinced that they would be used in good faith and reasonably for the benefit of public security. Therefore, remotely controlled non-lethal systems have to demonstrate positive and safe applications and this can only be achieved if these systems are utilized by well-trained and highly responsible professionals, strictly following clear policies and rules of engagement.

References

- [1] Amnesty International. UN: Ban killer robots before their use in policing puts lives at risk. Meeting of the UN's Convention on Certain Conventional Weapons, Geneva, 16 April 2015. <https://www.amnesty.org/en/latest/news/2015/04/ban-killer-robots-before-their-use-in-policing-puts-lives-at-risk/>
- [2] Amnesty International. Autonomous Weapons Systems: Five Key Human Rights Issues for Consideration. 2015. https://www.amnesty.nl/content/uploads/2015/04/autonomous_weapons_systems.pdf?x41799
- [3] Melzer, N. Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare. EU Directorate-General For External Policies, May 2013. [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPODROI_ET\(2013\)41](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPODROI_ET(2013)41)
- [4] Heyns, C. Autonomous weapons systems and human rights law. Presentation at the informal expert meeting organized by the state parties to the Convention on Certain Conventional Weapons 13–16 May 2014, Geneva, Switzerland. [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/DDB079530E4FFDDBC1257CF3003FFE4D/\\$file/Heyns_LAWS_otherlegal_2014.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/DDB079530E4FFDDBC1257CF3003FFE4D/$file/Heyns_LAWS_otherlegal_2014.pdf)
- [5] Crowley, M. Tear Gassing by Remote Control: The development and promotion of remotely operated means of delivering or dispersing riot control agents. Report of University of Bradford and Omega Research Foundation, December 2015.
- [6] Crowley, M. The use of riot control agents in law enforcement, in: Casey-Maslen, S. (ed.), *Weapons Under International Human Rights Law*, Cambridge University Press, UK, 2014, pp 334-356.
- [7] The Israeli Companies at Milopol: Beit Alfa Technologies. Israel Defence, 11 November 2013. <http://www.israeldefense.com/en/content/israeli-companies-milopol-beit-alfatechnologi>
- [8] McNulty, J. Remotely Controlled Non-Lethal Weapons Applications. NDIA 16th Annual Security Technology Symposium, Williamsburg, 2000. <https://www.hSDL.org/?view&did=443808>
- [9] Goldberg, A. and J. Casali. Non-Lethal Acoustical Weapons: Overview and Auditory/Nonauditory Risks. 2014. https://cdn.ymaws.com/www.hearingconservation.org/resource/resmgr/2014_Conference_Proceedings/Goldberg.pdf
- [10] LRAD. <https://www.lrads.com/application/law-enforcement/>; <https://www.lrads.com/application/defense/>
- [11] Rogoway, T. Are 'Pain Ray' Cannons The Next Must Have Toy For Commando Cops? 22 August 2014. <https://foxtrotalpha.jalopnik.com/are-pain-ray-cannons-the-next-must-have-toy-for-command-1624592203>
- [12] <https://bigthink.com/ideafeed/handheld-version-of-military-pain-ray-being-developed>
- [13] Eshel, T. RiotBot - Armed For Close Combat. Defense Update, 19 Oct. 2010. https://defense-update.com/20101019_riotbot.html
- [14] McLain, J. Full-Auto Teddy Bear: Non-Lethal Automotons and Lethal Human Teaming to Increase Overall 'Lethality' in Complex Urban Environments. Small Wars Journal. <http://smallwarsjournal.com/jrnl/art/full-auto-teddy-bear-non-lethal-automatons-and-lethal-human-teaming-increase-overall>
- [15] International Civil Aviation Organization. Circular 328 AN/190: Unmanned Aircraft Systems. ICAO, 2011. https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf
- [16] Bowden, M. How the Predator Drone Changed the Character of War, Smithsonian Magazine, November 2013, <http://www.smithsonianmag.com/history/how-the-predator-drone-changed-the-character-of-war-3794671/?no-ist>
- [17] Valdovinos, M., J. Specht and J. Zeunik. Law Enforcement & Unmanned Aircraft Systems: Guidelines to Enhance Community Trust. Washington, DC: Office of Community Oriented Policing Services, 2016. https://rems.ed.gov/docs/COPS_Community-Policing-UAS.pdf
- [18] GALLUP. In U.S., 65% Support Drone Attacks on Terrorists Abroad. 25 March 2013. <https://news.gallup.com/poll/161474/support-drone-attacks-terrorists-abroad.aspx>
- [19] Spallanzani, N. For When the Sky is not the Limit: Non-Lethal Drone Use by Law Enforcement. Seton Hall Legislative Journal, Vol. 41, issue 2, 2017, pp 443-466.
- [20] Connecticut would be the first state to allow armed police drones. REUTERS, 31 March 2017. <https://www.newsweek.com/connecticut-drones-police-police-drones-armed-drones-577648>
- [21] Entous, A. Special Report: How the White House learned to love the drone, Reuters, 18 May 2010, referred to in Alston, The CIA and Targeted Killings Beyond Borders, N 132.
- [22] Hambling, D. No, Taser-Firing Cop Drones Aren't Coming For You, 10 September 2015. <https://www.popularmechanics.com/flight/drones/a17288/police-drones-beanbags-tasers/>
- [23] Israeli Drone Supplies New Non-Lethal Response to Riots. IHLS, 16 May 2018. <https://i-hls.com/archives/83077>
- [24] Porter, A. Law Enforcement's Use of Weaponized Drones: Today and Tomorrow. Saint Louis University School of Law, Vol. 61:351, 2017, pp 351-370.
- [25] <http://www.desert-wolf.com/dw/products/unmanned-aerial-systems/skunk-riot-control-copter.html>
- [26] Boyle, M. The legal and ethical implications of drone warfare, The International Journal of Human Rights, 19:2, 2015, pp 105-126, DOI: 10.1080/13642987.2014.991210
- [27] Falk, O. Permissibility of Targeted Killing. Studies in Conflict & Terrorism, 37:4, pp 295-321, DOI: 10.1080/1057610X.2014.879380
- [28] Joh, E. Policing Police Robots. UCLA Law Review, Vol. 64, 2016, pp 516-543. <https://www.uclalawreview.org/policing-police>

MIGRATION, TERRORISM AND POSSIBLE ARMED CONFLICTS IN THE WESTERN BALKANS

Prof. dr. Saša Mijalković. PhD¹, Ass. Prof. Dr. Dragana Cvorovic. PhD²

University of Criminalistics and Police Studies, Belgrade, Republic of Serbia¹, University of Criminalistics and Police Studies,
Belgrade, Republic of Serbia²

E-mail: sasa.mijalkovic@kpa.edu.rs, dragana.cvorovic@kpa.edu.rs

Abstract: Ethnic, religious, cultural and ideological and political diversity of societies in the Balkan Peninsula have repeatedly led to armed conflicts and various forms of political violence in the past. Similar turmoils are evident so far, and it is highly unlikely that they would be absent in the future. For that reason, the geospatial of the Balkans is symbolically called the "powder keg". An additional security challenge is certainly the global forced migration that this georegion is faced with after 2015, which has also increased the fears of governments and citizens against refugee terrorism. In this regard, the aim of this paper is to point out that the fear of "Islamist terrorism" of migrants is unjustified, while at the same time extremist groups and radicalized individuals who have been present for years in the Balkans and who were resorting, who resort now and will probably resort to some forms of political violence in the future, are marginalized.

Key words: migration, extremism, terrorism, Western Balkan countries, national and international security.

1. Introduction

The Balkan Peninsula is a geographical area located in the south eastern part of Europe. It is bounded by the rivers Danube and Sava, the Mediterranean Sea, the Black Sea, the Sea of Marmara, the Aegean Sea, the Ionian Sea and the Adriatic Sea. It covers an area of about 470,000 km² and almost completely coincides with the region known as Southeast Europe. The territories of Montenegro, Macedonia, Bosnia and Herzegovina, Albania and Bulgaria belong entirely to this region, whereas the territories of Serbia, Croatia, Slovenia, Greece, Italy, Romania and Turkey more or less belong to it (Zoltan, 2007; Lampe, 2014; Svob, 2001).¹

Unlike the above geographical term, the term "Western Balkans" represents the Western political jargon that came into existence with the breakup of the Socialist Federal Republic of Yugoslavia. It used to refer to the part of the territory of the Balkan Peninsula according to the following formula: "the former Republics of the SFRY minus Slovenia plus Albania". Therefore, the Western Balkans is a geographical region consisting of Serbia, Montenegro, Croatia, Macedonia, Bosnia and Herzegovina and Albania.

Apart from ethnic and religiously motivated hatred which represents an etiological constant that keeps bringing new tensions and conflicts back to life (Zbigniew, 1997)², this region is characterized by considerable migrations, both from the East towards the Western Balkans, as well as from the Balkans towards the West and the North (Mijalkovic, 2009). From the aspect of potential conflicts, by far the most important migrations occurred in the 1990s (emigration - the departure of citizens of former SFRY Republics abroad and immigration - the arrival of Mujahideen, terrorists of Al Qaeda and other mercenaries from abroad to the Western Balkans) as

well as at the beginning of 2015 (as a result of armed conflicts in Syria) (Mijalkovic, 2016).

More precisely, migrations are a global phenomenon, whereas the geographical region of the Balkans is an integral part of the world's migration routes. In the World Migration Report 2018, published by the International Organization for Migration, there are estimates that in 2009 there were about 740 million internal migrants in the world; that in 2015 there were about 244 million international migrants; that in 2016 there were about 40 million internally displaced persons and about 25 million refugees. Of this, about 75 million migrants live in Europe, of which about 40 million were born in Europe (the so-called second and third-generation migrants).³ It is estimated that between 15 million and 30 million people have the status of an illegal migrant worldwide, and that only during 2016 about 2.5 million migrants were subject to smuggling worldwide.⁴ The law of large numbers suggests that it is possible to hide terrorists among migrants, and that those who transit through the territory of the Western Balkans are here precisely to commit terrorist attacks. This, along with unintentional, but also some tendentious statements by many European politicians and radical right-wing politicians, created an unreasonable panic and fear among Europeans who see terrorists in all migrants.

In this regard, the aim of this paper is to show, through a modest analysis of possible crisis hot spots and conflict areas, who the potential terrorists and bearers of similar forms of political violence are, as well as to contribute to the "breaking" of prejudices that these are migrants.

Finally, the authors also have the need to point out that the entire scientific institutes and scientific research projects have been devoted to research of this type, and that they are aware of the modesty of the results and conclusions that will be presented in this paper, whose goal is ambitiously set. Therefore, they did not engage in more detailed and comprehensive critical and comparative analyses of statistical data and other more detailed indicators of the phenomena that are the subject of the research, but have rather tried to draw new

¹ The paper is the result of the scientific research project entitled *The Development of Institutional Capacities, Standards and Procedures for Combating Organized Crime and Terrorism in the Conditions of International Integration*. The Project is funded by the Ministry in charge of Science in the Republic of Serbia (No. 179045), and it has been realized by the Academy of Criminalistic and Police Studies in Belgrade (2011–2019). The project manager is prof. Saša Mijalković, PhD.

² For example, Brzezinski refers to the conflict areas in Euroasia as the "Eurasian Balkans".

³ *World Migration Report 2018*, International Organization for Migration, Geneva, 2018, p. 2, 21, 67.

⁴ *The Global Study on Smuggling of Migrants 2018*, United Nations Office on Drugs and Crime, New York, 2018, p. 5.

conclusions on the relationship between migration and terrorism through cluster analysis of commonly known facts and events.⁵

2. Contemporary and potential terrorism and conflicts in the Western Balkans

The Western Balkans has been considerably exposed to terrorism in recent decades. According to the criterion of the ethnicity of terrorists, the most noticeable was the terrorism of Albanian extremists. In terms of their religious beliefs, it was the terrorism of radical Islamists (primarily Albanian extremists, Islamists in Bosnia and Herzegovina, Wahhabi and jihadists) (Mijalkovic & Bajagic, 2015).

In the following part of the paper, we present the most significant prevented terrorist intentions as well as terrorist attacks (all of which had their epilogues in court, or the trial is on-going (Cvorovic, 2013)). More precisely, there were examples of terrorism and terrorist attempts⁶:

- in *the Republic of Serbia*, namely, in the area of the Autonomous Province of Kosovo and Metohija, during the 1990s, as well as in the south of central Serbia (the Preševo Valley - the regions of Bujanovac, Preševo and Medveđa) at the beginning of the 2000s, the terrorist actions were carried out by Albanian extremists.⁷ Apart from that, in the police actions carried out in 2007 in the vicinity of Novi Pazar, 16 Wahhabis were arrested. These were the members of the terrorist group that planned terrorist attacks on police facilities and people, Mufti Zukorlic, the football stadium in Novi Pazar, and to government institutions and foreign embassies in Belgrade. Some of them were arrested in a police operation in the Ninaji Mountains, where armed conflicts with terrorists occurred, when a terrorist leader was killed, and a large quantity of weapons and explosives was confiscated. Their connection with ideological like-minded people in Albania, Bosnia and Herzegovina, Macedonia, Georgia and Syria has been proven;
- in *Montenegro* in 2016 a group of 14 people (from Serbia, Montenegro and Russia) was arrested, on suspicion of planning terrorist attacks and the violent coup during the presidential election. In 2018, a Montenegrin threw an explosive device at the United States Embassy in Podgorica, and then committed suicide by activating another explosive device;
- in *Bosnia and Herzegovina (the Republic of Srpska and the Federation of Bosnia and Herzegovina)*, the first attack took place in 1995 in Banovići, when an UNPROFOR officer disappeared and was killed, and the second in 1997 in Mostar, when a car bomb was activated. Both attacks were linked to Al Qaeda members in Bosnia and Herzegovina. In Kostajnica near Konjic, an Islamist fanatic killed three members and wounded one member of the Serbian family on Christmas Eve in 2002; in 2008 an explosive device in the FIS shopping mall was activated in Vitez; a group of radical Islamists activated an explosive in

a police station in Bugojno in 2010; next - in 2011, a radical Wahhabis started shooting towards the US Embassy in Sarajevo; another radical Wahhabis attacked a police station in Zvornik in 2015; that same year, one more radical Wahhabis in Rajilovac killed two members of the armed forces of Bosnia and Herzegovina. Besides, the security forces arrested several groups of radical Islamists who planned terrorist attacks not only across Bosnia and Herzegovina, but also in Europe. The most famous arrests (Cvorovic, 2016) of radical Islamists were in Sarajevo: in 2007 (4 Islamists who planned terrorist attacks on several targets in Europe and at the American Embassy in Sarajevo) in 2008 (a group of Islamists planning attacks on EUFOR units, the facilities and staff of the Government of the Republic of Srpska, the Catholic Church and the Armed Forces of Bosnia and Herzegovina); in 2015 (11 persons linked to the terrorist organization ISIL) as well as in 2018 (two radical Islamists who were preparing terrorist attacks at the State Investigation and Protection Agency (SIPA) in East Sarajevo and the police headquarters in Tuzla);

- in *Croatia* in 1995 radical Islamists linked to Al Qaeda and the Egyptian terrorist organization carried out a terrorist attack by activating a car bomb in Rijeka (the person who committed suicide was a citizen of Kuwait). Otherwise, as a member of the European Union and NATO, Croatia fears global Islamic terrorism, but it also fears possible attacks by Islamist terrorists from the territory of Bosnia and Herzegovina, whose targets would be Croats and Serbs;
- in *Macedonia*, terrorist attacks were carried out by the Albanian terrorist organization National Liberation Army during 2001; a group of Albanian terrorists from Kosovo and Metohija who were active in the vicinity of Tetovo in 2007; a group of Albanian extremists who killed five Macedonians in Smiljkovci, during civil riots and conflicts between Macedonians and Albanians in 2012; the terrorist National Liberation Army that claimed responsibility for attacking the government building in Skopje with rockets in 2014; a terrorist organization, the Kosovo Liberation Army, which in 2015 attacked a police station in the village of Gošnice near Lipak; a terrorist organization from Kosovo and Metohija that in 2015 infiltrated the territory of Kumanovo, as well as unknown terrorists who activated explosive devices in the center of Kumanovo the same year;
- when it comes to *Albania*, the Former Prime Minister Sali Beriša in the official media appearance in early 2017 acknowledged that Albania had assisted Albanian terrorists in Kosovo and Metohija by supplying them with weapons, among other things. Most of the weapons originated from military warehouses that were allegedly robbed (and actually opened for terrorists) during civil riots (the so-called "big anarchy") in Albania in 1997.⁸ So, there is no terrorism in Albania, but Albania was an exporter and a sponsor of terrorism.

Therefore, based on this brief overview of terrorism in the recent history of the Western Balkans, as well as on the brief account of the "conflicts of civilizations" - interethnic and interreligious tensions, one can conclude that the following geographical regions are the so-

⁵ In this paper, the authors relied on the numerous results of personal research carried out within the framework of the scientific research project mentioned at the beginning of the paper.

⁶ The analysis was based on the author's personal records that were generated by monitoring and investigating the phenomenon of terrorism

⁷ We talk about a large number of terrorist activities that have been described in the so-called White Book of the Government of the Republic of Serbia: *Albanian Terrorism and Organized Crime in Kosovo and Metohija*, Government of the Republic of Serbia, Belgrade, 2003

⁸ See more in: „SALI BERIŠA PRIZNAO: Albanija naoružavala teroriste OVK“, www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:658453-SALI-BERISA-PRIZNAO-Albanija-naoruzavala-teroriste-OVK, April 3rd, 2017. (visited on August 15th 2018).

called "tipping points", i.e. places of potential conflicts that may result in terrorism or certain armed violence:

- Kosovo and Metohija, which, as the "empire" of organized crime and terrorism in Europe, does not want to recognize the authority of the Republic of Serbia and at all costs strives towards statehood and independence from the Republic of Serbia. Finally, Al Qaeda's cells are also present in Kosmet, which would be put into the function of extreme Albanians (Sikora)⁹;
- Preševo valley in the Republic of Serbia (municipalities Bujanovac, Preševo and Medveđa) which is an integral part of the ideological-separatist project called the Great Albania, and now the so-called Great Kosovo (by annexing the Valley to the so-called Republic of Kosovo);
- Raška region in the Republic of Serbia (the so-called Sandžak, with its centres in Novi Pazar, Sjenica and Tutin) is a tipping point according to two grounds: firstly, radical Muslims (who call themselves Bosnians) tend to have certain autonomy in relation to the republican government; secondly, radical Wahhabis strive for a certain autonomy, referring to religious rights;
- the Northern part of Montenegro (Plav, Petnjica and Rožaje with the surrounding area) and the coastal area (the regions of Bar and Ulcinj) may be endangered by the activities of destructive Wahhabis and tekfiri, which would seek some sort of own or common autonomy with Wahhabis in Serbia and Bosnia and Herzegovina;
- parts of west, south and south-west region of Montenegro which rely on Albania and Kosovo and Metohija have also been a part of the separatist project of the Great Albania, so the separatist activities of the extreme Albanians are possible;
- Federation of Bosnia and Herzegovina is threatened by radical Wahhabis who strive towards certain autonomy (Bajagic, 2015; Hamad 2007; Hecimovic, 2009; Sindler, 2009; Azinovic, 2007);
- Croatia is currently not endangered by anyone. Although there is public opinion that Croatia might be threatened by Islamic terrorism, turned especially against Croats and Serbs, or against state institutions, such a scenario is possible, but highly unlikely.
- Republic of Albania is also not threatened by any form of political violence, and there is also no indication that something like that might happen in the near future.¹⁰

Thus, the experience of the Western Balkan countries with terrorism is known. At the same time, it is clear which geographical regions of these countries are particularly "tipping" - potentially conflicting. The situation is further complicated by the mass migrations that this region has been facing over the past several years.

3. Contemporary migrations and possible terrorism and conflicts

One can doubtlessly conclude that the fear of migrant-terrorists is excessive, but not groundless. Namely, only in 2016, more than half a million illegal border crossings were registered, and in 2015 more than 1,100,000 migrants illegally entered the territory of the European Union. Almost all these migrants were smuggled by organized crime groups.¹¹ At the same time, the biggest fear of terrorism in Europe is currently associated with terrorists of Al Qaeda and ISIL, who can immigrate or be smuggled into European countries. They are most often considered one and the same, although these are not partner organizations.

Namely, Al Qaeda is a global Islamist network of terrorists, but also numerous followers and fans of its ideology (supporters who are never officially recruited in the Al Qaeda terrorist network but blinded by its ideology are carrying out terrorist attacks and the so-called "white Al Qaeda" - Islamists who were born in the West, recruited by Al Qaeda). The Al Qaeda ideology is drawn from the tendentious and malicious interpretation of the Quran and other Islamic holy books, and the crimes are allegedly committed "in the name and for the glory of Allah." Their goal is to create Islamic states wherever Muslims live, as well as victory in the fight against cultural domination and the influence of the global West on the Islamic world (Mijalkovic, 2018).

Islamic State (ISIS – *Islamic State of Iraq and Syria*; ISIL – *Islamic State of Iraq and the Levant*; IS – *Islamic State*) is a geographical region that encompasses parts of Iraq and Syria, which, from the beginning of 2014, was under the control of militant Sunni fundamentalists - Salafists, who declared (otherwise unrecognized) statehood. In the middle of the same year, a caliphate was proclaimed, in which there is no place for Christians, Jesuits and Shiites, according to whom war crimes and genocide are committed. ISIS followers are present in Afghanistan, Pakistan, Morocco, Algeria, Tunisia, Libya, Egypt, Yemen, Nigeria, the Philippines, the Federation of Bosnia and Herzegovina and the self-proclaimed Republic of Kosovo. ISIS initially collaborated with Al Qaeda, which would later lead to misunderstandings, due to which Al Qaeda demanded the disintegration of ISIS.

From the point of view of emigration, it is interesting that the areas of the main points of Al Qaeda and ISIL are significant "emigration reservoirs". Namely, among the first 20 countries in the world that people mostly emigrate from, Syria is on the ninth place (5.5 million emigrants since the beginning of the conflict), Afghanistan at the eleventh place (2.5 million emigrants). At the same time, there is no single country from the Western Balkans on the list of the top 20 countries to which people mostly immigrate in worldwide.¹² The reasons for the emigration are clear - armed conflicts and fear for personal security; the reasons for non-immigration to the countries of the Western Balkans are also clear - a low standard of living. For this reason, many migrants from the territory of Syria and Iraq are actually only in transit through the

⁹ In 1995, Shiptar terrorists from Kosmet met Osama bin Laden, when an agreement was reached regarding logistic and financial aid to Al Qaeda and the formation of Al Qaeda cells in Kosovo and Metohija *Albanian Terrorism and Organized Crime in Kosovo and Metohija*, Government of the Republic of Serbia, Belgrade, 2003, pp. 26–28, 40.

¹⁰ The analysis was based on the author's personal records that were generated by monitoring and investigation of the phenomenon of terrorism.

¹¹ *SOCTA 2017 – European Union Serious and Organized Crime Threat Assessment – Crime at the Age of Technology*, European Police Office, The Hague, 2017, p. 49.

¹² *World Migration Report 2018*, p. 19, 33. The situation is the same when it comes to the list of 20 countries in the world that are the top destination of (potential) migrants. See p. 176 of the Report.

territories of the countries of the Western Balkans, without the intention of inhabiting it permanently.¹³

In general, routes of migrant refugees from the Asian region, primarily from the areas of Syria, Iraq and Afghanistan, which are significant from the aspect of the Western Balkans, are:

- by land: Turkey – Bulgaria – Serbia;
- by land: Turkey – Greece – Macedonia – Serbia;
- by land: Turkey – Greece – Albania – Serbia (Kosovo and Metohija);
- furthermore, generally, there are five migration directions from Serbia: towards Romania, towards Hungary, towards Croatia, towards Bosnia and Herzegovina and towards Montenegro, depending on the direction from which migrants arrived in Serbia and where they are headed (from Croatia to Slovenia or Hungary; from Bosnia and Herzegovina through Croatia to Slovenia or Hungary);
- by land: Turkey – Greece – Albania – Montenegro, then from Montenegro towards Serbia, Bosnia and Herzegovina or towards Croatia;
- by sea: Turkey – the Aegean Sea – Greece, then by land on one of the mentioned routes;
- by sea: Syria or Turkey – the Mediterranean Sea – Italy, Malta, not so often to France or Spain, or less frequently to Montenegro and Croatia, then further by land on one of the mentioned routes;
- by sea: Egypt – the Mediterranean Sea – Greece, then by land on one of the mentioned routes.

However, not all immigrants can reach the desired destinations. The restrictive immigration policies of Western European countries (the so-called "non-welcome" policy, "barbed wire" policy, "xenophobia" policy, etc.) have influenced migration considerably slowing down, and to a certain extent, shutting down the external borders of the European Union (Mijalković, 2016). This meant that migrants had to spend some time in shelters and asylum centers in the countries of the Western Balkans. That is why the fear of refugee terrorism has risen unjustly because "migrants have become more visible for the citizens of the Western Balkans".

Therefore, the general conclusion is that the territory of the Western Balkans, generally speaking, is not a desirable destination for life even of the many who are born there (and who are trying to legally or illegally emigrate), let alone migrants from faraway countries. More specifically, the Western Balkans is primarily an "emigration reservoir" for the countries of the West, the same as the Asian countries in which wars and conflicts are raging. At the same time, compared to emigrants from Asian countries, the Western Balkans is primarily a "transit zone" to the countries of the global West.¹⁴

In this regard, it is highly unlikely that a significant number of refugee migrants will be settled in the Western Balkans, and even less likely for them to do so in order to carry out terrorist attacks there. It is more likely that terrorists from the Syrian, Afghan, or Iraqi countries will target the geographical region of the Western Balkans as a separate task, with the sole purpose of committing terrorist acts. In this regard, it is not impossible for terrorists to infiltrate into the

columns of migrants, but none of these scenarios have so far (fortunately) happened (Mijalkovic, 2016).¹⁵

4. Conclusion

By means of a deductive analysis of the allegations from the previous parts of this paper, it can be concluded that (potential) terrorists, or bearers of other forms of political violence in the Western Balkans are: *extreme Albanians* from the territory of Kosovo and Metohija, Bujanovac, Preševo and Medveđa, from certain parts of Montenegro and Macedonia; *the so-called security forces of the so-called Republic of Kosovo* (mostly former members of terrorist organizations) that would enforce the decisions of the highest pseudo-state organs (most of them former leaders of the Kosovo Liberation Army); *radicalized Muslims (Islamists)* from the Raška region of Serbia, parts of Montenegro and Macedonia relying on Albania and Kosovo and Metohija, the Republic of Srpska and the Federation of Bosnia and Herzegovina; *Wahhabis* from the area of Raška region in Serbia, Montenegro and Bosnia and Herzegovina; *Mujahideen* in Bosnia and Herzegovina, and to a lesser extent in Kosovo and Metohija; *"Al Qaeda operatives"* in Bosnia and Herzegovina, Kosovo and Metohija, Raška region and Macedonia; *the so-called White Al Qaida*, from the territory of Bosnia and Herzegovina, Kosovo and Metohija, the Raška region and Macedonia; *the so-called European ISIL*, from the territory of Bosnia and Herzegovina, Kosovo and Metohija, Raška region and Macedonia; *the so-called foreign terrorist fighters* from Serbia, Montenegro, Bosnia and Herzegovina, Albania, Macedonia and Croatia; *migrants*, which is not theoretically impossible, but that has not happened so far.

From the presented list of proven and confirmed terrorists and bearers of other forms of political violence, it is most unlikely that a migrant would be found in that role. However, if something has not happened up to now, it does not mean that it is not impossible.

So, if refugee's terrorism is taken into account, and if a *migrant* is taken as the criterion of the risk analysis of terrorism, then we conclude that it is possible to find the following groups in the role of terrorists: *immigrants "from the last century"* - participants in armed conflicts throughout the territory of the former SFRY in the 1990s, which is very likely; *current immigrants or transit migrants* (foreigners) - members of Al Qaeda or ISIL who are infiltrated into convoys of migrants from the East through the territory of the Western Balkans, who are headed to Central and Western Europe, or intend to settle down on the territory of the Balkan region, which is less likely, but not impossible; *emigrants-returnees* - domestic citizens, at the same time foreign terrorist fighters, who are returnees from the battlefields in Afghanistan, Iraq, Libya, Syria or in some other country, which is very likely; *migrants of the so called second or third generation* (who were born in Europe, but whose parents or grandparents immigrated to Europe in the last century), who have become radicalized with some extremist ideology (Al Qaeda, ISIS, etc.), which is also likely;

¹³ Compare: *Serbia after closing the Balkan route*, Humanitarian Center for Intergration and Tolerance, Novi Sad, 2017, pp. 22–26; *SOCTA 2017 – European Union Serious and Organized Crime Threat Assessment – Crime at the Age of Technology*, 49.

¹⁴ Compare: *World Migration Report 2018*, p. 71.

¹⁵ Analyses indicate that refugee-migrants were almost not involved in terrorist attacks throughout Europe. One of the most famous terrorist attacks took place in Paris (suburb of Saint-Denis) on November 13, 2015 (the so-called Paris black Friday 13, French 9/11), when 129 people were killed, around 350 injured and substantial material damage was made. In fact, it is a matter of multiple synchronized terrorist attacks in 6 locations (*Stad de France* National Stadium, *Bataclan* Concert Hall and various catering facilities). Terrorists were radical Islamists, who were mostly living in Europe (France, Belgium), and only one terrorist was a Syrian citizen. It was established that before this event, terrorists had been in Syria, Pakistan and Iraq, where they participated in terrorist actions as volunteers and mercenaries. The Islamic State claimed responsibility for the attacks and declared that they were "retaliation for Syria." The aforementioned Syrian citizen came to France as a migrant refugee across the territories of Greece, Macedonia and Serbia.

The general conclusion is that the fear of refugees (migrants)-terrorists from Asia is unjustified, but that this option should in no way be ignored or underestimated. At the same time, for countries and peoples in the Western Balkans it would be more significant to devote themselves to the harmonization of relations, thus contributing to the prevention of existing political, ethnic and religious diversities and tensions, and thus of the conflicts most likely exhibited as terrorism.

5. Literature

1. *Albanian Terrorism and Organized Crime in Kosovo and Metohija, Government of the Republic of Serbia, Belgrade, 2003.*
2. Azinovic, V. Al Qaeda in Bosnia and Herzegovina: Myth or Real Danger? , Radio Free Europe, Sarajevo- Prague, 2007
3. Bajagic, M. Bosnia and Herzegovina in the Vortex of Radical Islamist Fanaticism, Extreme Wahhabism and Terrorism, Policy of the National Security, Institute for Political Studies, Belgrade, 2015, pp. 47- 82
4. ‘‘Balkan Peninsula ‘‘, available at https://sr.wikipedia.org/sr-el/Balkansko_poluostrovo, date of access 13. 8. 2018
5. Brzezinski, Z. *The Grand Chessboard: American Primacy and Its Geostrategic Imperatives*, Basic Books, New York, 1997.
6. Cvorovic, D. The public prosecutor and the police as key stakeholders pre-investigate the investigative stages of the new criminal procedure, In "Position and the role of the police in a democratic state", Academy of Criminalistic and Police Studies, 2013, p. 116
7. Cvorovic, D. *Deprivation and restriction of liberty by the police* (Doctoral dissertation), 2016, Belgrade: Faculty of Law.
8. Hajdú, Z. *Southeast-Europe: State Borders, Cross-border Relations, Spatial Structures*, Hungarian Academy of Sciences, Pécs, 2007.
9. Hamad, A. In the Network of Evil: International Terrorism and Al-Qaeda, Voice of Srpska, Banja Luka, 2007.
10. Hecimovic, E. G. Mujahedins in Bosnia and Herzegovina 1992-1999, Dan Graf and SEEMO, Belgrade, 2009
11. Huntington, S. P. *The Clash of Civilizations and the Remaking of World Order*, Touchstone, New York, 1996.
12. Lampe, J. R. *Balkans Into Southeastern Europe, 1914–2014: A Century of War and Transition*, Palgrave Macmillan, London, 2014.
13. Mijalkovic, S. *Suppression of Trafficking in Human Beings and Smuggling of Migrants*, Official Gazette and Institute for Comparative Law, Belgrade, 2009.
14. Mijalković, S. Nikač, Ž. Protection of National Interests of the Republic of Serbia in the Process of the International Integration, *Serbian Political Thought*, vol 2, Institute for Political Sciences, Beograd, 2012, pp. 273- 299.
15. Mijalkovic, S, Bajagic, M. Premises and guidelines for Drafting the National Strategy of the Republic of Serbia against Terrorism, In: *Suppression of the Contemporary Organized Crime and Terrorism VI*, Academy of Criminalistic and Police Studies, Belgrade, 2015, pp. 9-50.
16. Mijalković, S. Challenges To Identity in the Context of Terrorist Attack „Paris 2015“, *Security*, vol.1 , Ministry of Interior, Belgrade, 2016, pp. 24–45.
17. Mijalković, S. *National Security*, Academy of Criminalistic and Police Studies, Belgrade, 2018, pp. 169- 170.
18. Prorokovic, D. *Geopolitics of Serbia: Position and Perspectives at the Beginning of the 21st Century*, Official Gazette, Belgrade, 2012
19. SALJI BERIŠA Admitted: Albania armed the terrorists OVK ", available at www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:658453-SALJI-BERISA-PRIZNAO-Albanija-naoruzavala-teroriste-OVK from 3. 4. 2017. date of access 15. 8. 2018.
20. Schindler, J. Unholy Terror: Bosnia, al-Qa'ida, and the Rise of Global Jihad, Official Gazette, Belgrade, 2009.
21. Serbia after closing of the Balkan Route, Humanitarian Center for Intergration and Tolerance, Novi Sad, 2017.
22. Sikora, C. Z. A. *Organized Crime in Kosovo – Clan Structure – Main Links*, KFOR Material, available at <https://thebloodyyellowhouse.wordpress.com/organized-crime-in-kosovo/>, date of access, 15. 8. 2018.
23. SOCTA 2017 – *European Union Serious and Organized Crime Threat Assesment – Crime at the Age of Technology*, European Police Office, The Hague, 2017.
24. Švob-Đokic, N. (ed.) *Redefining Cultural Identities: Southeastern Europe*, National and University Library in Zagreb, Zagreb, 2001.
25. *The Global Study on Smuggling of Migrants 2018*, United Nations Office on Drugs and Crime, New York, 2018.
26. *World Migration Report 2018*, International Organization for Migration, Geneva, 2018.

THE IMPACT OF THE SECURITY SITUATION ON TOURISM IN THE COUNTRIES OF THE FORMER YUGOSLAVIA

Ing. Iveta Hamarneh, Ph.D., Mgr. Petr Jeřábek
Department of Tourism – University College of Business in Prague, the Czech Republic

hamarneh@vso-praha.eu

Abstract: Safety and security are vital in providing quality in tourism. More than any other economic activity, the success or failure of a tourism destination depends on being able to provide a safe and secure environment for visitors. The presented paper examines the impact of the security situation on the tourism sector in selected countries of the former Yugoslavia. Methods which were used for completing the paper include the literature review, content analysis of documents published by UNWTO, UNDP, WEF and IEP. Case studies for selected countries of the former Yugoslavia are also presented.

Keywords: SAFETY, SECURITY SITUATION, TOURISM

1. Introduction

To feel safe and secure is one of the basic needs of human beings is. Therefore an unexpected adverse event affecting essentials could lead to a crisis for a tourism destination. For this reason, an increasing number of tourism studies have focused on safety and security issues since 1970s. Events such as terrorist attacks, local wars, natural disasters, health scare of a rise in crime levels at a particular destination can lead potential visitors to evaluate whether or not they should change their travel destination or even cancel their entire traveling plans.

The tourism industry could not avoid the negative influences and consequences of these incidents. Moreover, some of these situations manifested the vulnerability of tourism on global, regional and local levels. Consequently, providing a safe and secure environment for visitors could determine the success or failure of a tourism destination.

Safety and security issues in the tourism sector came to the front by the evolution of mass tourism from the beginning of the 1950s. The main reasons for determining this evolution process are enumerated hereinafter:

1. Travel and tourism is not anymore an activity of a narrow social stratum or class but the whole widening middle class is getting progressively involved into it. This is a direct result of the growth of personal incomes and free time in developed countries.
2. Tourism scope covers more and more countries and regions in the world and not only highly developed countries enabled to generate out-going tourism flows are getting involved in tourism but also countries of the so-called third world. For them, tourism is part of their economic development strategy.
3. The rapid and scenic development of transport (aviation, automotive industry) contributed to the rise of geographical mobility.

Due to these reasons, the safety and security issues gained a higher and higher importance as the tourism itself became one of the largest industries in the world economy (contribution to the GDP, number of people employed in the sector, the extent of investments into the tourism industry etc).

2. Methodology

The presented paper examines the impact of the security situation on the tourism sector in selected countries of former Yugoslavia.

The analysis and data presented in this paper are based on secondary research and are focused on Slovenia and Montenegro, two countries with high tourism potential. These countries started, from a tourism aspect, to play an essential role in the region.

Objectives of the paper are:

- to characterize the terms of safety and security in the tourism sector.
- to evaluate safety and security situation in selected countries of former Yugoslavia according to chosen indicators.
- to assess the impact of the security situation on the tourist arrivals in decided countries of former Yugoslavia.

Methods which were used for completing the paper include the literature review, content analysis of documents published by United Nations World Tourism Organization (UNWTO), United Nations Development Programme (UNDP), World Economic Forum (WEF), and Institute for Economics and Peace (IEP). Case studies for selected countries of the former Yugoslavia are also presented.

For assessment of safety and security situation in selected countries, the following indicators were used: Global Peace index (presented by IEP), Global Terrorism Index (submitted by IEP), Human Development Index (presented by UNDP), and Travel and Tourism Competitiveness Index (presented by WEF).

Global Peace Index [1] measures the relative position of nations' and regions' peacefulness. The GPI ranks 163 independent states and territories according to their levels of peacefulness. The GPI covers global peace using three broad themes: the level of societal safety and security, the extent of ongoing domestic and international conflict and the degree of militarization. Factors are both internal such as levels of violence and crime within the country and external such as military expenditure and wars.

Global Terrorism Index [2] gives a general summary of the critical global trends and patterns in terrorism since 2000. It presents a composite score to provide an ordinal ranking of countries on the impact of terrorism. It is an attempt to systematically rank the nations of the world according to terrorist activity. The index connects some factors linked with terrorist attacks to build an explicit picture of the impact of terrorism, illustrating trends, and providing a data series for analysis by researchers and policymakers.

Human Development Index [3] provides a composite measure of well-being. All countries included in the HDI are classified into

one of three clusters according to achievements in human development: high, medium, or low. Many important aspects of human development relate also to people's security: loosely defined as people's freedom from fear and freedom from want in a broad sense.

The aim of the Travel and Tourism Competitiveness Index [4] is to provide a comprehensive strategic tool for measuring the set of factors and policies that enable the sustainable development of the travel & tourism sector, which in turn, contributes to the development and competitiveness of a country. Safety and security pillar of TTCI measures the extent to which a country exposes tourists and businesses to security risks mainly related to severe harm to people (violence and terrorism), petty crime is not taken into account.

3. Safe and security issues in the tourism sector

The sense of the terms safety and security differs considerably depending on the context in which it is being used and the researcher's discipline, leading to potential uncertainties. Linguistics and interpretation are responsible for some of the uncertainty [5].

The Oxford Dictionary [6] defined safety as "the condition of being protected from or unlikely to cause danger, risk, or injury," whereas defined security as "the state of being free from danger or threat". In tourism literature, the terms "safety" and "security" are usually used interchangeably as twin concepts.

According to Progress Report to the UNWTO Committee on Tourism and Competitiveness [7]:

- Safety is the set of precautions put in place to prevent tourists and industry workers from being exposed to situations where they believe that they are in personal danger, due to crime, accidents, and emergencies.
- Security is the set of precautions put in place against hostile acts that seek to inflict a large scale of damage resulting in maximum economic disruption or measures taken to guard against espionage or sabotage, crime, attack or escape.

The accumulated evidence throughout the world shows that the impact of security incidents on the tourism industry, the destination, the local community, and the visitors are, in most cases, negative and multifaceted. Consequently, impact concepts are grouped into six subgroups [8] depicting different facets of the impact of the security situation on tourism. Each subgroup of concepts also includes commonly used variables that measure these impacts (see Table 1).

Table 1: Impact concepts

Type of impact	Some variables used for the purpose of assessing the impact of security incidents
Impact on the destination itself	Tourist overall arrivals in a given period Tourist segmented arrivals in a given period Tourist overall receipts in a given period Tourist segmented receipts in a given period Duration of impact (crisis) Destination life cycle
Impact on tourist's behavior	Intention to travel to the affected destination Actual cancellations Actual bookings Actual avoidance of unsafe destinations The risk-taking tendency of various tourist segments Perceived vulnerability to specific types of crimes Characteristics of tourist image projection Familiarity with safe and unsafe areas within a given destination
Impact on the tourism industry	Evacuation of tourists by tour operators Local investor's behavior Human resource restructuring behavior Inclusion/exclusion of destination in tour operators' brochures Cost of doing or ceasing doing business Profitability Projection of destination image of tour

	operators The extent of economic interest in the tourism business at the destination
Impact on host governments	Changes in level of security measures in affected destinations Changes in short-, medium-, and long-term government policies towards tourism The extent of governmental direct/indirect operational involvement in tourism The extent of governmental direct/indirect financial involvement in tourism The extent of governmental direct/indirect marketing involvement in tourism
Impact on governments of generating markets	Availability of travel advisories in given generating markets The level of exposure to travel advisories in generating markets Position on travel advisories' risk scale The frequency of travel advisory updates
Media Behavior	The extent of coverage of the incident Types of media coverage Relative coverage of security situations of media platforms The impact of media warnings The extent of media messages directly aimed at potential tourists.

Source: [8]

Safety and security are vital to providing quality in tourism, and should be an overriding objective of tourism destination. According to Holloway [9] the issue of safety and security is also important to the image of a tourist destination and for visitor satisfaction.

The four possible generators of a given security situation [10] that might harmfully impinge on the tourism system are: crime-related incidents, terrorism, war, social and political unrest.

Many authors argued that the absence of crime was significant for the tourism sector in any country [11]. Crime is defined as an action or behavior that qualifies as the crime by the order of law [12]. A crime may occur in different locations and different situations, such as crimes committed by local residents against tourists, crimes committed by tourists against local residents, crimes committed by tourists against other tourists and planned crimes against tourism entities [13].

Tourism represents an integral part of the globalization [14], the terrorism embodying its darkest side. As a result of the globalization process, tourism and terrorism became inevitably linked. By accessing the most advanced destruction technologies terrorist threats and consequences of terrorist attacks have become more powerful and effective than ever before. Recent terrorist activities caused the rise of conservative measures at the airports and national borders. Thus tourism is being affected as well. On the other hand, many tourist attractions are positioned close to politically and nationally essential elements or statues; hence, tourist became an easy terrorist target [15].

Irrespective of their origins and backgrounds, wars require a great influence on the tourism demand, not only in close but wider areas if not on a global scale. As opposed to the terrorist attacks war breakouts affect wider regional areas and have far greater consequences on tourism than the terrorism [10].

Social and political unrests appear as military coups, violent demonstrations, uprisings and other forms of resistance. There are many potential reasons for such events (e.g., incompetent government, corruption, abuse of political power, weak state institutions and lack of responsibilities by the public sector) and in many cases they lead to the disintegration of the country or at least to collapse of the government. The latter is ideal for the development of war situations, terrorist actions, weapons smuggling and organized crime, which are all essential factors for the development of insecure image thus affecting general attractiveness. These and similar social events or unrests will result in the drop of international arrivals [10] irrespective of the real level of threats to the tourists. Social and political unrests as well as minor indications to that will result in booking cancellations and amendments. Amendments usually reflect in transfers to other destinations and

will negatively damage destinations under pressure as well as their close neighboring countries or regions.

4. Results and discussion

The development of tourism in the countries of former Yugoslavia has longstanding tradition. After the Second World War, Yugoslavia became popular for both, tourists from capitalist and socialist countries, since it offered not only the seaside and mountain tourism, but also remarkable blend of cultures having exotic effect in Europe. However, what seemed to be advantage for competitiveness in tourism turned into detonator of the war after the dissolution of Yugoslavia. During 90's the number of tourist arrivals and tourism receipts declined rapidly. Just after 2000 has turned the situation around with dominant position of Croatia and in the last decade the other countries of Western Balkan region has already started playing important role in tourism. The fastest growing importance of tourism for economy in the region has turned up in Slovenia and Montenegro. Besides the tourist attraction the safety of the destination plays very important role for visitors coming to country.

Slovenia as Destination of Tourism

Slovenia belongs to the richest country of the former Yugoslavia. In frame of tourism it offers many nature sights comprising of the Alps, Triglav National Park and short part of seaside. Apart from this, Slovenia is very well known for the vast area of karsts which belong to one the largest in the world. Ljubljana, capital of Slovenia, is also popular especially for its modern Plečnik's architecture stretching to the first half of the twentieth century. Nevertheless, the country has been in shadow of Croatia for a long time and served as transit country for tourist going to Croatian coastline.

While the period of the 2008 – 2011 global economic crises caused the decline of arrivals and receipts in tourism, it has recovered very quickly. However, in the case of Slovenia, the situation was more difficult since the country was affected by 2015 migrant crisis and Eurozone crises which nearly lead to bailout. Still Slovenia has achieved to maintain stable growth of arrivals since 2011. On the other hand, the amount of receipts stagnated which is result of the economic crisis as well as composition of foreigners who come to Slovenia and specification of tourism (see Table 2). The most tourists come from Italy, Germany, Austria, the Netherlands and Croatia. As for reasons why staying in Slovenia belong Health/Spa Tourism, Seaside or Cultural Tourism. Very high position has also Mountain Tourism which represents 26 % of all these types and is the most dynamic from all of them [16].

Table 2: Arrivals and Receipts in Tourism in Slovenia

Slovenia		
	Arrivals (mil.)	Receipts (USD/mil.)
2017	3,586	2,750
2016	3,032	2,424
2015	2,707	2,328
2014	2,411	2,737
2013	2,259	2,713
2012	2,156	2,580
2011	2,037	2,749

Source: [17]

Besides the cross-border tourism, the domestic tourism play more important role than decades ago. In case of Slovenia 26,5 % of tourist in last year were of domestic origin (STO, 2017). Domestic tourism is becoming very significant in all European countries which reflect the security situation in Europe. More and more tourists decide about their holidays in accordance with how secure the destination is. Due to this fact many tourists prefer their home countries, especially if they are considered to be secure.

Regarding to Slovenia, the country represents one of the most secure country in the world which reflects the situation in the whole Central European region. According to the GPI, with only one exception of period between 2013 and 2015, Slovenia has always belonged to ten most peaceful countries (see Table 3). The above-mentioned period was the most critical time in the Slovenian modern history, since the country was deeply affected by both, economical and migrant crisis. The later data, however, show that it was temporary situation. If we compare the GPI with GTI the risk of terrorism attack in Slovenia is low, which confirm the fact that this country belongs to the safest in the world.

Scoring in HDI brings also the view how the country can deal not only with development, but also with security. From the post-communist countries, Slovenia features to highest index. High level of living standard goes back to time of former Yugoslavia since specific form of communism with the combination of traditional contacts of Slovenes with Austrians and Italians help to overcome transformation difficulties. Due to this facts Slovenia has achieved not only to stabilize, but also to improve the living standards. As validate the data from Table 3 there is close relation between level of development and level of security.

The previous analysis can be questioned by TTCI index since Slovenia has declined in the last years. However, this index, comprising of fourteen pillars, evaluates wide range of realm of tourism. Regarding to security, which is under pillar two, Slovenia scored 6,20 and 17th position (TTCR, 2017). That means the second best result among the entire considered pillar. In contrast with whole TTCI index, in the pillar two Slovenia has improved its position and confirmed its belonging to the group of the most secure state in the world.

Table 3: HDI, GPI, GTI and TTCI Indicators

	Slovenia			
	HDI-UNDP	GPI	GTI	TTCI
2018	0,896 (25)	1,396 (11)		
2017	N/A	1,364 (7)	(134)	4,11 (41)
2016	0,890 (26)	1,408 (10)	(130)	N/A
2015	0,880 (26)	1,378 (15)	(124)	4,17 (39)
2014	0,874 (25)	1,398 (13)	(124)	N/A
2013	0,874	1,374 (13)	(124)	4,58 (36)
2012	0,874	1,330 (8)	(122)	N/A
2011	0,873	1,358 (10)	(122)	(33)

Source: [18]; [19]; [20]; [21]

Montenegro as Destination of Tourism

Montenegro is one the youngest state in Europe. It proclaimed its independence in 2006 after the successful referendum. As a part of Federation of Serbia and Montenegro the country suffered deeply from the consequences of sanctions due to the War in Bosnia and Herzegovina and Kosovo crisis in the 1990's. Just breaking-up the federation has brought the new impulse for development of tourism in Montenegro. The country offers not only intended coastline with a lot cultural and nature sights, but also the four national parks

which are also the aim of tourism. Apart from that Montenegro proclaimed itself as “first ecological state” in 1991 [22].

The unilateral acceptance of euro as national currency was also an impulse for tourism development. Despite the deep global economic crisis and followed crisis in Euro zone, Montenegro suffered more from the consequences of war period. Therefore the period of recovery meant for this small Adriatic state beginning of the new phase of tourism. As seen from the Table 4, the numbers of arrivals and receipts have grown constantly for last seven years. Tourists from Russia, who were the largest group of foreigners travelling to Montenegro, supported the majority of this success story. Russians belong to the most important investors in Montenegro as well. These investments play important role in tourism since many seaside resorts were reconstructed in the last couple of years. However, from the latest research come out that most tourists in Montenegro are from Albania (21,2 %), Serbia (16,5 %) and Israel (7,3 %). Russians comprises only 3,2 % all tourists and overnights [23]. The main aim, which creates more than half of arrivals, is realised in seaside areas. The rest of are situated in the capital Podgorica and mountain resorts.

The domestic tourism plays also important role in Montenegro. The existence of both, seaside tourism in summer and mountain tourism in winter with combination of short distances, create ideal conditions for it.

Table 4: Arrivals and Receipts in Tourism in Montenegro

Montenegro		
	Arrivals (mil.)	Receipts (USD/mil.)
2017	1,877	1,041
2016	1,662	925
2015	1,560	902
2014	1,350	906
2013	1,324	884
2012	1,264	826
2011	1,201	862

Source: [17]

As for security, Montenegro has dynamically improved its position in last years. Although it does not represent the safest places in the world, according to GPI and GTI, still, tendencies are positive. Moreover, in comparison with rest of the Western Balkan countries, Montenegro is the second safest country after Croatia (GPI, 2018). The main reasons of this success come from reassurance after the wars in 1990s, successful achieved independence and sustainable economic growth of the country. No less relevant role plays the negotiation process of EU's accession that pushed the country to realize necessary reforms.

In HDI Montenegro became for the first time the country with very high human development in 2015 (see Table 5). After Slovenia and Croatia, it represents the third country with this result. The tourism, which performs significant role in all three countries, creates not only the working places, but also brings capital that help to improve economic, social and safety situation, and general standard of living.

Regarding to TTCI the position of Montenegro can be questioned as in the case of Slovenia (see Table 5). Generally it exposes that competitiveness in tourism is weaker than it used to be in last seven years. However, the results of each pillar differs. While in the case of safety and security holds Montenegro 75th position, the worst results were recorded in culture resources and business travel and in international openness. On the other hand, there were seven pillars where Montenegro scored better than in security.

Overall, it is possible to state that even in TTCI safety and security pillar Montenegro improves year from year (TTCR, 2017).

Table 5: HDI, GPI, GTI and TTCI Indicators

	Montenegro			
	HDI-UNDP	GPI	GTI	TTCI
2018	0,814 (50)	1,893 (58)		
2017	N/A	1,950 (67)	(123)	3,68 (72)
2016	0,807 (48)	1,884 (57)	(117)	N/A
2015	0,802 (49)	1,854 (57)	(103)	3,75 (67)
2014	0,789 (52)	1,860 (55)	(86)	N/A
2013	0,787	1,976 (73)	(124)	4,50 (40)
2012	0,787	2,006 (81)	(116)	N/A
2011	0,784	2,113 (89)	(113)	(36)

Source: [18]; [19]; [20]; [21]

5. Conclusion

Tourism is one of the significant economic pillars of many world countries and, additionally, more and more countries admit that. The number of people being able to afford traveling rises not only due to personal income but also due to changes in the supply market. The world became the so-called global village, however not always with positive consequences. Security issues around the globe affect tourism industry on local as well as global level, not only by reducing demand but also guiding it, hence causing over or under demand pressures. Crime, wars, social and political unrests, environmental threats and the spread of infectious diseases are just some of the most common forms of threats to safe and secure tourism. All forms of security incidents have negatively affected their image and can cause a decline in tourist arrivals.

Peace, safety, and security are the primary conditions for successful tourism development. This statement is confirmed by the tourism development of two countries of former Yugoslavia - Slovenia and Montenegro. According to the data of UNWTO is identified the stable growth of arrivals since 2011 in both analyzed countries. This steady growth is caused, among others, the safety, and security situation in Slovenia and Montenegro. In accordance with the data of UNDP, IEP, and WEF Slovenia belongs to the group of the safest country in the world and Montenegro has dynamically improved its position in last years as regards the security situation.

In general, it can be concluded that security is a basic predisposition for prospective destination development, however, it is not the only one. Stakeholders and experts of tourism recommend assigning tourism resources, tourism infrastructure, the variety of tourism services, tourism management, virtual environment, the quality of tourism services, the image of tourism destination, and the events to the development factors of a tourism destination. From this point of view, it can be stated that Slovenia, as well as Montenegro, have good conditions for future tourism development.

6. References

- [1] *Global Peace Index*. [online]. IPE. [quoted 15. 11. 2018]. Available at: <http://economicsandpeace.org/reports/>.
- [2] *Global Terrorism Index*. [online]. IPE. [quoted 15. 11. 2018]. Available at: <http://economicsandpeace.org/reports/>.
- [3] *Human Development Reports*. [online]. UNDP. [quoted 15. 11. 2018]. <http://www.hdr.undp.org/>.
- [4] *The Travel and Tourism Competitiveness Report 2017. Paving the way for a more sustainable and inclusive future*. [online].

- [quoted 15. 11. 2018]. Available at: http://www3.weforum.org/docs/WEF_TTCR_2017_web_0401.pdf.
- [5] M. B. Line, O. Nordland, Røstad & I. A. Tøndel, Safety vs. security? In Stamatelatos, M. G. & Blackman, H. S. (Eds.) *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management*, New Orleans 2006.
- [6] Oxford Dictionary. [online]. [quoted 15. 11. 2018]. Available at: <https://en.oxforddictionaries.com/>, 2018.
- [7] *Project to enhance the understanding of the factors that explain Destination Competitiveness*. [online]. UNWTO. [quoted 15. 11. 2018]. Available at: https://www.mincetur.gob.pe/wp-content/uploads/documentos/turismo/publicaciones/CTC_ALTA.pdf, 2016.
- [8] Y. Mansfeld & A. Pizam, *Tourism, security and safety: from theory to practice*. New York: Routledge 2011. ISBN 13: 978-0-7506-7898-8.
- [9] J. C. Holloway, *The business of tourism*. (7thed). Harlow, England: Pearson 2006.
- [10] Y. Mansfeld & A. Pizam, *Tourism, Security & Safety*. Oxford: Elsevier Inc. 2006.
- [11] N. Mthembu, *Tourism crime, safety and security in the umhlathuze district municipality, kwazulu-natal*. Unpublished doctoral dissertation, Faculty of Arts in Partial Fulfillment of the Requirements for the Master's in Recreation and Tourism at the Department of Recreation and Tourism, University of Zululand 2009.
- [12] S. Shafer, *Introduction to Criminology*. Reston. VA: Resto, 1967. In Gray, C.M., 1979. *The Cost Of Crime*. Beverly Hills. Sage Publication Inc. 1979.
- [13] V. S. Prashyanusorn, Kaviya & P. P. Yupapin. *Surveillance system for sustainable tourism with safety and privacy protection*. *Procedia - Social and Behavioral Sciences*, 2(1): p. 74–78 2010.
- [14] E. P. Tarlow, A Social Theory of Terrorism and Tourism. In Y. Mansfeld and A. Pizam (Ed.), *Tourism, Security & Safety* (p. 33-48). Oxford: Elsevier Inc. 2006.
- [15] B. Faulkner, Towards a framework for tourism disaster management. In *Tourism Management*, 22, p. 135-147 2001.
- [16] *Slovenian tourism again with record-breaking results in 2017 – the challenge is to increase the added value*. [online]. STO. [quoted 15. 11. 2018]. Available at: <https://www.slovenia.info/en/press-centre/press-releases/8238-slovenian-tourism-again-with-record-breaking-results-in-2017-the-challenge-is-to-increase-the-added-value>.
- [17] UN World Tourism Organization. *Highlights 2012 – 2018*. [online]. [quoted 15. 11. 2018]. Available at: <http://marketintelligence.unwto.org/publication/unwto-tourism-highlights-2018>.
- [18] United Nations Development Programme. *Human Development Indices and Indicators 2018*. Statistical Update, New York. [online]. [quoted 15. 11. 2018]. Available at: http://hdr.undp.org/sites/default/files/2018_human_development_statistical_update.pdf, 2018.
- [19] Institute for Economics & Peace. *Global Peace Index 2018: Measuring Peace in a Complex World*, Sydney, June 2018. [online]. [quoted 15. 11. 2018]. Available at: <http://visionofhumanity.org/reports>, 2018.
- [20] Institute for Economics & Peace. *Global Terrorism Index 2017: Measuring and understanding the impact of terrorism*, Sydney. [online]. [quoted 15. 11. 2018]. Available at: <http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf>, 2017.
- [21] World Economic Forum. *Travel and Tourism Competitiveness Index*. Paving the way for a more sustainable and inclusive future, Geneva. [online]. [quoted 15. 11. 2018]. Available at: http://www3.weforum.org/docs/WEF_TTCR_2017_web_0401.pdf.
- [22] *Voluntary National Review 2016. Montenegro*. [online]. [quoted 15. 11. 2018]. Available at: <https://sustainabledevelopment.un.org/memberstates/Montenegro>.
- [23] *Foreign tourist arrivals to Montenegro rise 19.2% in 2017*. [online]. BISE. [quoted 15. 11. 2018]. Available at: <https://seenews.com/news/foreign-tourist-arrivals-to-montenegro-rise-192-in-2017-600141#sthash.fQkkmBEg.dpuf>.

THE ROLE OF HUMAN RESOURCES DEPARTMENTS IN CREATING THE SECURITY SYSTEM – THE OUTLINE OF THE PROBLEM

M. Dąbrowska-Świder. Msc.

Faculty of Logistics – Military University of Technology, the Republic of Poland
malgorzata.dabrowska-swider@wat.edu.pl

Abstract: *The article presents the direction of development of contemporary human resource management and the use of the human potential in the defense system based on human–employee as the capital of modern organization.*

Keywords: HUMAN RESOURCES, SECURITY SYSTEM, HUMAN CAPITAL, FACTOR STRENGTHENING DEFENSE

1. Introduction

The importance of the role of human resource management departments (less often referred to as personnel management) has been pushed into the background for several decades. This has been mainly determined by the economic deliberations that placed the best possible use of manpower to the foreground in order to achieve profit and were brought down to the search of new ways of its effective use. The human relations movement was born at the beginning of the 20th century and for a number of years was a popular approach to management, and Abraham Maslow and Douglas McGregor greatly contributed to its development [1]. The development of the organization in the continuously altering environment and the increase in the awareness and competence of the managerial staff caused that the person responsible for the human resources matters is currently directly subordinate to the managing director, and the strategic plans concerning the activities of the organization are closely related to the plans on the employment of employees.

2. The role of personnel departments in the light of the changing conditions of the functioning of contemporary organizations.

The awareness of people responsible for the functioning of modern organizations means that at the moment the recognition of significant individual characteristics of each human being as unique and enhancing the value of each organization constitutes its most important part in the form of human capital, which consists of knowledge, qualifications, skills, competences and experiences. Having specialized employee personnel increases the competitive advantage in the modern economy. Acquiring, improving and keeping the necessary employees is the subject of human resource management. In the subject literature, two models of human resource management are cited most often: the Michigan model and the Harvard model [2]. The first of them was created in the eighties, when a strategic approach to the personnel function started to emerge. The Michigan model puts the overriding role of the company's strategy in the foreground in relation to the organizational structure applicable to the use of the personnel potential of a given organization. The basic functions of human resource management resulting from this model include: selection of employees, assessment of their work, rewarding and development. Each of these functions is related to the others by creating a resource cycle. The one-way flow of data from the environment to the organization is the weakness of this kind of solution, as well as the flow of information from the mission and strategy to the organizational structure and human resource management. In addition, the focus of the organization's management on the creation of such a kind of connection between the formal structure and the human resources system can be noticed to affect the implementation of strategic goals of the organizational unit. The Harvard model takes into account the pressure of various factors affecting the organization and appreciates the involvement in the management process of line managers and the perception of human resources affecting the strategic development of the company. The Harvard model takes into account the following

areas: employee participation, employee mobility called the personnel fluctuation (moving, firing, hiring employees), reward systems (wages, shares, stimuli) and work organization. In this model, it was assumed that the above-mentioned areas are of interest not only to employees, but also to external participants of the organization (e.g. shareholders), as well as being under the influence of external factors, such as the broadly understood environment of the organization in the form of the labour market situation or applicable legal conditions. This concept of management also shows what effects the decisions made based on the arrangement of interrelations and relationships between people and situational factors in the organization cause. The presented management models affect the theory and practice of management, but mostly they constitute the beginning to conduct research in many other countries including the economic situation, traditions and experience, as well as cultural factors occurring in a given country.

In American organizations and in European Union member states, there were no problems with shaping the importance of the function of managing human resources with all the elements that make up this area in the awareness of the managerial staff. These include: human resources planning starting from the analysis of a single workplace by forecasting future employment, to obtaining employees from among the employees or from outside the organization based on the application of modern methods of candidate evaluation. Another key element is the continuous work inside each organization on the improvement of own resources by enabling employees to work in positions adapted to their skills and in the future to carry out tasks at other workplaces based on the improving training and continuous evaluation for the development of employees through promotions and raises. Determining the remuneration system in such a way as to provide adequate incentives to encourage better and more efficient work and to establish a good non-wage benefits program as a means to keep or attract employees is an extremely important element.

The comparative research conducted in 2000 on a sample of managers from non-European Union countries (Poland, the Czech Republic, Norway) allowed to establish that also for them building a competitive advantage on the EU market is possible based on qualifications, employees' experience and knowledge about the needs of customers, competitors and own position on the market [3]. It is worth noting that over the last two decades, there has been a significant development of departments responsible for personnel policy from administrative functions to a personal approach, the main essence of which is the recognition of an employee as an individual subject with specific skills, competence, personality traits that should be properly used, giving the right direction of development within the set program, catching the appropriate talents and predispositions to perform specific tasks or activities at specific positions. Adopting such an approach confirms the recognition of a man as the most valuable element-resource from among all owned by each organization. Currently, it is becoming more common to use the wording of human capital in place of the existing human resource, which constitutes the expression of respect for each employee.

3. *Man – employee as a capital of modern organization*

Contemporary theories referring to people's management make everyone aware that the most important intangible resources of any organization include knowledge, relations with clients or business partners, and the creation of a distinctive organizational culture. Therefore, the basic objectives of each organization include the creation of such an administrative functioning mechanism that would allow for proper recording of such elements in such a way so as not only to be able to store this kind of knowledge, but also to acquire it from the members of the organization and to pass it on to the employed personnel for its further use. Another key element of this concept is to create such an organizational structure that would encourage employees to share their knowledge with other members of the organization without fear that after its acquisition they will no longer have an important role in the organization, and the employer will recognize them as useless and will be able to get rid of them easily. This kind of thinking leads many employees to keeping their "secrets" only for themselves and thus extending their career in companies. Often, there are situations in which outstanding specialists or experts blackmail their current employers, not only with the mere fact of going to the competition, but also by sharing their knowledge. Developing a model of a high organizational culture in this situation is the only form of protection against this type of behaviour.

Human capital differs from other forms of capital (economic, social, structural, organizational, intellectual, client, etc.), and its basic elements include: messages, experience, skills, abilities/features, attitudes, intellectual attributes (team work, creativity, innovation, creative thinking), motivation, health, values and ethical norms, potential for development, etc. [4] From among many definitions of human capital, the one developed by M. Juchnowicz is noteworthy, which says that *"the currently possessed and potential knowledge, embodied in the person of the employee, useful to the employer on the basis of specific employment relations"* [5]. On the basis of this type of approach to the human factor, the treatment of contemporary organizations as knowledge organizations is revealed, so those whose main purpose is to use the fully owned knowledge, inspire their members to continuous learning and broadly understood improvement at the level of individual, team and whole organization's activities. D. P. Lepak and S.A. Snell believe that effective personal policy should be based on two fundamental criteria: the value and uniqueness of human capital [6]. Whereas, the value of human capital concerns its suitability for the organization in the area of building a competitive advantage or reducing potential threats. Employees create an added value in the company if they cause the reduction of its costs or provide greater benefits to customers. The uniqueness of human capital refers to the degree of difficulty of duplicating employee skills by the organization's competitors. It includes specific skills of particular people with the so-called personalized knowledge, which is the result of own experience, skills, value systems and intuition.

4. *Features of traditional and modern organizations*

Modern organizations operating in a dynamic environment, which consists of many factors of an economic, legal, social, demographic, economic and geopolitical nature, operate under constant pressure to achieve goals, such as: maximizing profits, market value and sales based on cost minimization. When comparing traditional and modern organizations – based on knowledge, the latter requires flexibility in the process of acting and constant responding to changes. The following criteria are to serve this purpose: flattening the organizational structure and limiting the role of hierarchy, focusing on personnel development by maximizing its potential, delegating the authority with a high degree of building mutual trust, tolerating risk in the organization's activity and developing options for its occurrence instead of following procedures to its elimination, planning the career of employees,

drawing conclusions from mistakes made, and not only searching for those guilty and drawing sanctions against employees, replacing the ill-conceived loyalty often brought down to professionalism, integrity and entrepreneurship. In terms of shaping development factors, focusing on knowledge that is of paramount importance to tangible factors, responding to individual customer needs and searching for new preferences, meeting market demands, building relationships between organizational units and between companies, dynamic development for the future, and finally, placing the adaptation of market processes over marasmus, a sense of stability and security, and searching for specialists with high competences and the need for lifelong development. Given the above conditions, it cannot be concluded that a modern organization is a new approach to the achievement of goals based on strong human resources.

5. *The use of the organization's human potential as a factor strengthening defence.*

Human capital cannot be bought as is the case for any tangible good, but it can certainly be created and refined through the use of tangible goods and services of other people, and by sacrificing time. The role of human resources cells in the contemporary organization is not subject to discussion, and certainly is an integral part of any organization and not only performing functions related to the recruitment processes, employee development, employee assessment in the context of information exchange between them and their supervisors, but also plays a fundamental role in terms of creating missions and strategic goals of each organization by creating intangible resources. Together with tangible resources it creates assets, which in turn determine the value of the company. Because it is very difficult to estimate intangible values, it is nevertheless assumed that they amount to 85% of the average market value of a modern company. In the case of companies based on knowledge, this factor has an ever higher value. Such companies are market precursors in the field of implementing and introducing modern recruitment methods, new practices and solutions eagerly reproduced and absorbed by the market, new development programs, modern methods of remunerating and motivating employees, building the company's image and acquiring talents. Personnel departments in modern organizations have knowledge resources for employees in the form of information contained and recorded in IT programs. On the basis of the information available, it is possible to group all employees based on a uniformly accepted scheme, which should also take the form of a well-formulated uniform template. The list of data necessary to complete it would be developed at the central administration level and directed there after proper completion by the personnel department. This raises the basic question of what a template should contain. First of all, the education and knowledge of the employee in terms of education. In this way, a group of mechanical engineers, computer engineers, construction engineers, chemical engineers, transport engineers and many other scientific disciplines emerge. Another key information would concern the practical skills of the employee, e.g. the level of proficiency in the field of foreign language skills, and the central register of people with specific skills appears on this basis. It is similar in the case of determining the type of a driving licence owned. The next required information would refer to the skill of using weapons, knowledge of martial arts, first aid skills, membership in sports clubs, shooting clubs, hunting clubs, etc. At the same time, it should be stipulated that all persons providing this type of data would be confidential, intended for use only by relevant state administration authorities and only in the case of crises, conflicts and threats to the subject's security (state, nation, organization) of a military and non-military nature. Additional important information obtained would be related to the psychophysical features mainly associated with cooperation and dealing with people (e.g. physical fitness, creativity, team work skills, reaction to stress situations, ability to comply with specific rigours, leadership skills, openness and cognitive curiosity, analytical skills, responsibility and reliability, communicativeness,

insight, inquisitiveness, etc.). The list of desirable psychophysical features, referred to as soft competences, would require than an appropriate team of psychologists and experts should be appointed for its development. On this basis, we would receive further important reports on the potential of predictable behaviour.

The weakness of the currently used IT programs with a nationwide range is the single-track aspect of data collected by them. For example, the program for payers of contributions, PŁATNIK, which collects information related to the maintenance of a database on future pension benefits or the E-Deklaracja program collecting information closely related to paying taxes. As it can be seen, nobody tried to create a database that collects the necessary information raising the level of state defense. This is obviously a huge challenge for the whole defense system, but in the era of available organizational and technological capabilities of each country, it is certainly possible by completing one additional form by each employee, properly formulated, at the time of employment. Of course, at this point the question arises about the responsibility for maintaining the current base of employees because this is related to the need to expand the rights of personnel departments with this additional function. The evolution of human resources management, which takes place before our eyes, is accelerating and, as it can be seen, it must meet the increasing challenges of the 21st century. This can be especially noticed in the case of global corporations that are able to cope with the huge flow of information.

6. Conclusion

Modern organizations are aware of the importance of having valuable human capital, which is a tool for effective implementation of the strategy, as well as allows for taking full advantage of opportunities coming from the environment and enabling effective elimination of threats. Human capital is currently defined as the main success factor for an organization that contributes to achieving a competitive advantage. The basic task of modern organizations is to properly manage the category of human capital. The applied methods of managing employees constituting the element of organizational capital significantly affect the shaping of human capital. The style based on the participation of employees in decision-making processes is an additional element conducive to the development of human capital. Unfortunately, many managers have high concerns about delegating part of their tasks to employees. Managers play an important role in the effective shaping of human capital, or rather leaders who themselves strive for self-education, thus setting an example to subordinate employees. An effective manager knows that in a modern organization you need to share power and build it on the basis of mutual understanding and cooperation. The participation of tasks allows the management to open up to suggestions and ideas of employees. Thanks to this, it is possible to use and stimulate an important element of human capital, namely the ability to creativity, which is an invaluable source of innovation in the organization. As part of the participatory leadership style, hierarchical relations get flattened, which leads to a faster flow of knowledge and information among the members of the organization. The creation of an appropriate system of motivation and stimulation of job satisfaction is an important element of the process of shaping human capital. An important goal of motivating is to ensure that the most valuable employees remain in the organization, contributing largely to the organization's success. Keeping the employees is directly related to the retention of knowledge they have. In addition, if an investment has been made into these employees earlier, through appropriate training, their leaving is directly related to the loss of profits that will be attributable to the next employer. The organization's management bears the main responsibility for introducing effective ways to motivate employees. These activities should, above all, create appropriate working conditions and ensure adequate remuneration for employees' work. Encouraging employees to develop the entrepreneurial spirit and commitment is also an indispensable element. Motivational policy should take into account both the development of employees and provide economic aspects (cash

rewards, additional benefits, insurance and other) as well as non-economic ones (intangible, promotions, atmosphere, building career paths of employees, distinctions and praise). Motivating constitutes activities related to the optimal use of professional qualifications of employees and has a great impact on building trust and creating positive attitudes of employees in the organization [7]. The identification of existing barriers and limitations that may arise during the implementation of this process is the key to effective management of human capital. The main barrier is the fact that human capital is not owned by the company, so it is difficult to shape it properly. On the other hand, the lack of relations between employees is connected with the lack of knowledge and information flow between them, which leads to a substantial limitation of the organization's development. So the organization that will find a method of effective acquisition and maintenance of human capital in its ranks, according to the old, but still applicable, rule "whoever has the information has the power", will win on the market.

7. References

- [1] R. W. Griffin, *Fundamentals of organization management*, PWN Publishing House, Warsaw 1997, p. 80.
- [2] A. Pocztowski, *Human resources management. Outline of problems and methods*, Antykwa, Kraków 1998, p. 19.
- [3] M. Sępek, *Human resources management. Entrepreneurship and management*, Social Higher School of Entrepreneurship and Management, 2010, Volume XI, Notebook 11, p. 52–71.
- [4] B. Jamka, *Human factor in a modern enterprise: a resource or capital?*, Difin Pub., Warsaw 2007, p. 16.
- [5] M. Juchnowicz, *Flexible human capital management in the knowledge organization*, Difin Pub., Warsaw 2007, p. 18–20.
- [6] B. Wyrzykowska, *From human resources to human capital*. Scientific works of the Jan Długosz Academy in Częstochowa 2013 from VII. Pragmata tes Oikonomias.
- [7] K. Beyer, *Human capital management in the process of shaping intellectual capital*, Faculty of Economic Sciences and Management, University of Szczecin 2016.

ANALYSIS OF THE SYRIAN CRISIS AND ITS ROLE IN INTERNATIONAL RELATIONS

Chief Assistant Professor PhD eng. Dolchinkov N. T.,
National Military University „Vasil Levski“, Veliko Tarnovo, Bulgaria,
National Research University "Moscow Power Engineering Institute", Moscow, Russia
n_dolchinkov@abv.bg

Abstract: Over the last decade, the fighting in the territory of the Syrian Arab Republic has evolved with a variable advantage for the warring countries. Government forces, "Islamic State" terrorists, Kurdish separatists, and various factions of moderate opposition at various times prevail over certain parts of the territory of the multinational country. Is the civil war ending or will it all turn around in the next round of military roulette? Whether the civilian suffering will end will show the near future

KEYWORDS: SYRIAN ARAB REPUBLIC, RUSSIAN FEDERATION, ISLAMIC STATE, COUNTRY, COMBAT, FUTURE, TERRORIST, CIVIL WAR, MILITARY, KURDISH SEPARATISTS, OPPOSITION.

1. Introduction

Syria is a Middle East country bordering Lebanon to the west, Israel to the southwest, Jordan to the south, Iraq to the east, and Turkey to the north. It obtained its independence from the French term for Syria in 1946, but its history began in the fourth millennium BC. Its capital, the city of Damascus, was the seat of the Umayyad Empire and the provincial capital of the Mamluk Empire. Historically, Syria has often included the lands of Lebanon, historic Palestine and parts of Jordan. This region was called Great Syria or the Arabic name of Bilad al-Sham. After the Six-Year War in 1967, Israel occupied the Golan Heights in the southwest of the country. There is also a dispute with Turkey over the possession of the provinces of Hatay and Idlib.

Syria has a population of 22 million people. Most of them are Sunnis, as well as 16% other Muslim groups such as Aulawi, Shiites, and about 10% of Christians. Since 1963 the country has been governed by the BAAS party. The current president of Syria is Bashar al-Assad, son of Hafez al-Assad, who has been in charge since 1970 until his death in 2000.

The boundaries of today's Syria emerged after the end of the First World War when the Ottoman Empire collapsed. In 1920, French and English diplomats negotiated the division of influence zones into the territories of the former Empire.

The exertion of the Syrian terms of the French is not an easy task. After many difficulties in 1945, the Syrians gained their independence. In the next 25 years, the Syrians have a very restless political life and witnessed a series of military coup. They also opposed initially the supporters of the Arab Socialist Party BAAS.

2.1. Historical development of Syria

In 1958, the unification of Syria and Egypt was proclaimed within the United Arab Republic under the presidency of Egyptian President Nasser. At the end of next year, frictions between Syrians and Egyptians became intolerable, resulting in a break between the two countries and the re-establishment of the two independent states. Saddam Hussein's coming to power in Iraq in 1979 further exacerbated the conflict in the region.

Syrian politicians also actively intervene in Lebanon's policy. The civil war that began in Lebanon in 1975 continued for 15 years. In October 1989, tired of the war, western politicians accepted the Syrian influence recognized by the Arab countries in Lebanon. Only now can the Syrians move on to the implementation of the Great Syria project. According to him, the territories between the Mediterranean Sea, the Gulf and the Red Sea must be indivisible. But after 1920, they were fragmented and Syria, Jordan, Saudi Arabia, Iraq and later other countries appeared on the map in this region - Israel, Lebanon, Palestine.

The Syrian economy is characterized by strong state interference in economic life. It was only in 2001 that private banking operations were allowed, and two years later, the first three non-state banking institutions appeared.

In the last 10 years, average GDP growth of Syria is 2.3%. Unemployment is high - 20%. Inflation is 5.1% in 2014. All this is

explained by the fact that there is a war on the territory of almost the whole country.

Under the turmoil in the Arab world on March 15, 2011, a revolt in the country broke out, later transformed into a blood-war civil war that continues to this day.

Syria is divided into 14 districts (muffafas). The districts are subdivided into a total of 61 districts, which in turn are divided into 206 municipalities (Nakhia) (Figure 1).



Figure 1: Territorial division of Syria

Syria's population in 2012 is estimated at 22,457,000. Syria is one of the most densely populated countries in the Middle East. In 1986, the density was 57 people per square kilometer, and in 2004 it was 363 people per square kilometer. However, the population is very unevenly distributed, with most of the Syrians living in the western part of the country, in and around Damascus and Aleppo and along the River Euphrates. Few over 90% of the population are Arabs, the remaining over 9% as mentioned above are Kurds, Armenians, Turkmen and Syrian Greeks.

According to estimates in 2013, 33.9% of the Syrians are under the age of 14, 20.8% are between the ages of 15 and 24, 36.9% are between the ages of 25 and 54 and only 8.5 % are over 55 years of age. Over 12,280,000 people, or more than half of Syrians, are under 25.

2.2. Civil War in Syria

The civil war in Syria is multifaceted and has many conflicts that turn into armed conflicts in different regions of Syria. As I said, it began in the spring of 2011 as a local civil conflict under external influence and similar to what is happening in other Arab countries, and has gradually grown into a rebellion against the Bashar Assad regime, in which, over time, not only the largest countries in the region, but also many international organizations, military-political groups and global powers.

The main parties to the conflict are regularly armed and have military and paramilitary formations. On the side of President Bashar al-Assad are the Syrian Arab Army, the National Forces of Defense, and the other side of the barricade are forces that have very different goals, views and tasks, such as the so-called "moderate" opposition like the Free Syrian army, Arab formation of the Sunni tribes, Kurdish regionalists (the Union of People's Self-Defense), as well as various types of extremist Islamic and terrorist jihadist groups (Islamic State, Jabhat an-Nusra, etc.). In the conflict, countries receive military assistance from other countries: support for government forces is Russia and Iran, while the Syrian opposition is backed by Western powers and the Gulf monarchies. Turkey should also not be ignored here, which also has its own interests in the region and is actively involved in the actions of Syrian territory. Because of the significant involvement in the conflict of foreign states and organizations, Syrian and international experts characterize it not as a war between the regional powers but as a war of the world powers.

Began in March 2011, as a result of the "Arab Spring", anti-government demonstrations led to riots in various Syrian cities, and in the summer of that year it escalated into a full-scale armed conflict. The main demands of the opposition include mainly the resignation of President Bashar Assad, the abolition of the 1962 order of a state of emergency and the conduct of democratic changes in the country without the involvement of current rulers.

Initially, the struggle was between the government army and the forces of the Free Syrian Army (SAA). The Syrian National Council (SNC), the Syrian National Council (SNC), which at that time included all anti-government groups, was the umbrella of the Syrian opposition. Nevertheless, later, the division of the opposition came into being - the first of its members came out of Kurdish organizations to form their own government (the Higher Kurdish Council), and in 2013 the most radical Islamist groups formed in the Islamic State and groups close to it.

Because of the division into the ranks of the rebels, the positions of the SAA have significantly diminished and the secular opposition has collapsed. Various types of Islamist groups have begun to play a leading role in opposing government forces in various parts of the state, including the Al-Qaeda Al-Qaeda terrorist organizations and the Islamic State (IDA) terrorist organizations being the most capable and active over the years.

The rapid onset of ID and the capture by Syria and Iraq of the significant territories of the terrorists in the summer of 2014 caused the start of the military intervention of the United States and its allies, who, since September 2014, have beaten air against Syria's Islamist positions. I must also mention the many oil-trains that were transported through Syria with the tacit support of the United States, Turkey, and others, and they were realized in a very interesting way, and this had an impact on oil prices on international markets. A number of trainings of the so-called "moderate opposition" were also caught up in the hands of the terrorists. On September 30, 2015, following a Russian accord with President Bashar al-Assad, a military operation in Syria was launched by the Air Force and Space Forces of the Russian Federation, acting in close cooperation with the government troops.

According to the UN, by 2015, some 220,000 people have died during the conflict. The war was one of the main reasons for the European migration crisis, which prompted the mass exodus of refugees from Syria and other countries that used the conflict in Syria to incite massive migration to Europe, and mainly focused mainly on Germany, France and Scandinavia. The conflict is characterized by numerous fierce fighting, indiscriminate destruction of settlements, slaughter and numerous war crimes against civilians, and the economy and infrastructure of the country have suffered huge damage. The law on slavery, slavery is legalized in Islamist-controlled territories, religious minorities are being persecuted, and sites of cultural heritage have been destroyed, which destruction has even been shot by representatives of radical Islamist movements and shown to the entire world.

The main event in 2016 was the success of the government troops and their allies (Russia, Iran) in the battle for Aleppo.

Opposition detachments, who held control of the eastern half of this strategic city in northern Syria for four years, suffered a crushing defeat. Unlike the other Syrian-controlled cities (mostly Homs and Hamas), whose siege has dragged on for months, and government forces have achieved their goal only through the tactics of prolonged blockade and isolation (lacking in food, reinforcements and ammunition, agreed to leave the city), here is a radically different scenario. The result of the Battle of Aleppo strongly changed the alignment in the positions and command of Syrian territory of Syrian government troops with the opposition forces.

In addition to the successes of the government's army, 2016 led to two more fundamental changes. First, a new participant joined the Syrian conflict - Turkey included its troops in northern Syria. The official purpose of the operation was proclaimed as a fight against terrorism and an "Islamic state," and in fact a major enemy of Ankara are Syrian Kurds who will try to create their own autonomy along the Turkish border. This will lead to internal Kurdish rebellions living on Turkish territory and a request for autonomy and independence in Turkey at a later stage. Secondly, in 2016, the positions of an "Islamic state" have significantly weakened. In May the Liberation of Palmyra's government troops ended. In neighboring Iraq in 2016, the "Islamic State" suffered huge territorial losses: governmental Iraqi troops and their allies seized territories that were rich in oil and controlled by ID.

2017 led to radical changes in the situation in Syria. The main result of the year is the defeat of the Islamic State group, which has lost much of its influence since 2015, and has been pushed by a large part of its territory controlled by Syria and Iraq. Speaking of the complete physical removal of the terrorists' forces, however, it is too early. Since mid-2018, ID rebels have been controlling small areas in the Dar Dar province in southern Syria, as well as several settlements on the east coast of the Euphrates between the towns of Al-Bukhamal and Deir Az-Zor. The presence of ID is maintained in the two enclaves in the Syrian desert at the crossroads of the provinces of Homs and Deir es-Zor and Homs and Es-Suwade, as well as in the region of Idlib province in the northern part of Syria bordering Turkey.

The defeat of ID allowed Russia to announce by the end of 2017 the termination of the operation of Russian military security services. Meanwhile, the completion of the active phase of the war did not lead to the peace-Syria opposition, and the outside forces supporting it show that they do not intend to participate in the post-war reconstruction if it continues to be headed by Bashar Assad. Some provocations have even been fabricated with the use of chemical weapons.

In 2018, the Turkish invasion of Syria continued, and by mid-March Africa and the surrounding area were occupied by the Turkish army. Syrian government forces, pro-government alliances, and allies have been able to regain control of large areas in the center of Africa, the south and southwest parts of Syria, and remove many enclaves from the armed opposition, but have not committed blood-warfare, and so far there is refraining from conducting military conflicts. So far, this process is taking place, but there remain separate small outbreaks of tension in these areas of the country, but I hope that by addressing the problem in Idlib these local counter-actions will be resolved. The completion of this process is expected to lead to a country-led government-led division of: a cultural, industrial and agricultural center (more than 60% of the territory and 80% of the population) and the peripheral zone [4].

To the peripheral areas we can now take the places where there are still remnants of warring groups like:

1. Idlib province, which is controlled and distributed among all opposition and terrorist groups ("Tahrir Ash-Sham", "Jehhat Tahrir Surya", etc.), and we must note the presence and control of certain points in the Turkish Air Force and according to the latest agreements between the presidents of Russia and Turkey and the armed forces and military police of both countries;

2. Turkish occupation zone in the ethnic Kurdish regions of the northern part of the province of Aleppo (with the active participation of the Free Syrian army supported by Turkey);

3. Controlled Zone of the "Syrian Democratic Forces" (UDF) in the predominantly Kurdish regions of the northern provinces (the self-proclaimed Democratic Federation of Northern Syria);

4. The Zion Control in the province of Deir Az-Zor on the east coast of Euphrates, and in the south of the province of Raka, which is dominated by the Arabian Sunni tribes and the remnants of the ID units, is also in the process of being completed.

Regarding the remnants of ID's, as noted by Alexander Bornitnik, FSB Director at the Seventh International Conference on International Security (April 2018) in Moscow, "in an effort to maintain their fighting potential, to preserve the existing and to create new areas of influence, they increasingly avoid open armed clashes and rely on the methods of guerrilla war." Experts believe that the most convenient place to conduct a rebel war (and eventually attempt to revive ID) will be the neighborhood adjacent to both sides of the Syrian-Iraqi border and Idlib province with the help of outside support and provocative actions.

According to some analysts, the outcome of the Syrian conflict depends not only on the future of Syria, but also on the balance of power in the Middle East, on the prospect of fighting international terrorism and, to a certain extent, emerging new world order.

According to Russian military, during the war period of 2011, Syria has left more than 6.9 million people. According to preliminary estimates from the middle of 2018 to return to their homes in the near future can more than 1.7 million Syrians in the event of a ceasefire and the authorities are ready to accept and settle only 336 000. This is explained by the fact that in the major cities the infrastructure in the combat zone was destroyed within 40-70%.

Protecting the population from disasters, accidents and catastrophes is a priority activity in civilized countries [7].

How do things stand with the notorious use of chemical weapons by the Syrian state in my opinion. The first reports of the use of chemical weapons in the Syrian conflict appeared on March 19, 2013, when the Syrian authorities said the opposition had used it during battles near the village of Al-Assal (Aleppo province).

On August 21, 2013, reports have appeared in the media about the use of saccharin on the outskirts of Damascus and East Gut. As a result of the chemical attack, it is reported that 600 to 1300 people have been killed. The Syrian authorities and the opposition rejected the accusations of using a chemical attack by transferring responsibility. The US accused government forces of committing the attack. France and the United States, with the support of several Arab states, have seriously considered the issue of a punitive military action against Syria, which they subsequently implemented with massive air strikes.

On December 27, 2014 in Moscow, experts from Russia, the United States, China, Syria, Norway, Denmark and the United Nations discussed the organization of the safe export of chemical weapons from the territory of Syria. The first consignment left Syria on a Danish ship on January 7, 2014. From 7 July to 13 August in the Mediterranean Sea aboard the American ship Cape Ray, the most dangerous chemicals were destroyed. In January 2015, Syria began liquidating facilities for the production and storage of chemical weapons [2].

In August 2015, a joint mechanism of the UN and the OPCW was set up to investigate the use of chemical weapons. On 4 January 2016, the OPCW confirmed the completion of the destruction of chemical weapons declared by the Government of Syria. Work on destruction was carried out on businesses in the United States, Finland, the United Kingdom and Germany.

On 26 October 2017, the United Nations Security Council handed down the report on the UNHCR Joint Mechanism for the Investigation of the Use of Chemical Weapons in Syria. The report says the Syrian Arab Republic is responsible for the use of saccharin in the Syrian city of Han-Sheikhun, and the ID is responsible for the attack in the Um-Hosh settlement in September 2016, where sulfuric acid is used. The Russian side assesses the report as amateur and is based on assumptions and selective use of the facts [5].

On 18 November 2017, the Joint Mechanism for the Investigation of Chemical Attacks in Syria ceased to exist as the

UN Security Council failed to reach an agreement on the extension of the mandate of experts investigating the use of chemical weapons. Russia vetoed the US draft resolution. In turn, seven countries have refused to support the proposed resolution by Russia, Bolivia and China.

On April 7, 2018, several NGOs accused the government of a chemical attack on the inhabitants of Duma (Eastern Gut). In Damascus and Moscow, these accusations were rejected, calling the published videos fabricated and fake. It is a very interesting fact that the shown figures are from the profile of a 7-year-old child in the area [5].

Nonetheless, the US State Department, in unprecedented categorical declarations, accused the Syrian government, backed by Russia and Iran in the use of chemical weapons, and Trump's president warned that Russia would "have to pay a great price for Assad's support." The East Gut incident occurred amid a deepening crisis in Russia's relations with the United States and the West as a whole, and the United States has demonstrated its determination to continue to deepen its conflict and relations with Russia, which may also lead to a direct military strike with Russia on the Syrian Territory.

Civilian Refugees in Syria are citizens and permanent residents of the Syrian Arab Republic who left their country after the start of the Syrian civil war in 2011 seeking asylum in other countries. It should be noted that, at the same time, millions saw themselves as refugees from Syria for immigration to Europe. This was skillfully used by stakeholders to strengthen the cross-cutting pressure on Europe.

In 2016, the UN identified 13.5 million Syrians in need of humanitarian assistance, of which more than 6 million were internally displaced in Syria and more than 4.8 million were refugees outside Syria. In January 2017, the UN had 4 863 684 registered refugees outside Syrian territory. Turkey is the largest host country with a total of 2.7 million registered refugees and it, in agreement with the EU, detains these emigrants, for which it has signed a treaty with the EU and has received 3 billion euros in several tranches.

The consultations with Representatives of the Astana guarantors (Russia, Iran and Turkey) were held for the last time on 10-11 September 2018 in Geneva with the UN Secretary-General's special envoy for Syria, Stefan de Mistura, and concluded with decisions have approached the achievement of constitutional reform and conflict resolution. The participants were able to agree on government and opposition lists of candidates, as well as to agree on a mechanism for forming the third list - from civil society. Essential requirements for the new constitution of Syria are preserving the integrity of the state, recognizing the equality of all nationalities and religions, dropping "Arab" on behalf of, holding transparent and fair elections. In early September, even in some parts of the country, local elections took place, involving representatives of various political unarmed forces. Ex-Armed Oppositionists also took part in these elections, taking advantage of the government's opportunity and joining the Syrian reintegration. The conduct of these first elections has stayed away from our information media [4].

As Russia's Foreign Minister Sergei Lavrov said, Moscow is ready to cooperate with all partners interested in the quickest settlement of the issue in Syria and the post-war re-establishment of the country.

"Today, the liquidation of Terrorists on Syrian land is over. The country is turning to peace and political settlement. The agenda includes the restoration of destroyed infrastructure, the establishment of economic activity, the return of millions of refugees and internally displaced persons to their homeland," the Russian Foreign Minister said. According to Lavrov, aiding the Syrians in solving these problems could become an important area for international cooperation, with talks between Russia, Turkey, Iran, France, Germany and other countries already taking place [3].

On September 18, at a meeting in Sochi, the Russian president and his Turkish counterpart, after nearly five-hour talks, came to a new peaceful solution to the conflict, which was adopted differently

by world leaders. In it, they negotiate a peaceful solution to the problem by creating a demilitarized 15-20 km zone along the border of the area by 15 October. During this period, all armed groups may be withdrawn from the area and will not be impeded or subjected to repression. The process will be controlled by the Russian and Turkish armed forces and the military police. In this way, both countries isolate European countries and the United States and stop the possibility of military intervention from third countries in the region.

On 19 September 2018, a Russian aircraft IL-20 of the Russian Armed Forces was disembarked over the Mediterranean Sea in preparation for landing. The defeat is from the Syrian Air Force, which fired four Israeli F-16s that were preparing to strike in Syria. Israeli planes used the Russian plane for cover, and the Israeli authorities have informed the Russian side of the prepared strikes 1 minute before applying them, which is a very short time. The announcement says air strikes in northern Syria are being bombed on a western coast near an international airport and a densely populated area. After the incident, there were numerous talks between the Russian and Israeli high-level countries.

What the next steps will be and how the Syrian issue will be resolved is difficult to predict. The situation is very dynamic and often unpredictable with the many provocations and fake news on which global political decisions are made. I hope soon to find a lasting solution to the problem and to bring peace back to Syria and reach a peaceful solution to regional problems. The people of this country must live under normal conditions and solve their own problems, not to become a hostage to the political ambitions of world leaders and an experimental field for testing new weapons.

3. Conclusions:

1. The civil war in Syria began in 2011, following the example of the Arab Spring in Iraq, Libya, Egypt and other Arab countries, with the active intervention of external forces that directly and indirectly supported the forces of the so-called opposition. Things were shaken out of control and led to the entry of the Islamic State and related Islamic groups into Syrian territory.;

2. A major influence on the spread of the conflict has been the financial support of some of the great powers and the rich Arab countries that implicitly support the extreme Islamists;

3. The conflict has provoked a migratory wave to the borders of Europe, which has been skillfully used for political purposes and which still provokes great controversy both within and outside the EU. This wave was used by residents of many other regions of the world to transfer to Europe, including members of the "Islamic State" and other terrorist groups.

4. The agreement between the presidents of Russia and Turkey provides a basis for a peaceful solution to the problem and, at the same time, it isolates other countries from the resolution of the conflict. This has caused some bad reactions in some countries but has been accepted by the international community.

4. Literature:

1. Долчинков Н. Т. Конфликтът в Сирия и неговото значение за състоянието на международната сигурност, Научна конференция «Актуални проблеми на сигурността» НВУ «Васил Левски» Велико Търново, 2018.

2. Сводки на ООН и ОСХО, 2017, 2018 г;

3. Официални съобщения на пресслужбата на Президента на Руската федерация, 2018;

4. Официални съобщения на пресслужбата на Президента на Турската република, 2018 ;

5. Официални съобщения на пресслужбата на Президента на САЩ, 2018;

6. Lilov I. Georgiev I. Maintenance System Research for Armored Vehicles in Peacekeeping Operation as Close Queueing System in Dynamic Regime, The 23rd international scientific conference Knowledge-Based Organization -Sibiu 15-17.06.2017;

7. Пъдарев. Н. И. Антропогенни аварии и катастрофи. ПИК, В.Т. 2016.

NUCLEAR WEAPONS IN RUSSIA

ЯДРЕНИ ОРЪЖИЯ НА ВЪОРЪЖЕНИЕ В РУСИЯ

Chief Assistant Professor PhD eng. Dolchinkov N. T.,

National Military University „Vasil Levski“, Veliko Tarnovo, Bulgaria,

National Research University "Moscow Power Engineering Institute", Moscow, Russia

n_dolchinkov@abv.bg

Abstract: *The main types of weapons in the nuclear artillery are shown. The main types of used controlled and unmanageable ballistic missiles manufactured in Russia are examined. It shows the application of ballistic and winged missiles and their role in the theater of warfare.*

Keywords: *nuclear weapons, Russia, development, intercontinental ballistic missiles, nuclear craft.*

1. Introduction

After detection of radioactivity in the early years of the century, scientists believed that the source of radioactive emissions into the atmosphere are only earth and rocks. Very soon, however, it is noted that with the increase in altitude (in experiments with balloons) the radioactive radiation has increased due to cosmic radiation. Later it was found that cosmic radiation contains two components: primary radiation - of galactic origin penetrating the atmosphere, and secondary cosmic radiation - derived from the reaction of cosmic rays with the nuclei of elements in the air, space dust, which is layered on the planet and others. This activity is mainly driven by the light radionuclides, such as: beryllium, sodium, aluminum, vanadium, etc. Cosmic rays that reach the Earth's surface can create radioisotopes decay but compared to other naturally occurring radionuclides is extremely low and not particularly important [1].

This discovery quickly going into medicine and created the first X-ray machines that led to a revolution in medicine. Subsequently advanced and modernized X-ray machines of the latest generation repeatedly raising the precision of diagnostic activity and allow saving hundreds of lives [3].

At the same time found that radioactive rays are a major polluter of the environment with an extremely strong impact on the life and physiological activity of organisms ranging from incentives to killing.

It is known that everything on our planet it is subjected to constant exposure from the natural and anthropogenic, earth and space sources on ionizing radiation, ie find are in an conditions, created from the natural and technogenic radioactive background. Yonizirashitite lacheniya accompany [2].

2. Development of Russia - NATO relations

Over the last two years, US-Russia relations (as well as Russia's relations with NATO) have reached a dangerously low point - the lowest point since the end of the Cold War. As a result of these developments, the issue of nuclear weapons and nuclear supplies has come to the fore again. Numerous extraordinary government declarations point out that both sides are rehearsing nuclear strikes against each other. Former NATO Secretary General Jens Stoltenberg, for example, said in an annual report that the Russian Air Force had conducted a training mission in 2013, is actually a "simulated nuclear attack" against Sweden. The report revealed that the Tu-22M3 supersonic bombers had been involved in the mission to carry long-range shocks, disguised as Su-27 fighters. Meanwhile, NATO member Turkey was a few steps away from a war with Russia, which in no way alleviates the situation.

In this context, it is useful to assess the state of nuclear weapons of both the US and Russia. How does the current situation affect the strategic balance and is it possible for each party to be convinced of

how unreasonable the start of a conflict is? What are the prospects for the development of the nuclear weapons of these two superpowers?

Both countries are bound by the new START 3 contract.

The contract for the further reduction and limitation of strategic offensive arms signed on April 8, 2010 by Presidents Obama and Medvedev commits their countries to reduce the amount of their nuclear warheads to 1,550 units. Also under the contract, the number of deployed intercontinental ballistic missiles and heavy bombers shall not exceed 700. In accordance with the data published by the US State Department on April 1, 2016, the two countries have reached or are close to specified indicators. The United States has 741 deployable startup facilities equipped with 1481 nuclear-weapon heads while Russia has 521 launchers equipped with 1,735 nodules. The difference is insignificant and does not affect the strategic balance. For now, Russia has fewer run-ups, but this discrepancy is due to the fact that intercontinental ballistic missiles carrying separable heads with independent guidance have a much broader scope of application - an intercontinental ballistic missile can carry up to ten independent heads of war. Here are the available nuclear missiles of Britain and France, which are also members of NATO.

2.1. Russian land-based intercontinental ballistic missiles: emerging anti-missile defense technologies.

Russia currently has a wide range of ground-based intercontinental ballistic missiles including mobile launching facilities. In 2015, the Missile Force with Strategic Purpose of the Russian Federation (RSCN RF) received 24 new missile complexes of the RS-24 "Yars" type (classified as SS-27 Mod 2 in the NATO classification) both in mobile and in shaft variant. These missiles can carry three or four self-directed nuclear warheads capable of penetrating missile defense systems. It can certainly be assumed that the volume of supplies of such missiles in 2016 will not yield to the quantity delivered in 2015. So Russia will be able to replace the Topol missiles (which are basically the equivalent of the LGM-30G Missile III) with the latest generation of missiles specifically designed to overcome enemy missile defense systems.

Russia also has heavy, ground-based, intercontinental liquid fuel missiles. The P-36M2 "Voevoda" (NATO-rated SS-18 Mod 5, Satan), which have been in arms since 1988, are well known. Such a rocket can carry up to 10 nuclear warheads of up to 750 kilotonnes each. This year, tests will be carried out on the latest missiles of the RS-28 type (also known as the "Sarmath"), which are planned to replace Voevoda missiles in 2020 and are equipped with everything they need to deal with missile defense systems. Above all, it is expected that these missiles will have the ability to launch their warheads on a sub-bore trajectory (shorter than the circular orbit banned by international agreements) and strike

virtually anywhere (from anywhere in the globe), even from the South Pole. This will force the likely opponent to build an integrated missile defense system, which is extremely costly, including the United States. Moreover, nuclear warheads will enter the atmosphere at supersonic speed and will move along an extended trajectory, maneuvering at a speed of 7 to 7.5 kilometers per second. The timing of the missile preparation will be reduced to a minimum and will continue for less than a minute after the order is received.

In addition, Russia also has the mysterious missiles RS-26 "Ruby", for which almost no information is available, but it is known that there is obviously some modification of the RS-24 "Yars" for inter-continental and mid-range impact. The minimum range of these missiles is 2000 kilometers, which is enough to break the US missile defense system in Europe. The United States opposes the deployment of RS-26 missiles on the grounds that this is in violation of the Medium-Range Missile Shuttle Intervention Agreement. But such a statement does not resist criticism: the maximum range of action of RS-26 rockets exceeds 6000 kilometers, which in practice means that they are intercontinental ballistic missiles and not mid-range ballistic missiles.

Given the facts, it appears that the United States is largely lagging behind Russia in the development of ground-based intercontinental ballistic missiles. The United States, in fact, has one - to be fair - a very old intercontinental ballistic missile model - the LGM-30G "Minuteman III", capable of carrying only one nuclear warhead, and the prospects for developing a new model for their replacement are very vague. In Russia, the situation is completely different. Intercontinental ground-based ballistic missiles are renewed and modernized on a regular basis - the process of developing new missiles has never stopped. Each new intercontinental ballistic missile model is designed to penetrate missile defense systems, which means that the European missile defense project and the ground missile defense system in the middle of the flight (US anti-missile defense anti-missile defense system capture of approaching nuclear warheads) in the foreseeable future will prove to be absolutely ineffective against Russia.

What are the most terrible Russian weapons endangering the US? The rating was made by American experts on Russian strategic nuclear forces and appeared under the title "The Five Types of Russian Nuclear Weapons, of which the West Should Be Afraid"

2.2. Who are these weapons?

"Borey" separately, "Bulava" separately. First of all, US experts have put Russian Nuclear Strategic Submarines of the Borey type 955, which have 16 ballistic missiles in armament and are the basis for Russian nuclear capability.

Secondly on this list is the intercontinental ballistic missile R-30 "Bulava-30", with which the submarines Borey are armed. This weapon can hit targets at a distance of 11,000 km, each Bulava carrying 10 nuclear warheads.

The third place in the rocket rating is the Yassen multi-purpose nuclear submarine - project 885, armed with anti-missile wing missiles.

Fourth, Americans have set up a Russian tactical nuclear weapon, which is not covered by the Strategic Offensive Arms Reduction Treaty, the HNV 3.

Fifth place, Western experts have set up solid-fuel intercontinental ballistic missiles with a portable, CS-24 combat division, the Yars, which can carry up to four individually targeted warheads.

It is also mentioned the new super-heavy Russian Sarmat rocket-based rocket, which will replace the former "Voevoda" superstar, also known as "Satan".

It is supposed that Sarmat will be liquid fuel and will be able to carry 10 battle blocks with a range of 121,000 km. They will be deployed in Dombarowski - in the Orenburg region, and in Ujmur - in the Krasnoyarsk region.

All Russian strategic missiles - both marine and ground-based, including the operational-tactical complex Iskander-M, have all the means to overcome the US missile defense system.

Along with the analysis, another appeared with a list of Russian weapons that the Pentagon should be afraid of. It turns out that it is much longer.

So, among the dangerous Russian weapons is the Su-35 multi-purpose fighter, the Amur atomic submarine, the major new T-90C tank, the supersonic P-800 Onyx anti-missile missile based on the Indian multi-purpose wing rocket Bramos, used for offshore and coastal purposes, both from ships and from submarines, and in the perspective of aircraft.

T-90 tanks are much cheaper than Western Leopard-2 and Abrams tanks. The tank has a modern fire control system and effective protection systems. Its 125 mm caliber can be loaded automatically. He can shoot with traditional shells - armored, cumulative, fugitive and cumulative, as well as reactive missiles "Reflex".

At present, Russian tankers are creating not just a new tank that will be better than the T-90, but also the best army platform. On its base will appear the powerful tank, the armored shell for the crew, the new fire control system, the connection and navigation system, the target computing complex, the onboard information control system and other fire safety systems. For now, Arma is a secret project and is likely to appear in the preparation of the anniversary parade for the 70th anniversary of the victory of the Alabins polyon.

Among the most anticipated new Russian weapons is Su-35, which is a modernized version of the Soviet Su-27, although this is not quite accurate. From Su-27 the new plane took the planer in a highly sophisticated look. The engine of his engines has the ability to change his drawing, to divert up or down or to the left to the right, and to perform wonders of the aerial acrobatics that no American fighter can do. The Su-35 is very fast, it can rise to high heights and has a huge load, ie. combines advanced capability to capture high speed light targets and unique high-powered engines. This was demonstrated in the conflict in Syria.

The P-800 "Onyx" versatility wing is unique in its way of operation. Once it falls into the water trail of the frigate or aircraft carrier, it will not leave it until it strikes the most unprotected spot.

Arms in the Russian Army are still the supersonic anti-missile missiles "Mosquito" and "Granite", of which Western ships have no protection at this stage of the development of the world.

For the first time, the world saw a successful test of the Russian intercontinental missile system of the future "Sarmat".

On March 1, 2018, Russian President Vladimir Putin told Russia and the world that the country had successfully set up and conducted nuclear missile tests from a new era: Sarmat or RS-28. She is loaded with the most devastating warhead in the world.

The new intercontinental missile system replaces its 25-year-old predecessor, known as VC-20C Voevoda. His rocket weighs 200 tons with a payload of 10 tons and is the only one in the world capable of crossing 17,000 km before eliminating everything on his way.

Each rocket will have more than 15 separate heads with individual targeting of battle blocks, each with a 150 to 300 kilotone charge, the impact of which can create a crater with the size of the Grand Canyon.

This is just one of the five most anticipated weapons of the future - see who the rest are!

The manholes built in Russia for the new super-heavy 100-ton ballistic missile "Sarmat" will be in the Orenburg region and Krasnoyarsk region. Thus the heir of the notorious "Satan" comes into the final right.

"Sarmat" is one of the major new puzzles of the Russian military-industrial complex. The rocket will replace the RG 20B "Voevoda" (the western classification "Satan").

Vojvoda is currently the largest and worst strategic missile ever created. It weighs 210 tons and carries 10 nuclear warheads of 750 kilotonnes each.

Once in the USSR, these missiles were 308, now 52 in Russia, and are on duty at Dombarsky and Ujour, in Orenburg and Altay.

Prepared in Dnepropetrovsk, but because of the complicated relations in Ukraine the Russian side no longer relies on this cooperation.

The new missiles, which are due to enter the armed forces by 2022, are likely to appear earlier.

With its characteristics, Satan is unresponsive to the action of any electromagnetic impulse and can start from the shaft even after it has hit a nuclear warhead. The rocket carries a large complex to overcome missile defense, including the promising US. It can deliver to anywhere in the world 10 tons of weight, 10 nuclear warfare units with individually directed megaton class. Only one such rocket is enough to completely destroy New York. It was because of this in the West that it was called "Satan".

No less impressive will be the new missile, the successor to Satan - Sarmath. It will be produced by Makeev, who has experience in creating large ballistic missiles. Some time ago, it was the weapon for the largest nuclear submarines in the world - 941 of the Typhoon project, the RSM-52 rocket. This solid-fuel rocket weighed 100 tons and delivered 10 nuclear warheads to the target. But for financial reasons, both the whole range of the most powerful submarines and the RSM-52 missiles were retired. The last launch of the last such missile was in 2012. The last submarine, Dmitry Donski, still under construction, will also be retired.

The new supercharged "Sarmath" rocket will be fuel-efficient. Unlike solid-fuel rockets, liquid fuel has the highest performance. For example, in the course of the Stability-2008 exercises, the Sineva Marine Rocket has established a world record for a range of 11,500-kilometer rocket flights in this class.

The new Sarmat land-based missile will have a weight of no more than 110 tonnes, it will have a warhead with several nuclear warheads with individual guidance. According to some data, these will be maneuvering hypersonic blocks, such as those with the latest Russian strategic missiles Topol-M, RS-24 "Yars" and Marine Bulava.

Such a set-up gives the rocket almost total invulnerability in overcoming the missile defense system, the one the US is currently building along the borders of Russia and the one it will create in the future. No rocket system can trace the missile or its warheads that fly over individual ballistic curves if they suddenly hide in that arc and start flying with supersonic and even hypersonic velocity, clinging tightly to the relief of the area maneuvering the course and the height. It is impossible to intercept and even destroy such a rocket. The breadth of the Sarmath range will also exceed 11,000 kilometers.

"Sarmath" will be located in shaft launches. This is also testified by the fact that the rocket will be built to the size of the old heavy missiles RS-20 and PC-18.

The new missile sets a number of innovative requirements to overcome any missile defense, which may include a space-strike echelon. At the same time, a deep modernization of the existing rocket launchers is envisaged, which implies their technological transformation and a new qualitative level of security fortification with the creation of passive object missile defense elements. This will allow the life of the launch shafts to be increased by attacking the enemy, both with high-grade weapons and with nuclear weapons.

The missile shaft is a complex engineering facility that not only ensures the launch of the rocket, but also guarantees its storage even when it comes to a nuclear warhead. In the USSR years ago, they experimented with a similar attack on nuclear warfare. It turned out that no more than 7-9 nuclear warheads were to be brought out of the battlefield duty-on-the-shash racquet, which, on top of everything, should fall into the target. Such resilience guarantees Russia a retaliatory blow to the United States. This means that Makejev will make a rocket that will be able to launch after a nuclear explosion and hit the target in the other hemisphere.

Years ago Voevoda became the factor that forced the United States to sit on the table of talks on limiting strategic offensive weapons. Today the story is repeated. Russia is again building a

supercar. "Sarmath" will outperform Satan with its tactical and technical features. It will be a unique weapon that will hardly ever appear in the US.

Military experts in the world are amazed by the Russian novelty - rocket complex with intercontinental ballistic missile RS-26 "Ruby". On the possibilities for further development of the Yars project, analytical televisions even devote special broadcasts.

At the beginning of March, a military expert told a radio station about the uniqueness of the new Russian missiles and the concerns of foreign armies before Russian MBR. The following talk took place on the TV show:

"The new Russian missile RS-26 is flying on a constantly variable trajectory. There is no such weapon in any single army in the world," the expert notes, and the question of the astonished journalist about the US system of missile defense: "You can forget about PRO. She is powerless to RS-26."

"Recall the last hint of the Russians, please, do not annoy us. And now, by words, I moved to deeds. This is not even the famous "Topol-M". The PC-26 battle heads fly over and steadily maneuver. Part of them will surely overcome the missile defense system and reach their targets."

"What is it? Are the trousers out of fear or are they ready to answer?"

"Not only did the US tremble that we in China are not funny. Now Russia is under safe protection that you can not say about the other countries in the world," sums up the Chinese military analyst.

Why did the RS-26 missiles so scared the world's expert society? Thanks to the use of high-strength polymer materials at temperatures up to 850 degrees, the creation of the Wotkin plant is considerably lighter than its predecessor. For example, the Yars mass reached 120 tons against 80 tons of "Ruby", but the cumulative nuclear power consisted of 1.2 megatonnes (4 x 300 kt).

One of the biggest concerns is the fact that the range of the missile flight reaches 11,000 kilometers. This means that her warhead can strike any object in the US.

Already in December last year, Deputy US Secretary of State for Armaments Control and International Security, Rose Gemehuller, called for new sanctions to be imposed against the Russian Federation, claiming that the Russian side allegedly violated the treaty for the eradication of medium- and low-range missiles (5500-1000 -500 km) since it covered the upper segment of the range.

The PC-26 is characterized by a quick and short start - the missile passes the acceleration start in less than 5 minutes. NATO ground assets in Europe will not even fix the separation of the warheads, which long before the goal "sinks" down is flying almost horizontally. The missiles themselves also constantly change the direction and height of the flight by making false targets.

RS-26 missiles are already ready for mass production, and this year the Rubege complex has to go into arms in the Russian army.

Russia has unveiled its largest nuclear missile that is powerful enough to destroy a country with French territory with one blow, world agencies report.

Russian leader Vladimir Putin wants to replace the arsenal of intercontinental ballistic missiles R-36 (the Nazi name SS-18 Satan) with a new super-missile RS-28 Sarmath.

This class of 5th-generation Russian strategic missile-based rocket complexes is equipped with between 10 and 15 nuclear warheads, depending on their power, according to the graphs revealed online by OAO "GPC Makeyev".

In case of 10 warheads the power is estimated at 750 kilotonnes each. The Hiroshima bomb has a power of 13 kilotons.

Western experts believe two missile options will be designed to hit targets in the United States and Western Europe. For the United States, the missile will have a range of 16,000 kilometers and West European countries 9,000 kilometers.

Hurricane and Nagasaki nuclear bombs thrown over Japanese cities are a "toy" compared to RS-28 Sarmath, which will enter the armed forces in 2018, according to experts.

In June 2011, the Russian Ministry of Defense signed a government contract to set up the complex, which will be part of

Russia's arsenal of nuclear containment and overcoming enemy missile defense.

Weapons experts in Moscow note that the complex will be able to overcome radar and be able to hit London or the East and West Coast of the United States.

2.3. Nuclear craft

The first submarine of the Borey project was listed on the Russian VMF on August 19, 1995 under the name St. Petersburg, but on 1 May 1996 its name was changed to Yuri Dolgorukii. Its construction began on 2 November 1996 and officially left the workshop on 15 April 2007. Its crew was formed in 2003.

On February 12, 2008, it was launched on water and on November 21 of that year its nuclear reactor was launched. Since March 2009, the nuclear submarine has been tested at sea. On December 17, 2010 is scheduled the first test launch from the submarine board of the newest Russian ballistic missiles "Bulava", which is intended to be equipped with all nuclear submarines under the Borey project.

If the Bulava trials on the Yuri Dolgokuriy board pass successfully, in Spring 2011, they will continue with the launch of two Bulava missiles (they start one after another within a few seconds). In the event of success, the underwater cruiser with his planned armament will be immediately admitted to the naval fleet of the strategic nuclear forces of the Russian Federation.

On 28 June 2011, the first experimental launch of the Bulava missile was successfully carried out on board the latest submarine. In mid-May 2018, four missiles were launched from the atomic submarine that hit targets in eastern Siberia. The launch has achieved the set goals.

A giant Russian underwater boat appeared in the Baltic Sea. It is part of the North Russian fleet and is on its way to St. Petersburg where it will take part in the naval parade. Its route passes along the German Baltic coast. The beaches are now full of tourists who have had the impressive opportunity to see how the black giant is in the sea. Against the backdrop of the world's largest nuclear submarine, on its way to Russia, sailboats look like toys.

The length of the Russian submarine "Dmitry Donski" - the heaviest underwater cruiser with strategic purpose, is 172 meters. Its crew consists of 150 to 180 people. The ship is equipped with intercontinental ballistic missiles. In 2015, Dmitry Donsky sailed from Severevikvinsk to St. Petersburg for a parade of Russian Navy. In order to reach the ultimate goal, the huge submarine must bypass Scandinavia and pass through the Baltic Sea.

The giant goes through the Big Belt - the most significant Danish Strait that connects the North with the Baltic Sea (Danish Storebælt), under the watchful eye of a Danish ship. He then took to the shores of Schleswig-Holstein and Mecklenburg-Western Pomerania.

Dmitry Donski, as well as the flagship of the North Russian Navy - the cruise ship "Peter the Great", are the largest in their class. The Russian Ministry of Defense has posted in Twitter a short video about the takeover of the submarine from Severovinsk. Residents of St. Petersburg will see this huge ship parade on July 30th.

3. Conclusions:

1. The development of Russia's nuclear weapons over the past decade has seen a significant increase in quality, and its technological level is ahead of the opponents.

2. International treaties and agreements on the development and distribution of this type of weapon are adhered to and progressing to a new class of weapons technology.

3. The development of nuclear weapons has a rather dissuasive effect.

4. Literature:

1. Dolchinkov N. T., N. B. Nichev, Characteristics of radiation, Revista academiei for țelor terestre NR. 2 (82)/2016;

2. Dolchinkov N. T., N. B. Nichev, Radiation background of the atmosphere, soil and water in bulgaria and its monitoring in the contemporary political conditions, Military sciences and national security, Sofia, 2017;

3. Vasilev D., Radioecology, Titus Consult, Sofia 2005;

4. Широкоград А. Б. Атомный щит России, Вече, Москва, 2017;

5. Широкоград А. Б. Энциклопедия отечественного ракетного оружия, АСТ, Москва, 2003;

6. Шунков В. Н. Артиллерия особой мощности, Харвест, Минск, 2004.

ANALYSIS OF THE RELATIONSHIP BETWEEN ENERGY DEPENDENCE AND NATIONAL SECURITY

Chief. Assist. Prof. N. I. Padarev PhD
 “Vasil Levski” NMU – V. Tarnovo, Republic of Bulgaria

nikolai_padarev@abv.bg

Abstract: Security is often commonly used and most meaningful concepts in contemporary political vocabulary. Furthermore, it has been engrossing in a fascinating subject in aspects of the survival of nations and states in the world. There is no doubt about the fact that energy security is factor influencing the security area. This paper analyses the impact of energy dependency in the World and in our country.

Keywords: SECURITY AREA, ENERGY DEPENDENCE

1. Introduction

In recent years, the issue of energy security has become more and more important. There are some concerns like a:

- depletion of petrol and other fossil fuels;
- reliance on other sources of energy;
- geopolitics (such as supporting dictatorships, increasing terrorism, "stability" of nations that supply energy);
- the energy needs of the poorer countries and the demands of developing countries such as China and India;
- discussing economic efficiency with the population;
- climate change;
- renewable energy sources and other alternative sources of energy,

energy insecurity, combined with other global problems, risks leading to conflict by repeating past mistakes in history.

The purpose of this report is a present a reasons for negative impact on security environment and ways to solve the problems.

2. Reasons for a Negative Impact of Energy Production on the Security Environment

The state of the energy industry is characterized by instability stemming from continuous increase in consumption and depletion of natural energy sources, accompanied by their harmful effects on environment. The energy sector is an area of the human activity that has a probably most devastating impact on nature. Bulgaria has a diverse power generation mix, including nuclear, thermal and water power plants.

Energy production, mainly from the conversion and combustion of fossil fuels, and the energy consumption of all economic sectors accounts for 79% of greenhouse gas emissions. Other greenhouse gas emissions are due to industrial processes other than energy consumption, agricultural practices or waste management. These percentages have remained largely unchanged since 1990. Electricity and heat production are share of 79% of energy includes, as well as fuel for burning fuels in industry, buildings, transport and agriculture. The next changes in the way we produce electricity and heat and in the way we use energy in our economy are essential to reducing greenhouse gas emissions. [12]

Since greenhouse gas emissions are mainly cause by energy production and consumption, energy efficiency can have a significant impact on reducing emissions. In addition, demand for energy investment and imports is decreasing and consumers save money. Energy efficiency is describe as the fastest and most cost-effective way to overcome energy security, environmental and economic challenges [13]. Therefore, a set of measures in a number of greenhouse gas emitting sectors [14] are defined in EU legislation and energy efficiency targets for 2020 and 2030 are set.

Energy dependence shows the country's dependence on imported energy and resources. It is defined as the ratio of energy imports and gross domestic energy consumption. Ha Table 1 are show energy consumption data by energy products in five years period.[1]

Table 1: Final energy consumption by energy products ^{Грешка!}
 Източникът на препратката не е намерен.

	2012	2013	2014	2015	2016
	Thousand tonnes of oil equivalent				
Total	9044	8597	8847	9367	9517
Industry	2576	2576	2608	2701	2634
Transport	2871	2604	2937	3255	3348
Others	3597	3417	3302	3411	3535
Agriculture, forestry and fishing	198	193	192	188	186
Households	2377	2257	2184	2213	2261

Bulgaria has greatly reduced its energy dependence - from 62.8% in 1990 to 34.5% in 2014. Eurostat are shows data in [2]. Energy dependence measures how much a country is force to import energy for its own consumption.

Total energy dependence for the European Union in 2014 was 53.4%, which means that it imports slightly more than half of its energy consumption. The development of the EU's dependence on energy imports is volatile, but the level has remained above 50% since 2004. [2]

Many people fear that the World is rapidly using a diverse but limited amount of fossil fuels. Some scientists fear that we have already reached a peak in the extraction and production of fossil fuels. The World relies petrol so much, for example, if there is a peak, or even peak is far away, it is ecologically, geopolitically and economically, and it is wise to invest in alternatives types.

On the one hand, exhaustion of fossil fuels, climate change Requires adequate environmental decisions for future generations. On other hand, the deepening global economic crisis, global hunger, food shortages and rising prices make it a matter of utmost to manage and recover waste, a huge source of which is agriculture and waste products (domestic, commercial , industrial, institutional, etc.). [3]

In recently years, issue of the environmental impact of energy has remained topical. It is difficult to assess value of energy production on pollution of nature and disturbance of landscape, destruction of plant and animal species. In the information sources [4, 5, 6, 7] are shows that data emissions from energy sources.

3. Ways to Improve Energy Security

Places like a Nigeria, Iraq, Iran, and so on are produce oil, but they pose problems to varying degrees for oil-consuming countries, as they cover stable supply and stable management. The other one, like a Venezuela, threaten to use oil and its associated profits to develop even their own country and region.

As more and more developing countries are industrializing, they will naturally want more energy to quench the thirst for growth. This will lead to greater involvement in international relations, and in fact, China and India are increasingly active in many regions of the world.

The future can also see resource conflicts. Dependence on fossil fuels and unnecessary resource use will worsen climate change, which threatens many of the world's ecosystems, will raise sea levels and affect food production, resulting in instability and conflicts caused by resource scarcity.

Nuclear power is one of the alternatives to fossil fuels that many countries are considering, given their efficiency and environmental friendliness during operation. Many environmentalists are afraid of the consequences of nuclear energy incidents and the inadequate storage of radioactive waste and say they are not worth it, but instead should invest in other alternatives for renewable energy.

The ownership of oil and natural gas from a number of countries is a way to change the security environment of countries that depend on them. In recently years, we have witnessed conflicts, violence and destabilization that hinder the development and security of vulnerable areas. [10]

In 2000, the European Commission launched the European Climate Change Program, which includes the following measures [8]:

- optimizing fuel consumption of the cars and energy efficiency of the buildings;
- increased renewable energy sources such as wind, solar, tidal power, biomass and geothermal energy;
- Reduction of the methane emissions from landfill.

According to Kyoto Protocol, the European Union has assumed responsibility of reducing greenhouse gas levels emissions by 8% to 1990 for 2008 - 2012. In this connection, the European Council also committed itself to a higher 30% reduction in greenhouse gas emissions by 2020 compared to 1990 as a contribution to a global post-2012 agreement [8]

Bulgaria fulfills the commitments under Directive 2001/81/E on national emission ceilings atmospheric pollutants, which include the achievement by 2010 and subsequent maintenance of total annual emissions for sulfur dioxide - 836 thousand kt/y; for nitrogen oxides - 247 kt/y; for volatile organic compounds - 175 kt/y; for ammonia - 108 kt/y. [4]

According to the contract of accession, between European Union members and Bulgaria, in 2010 Bulgaria committed to 11% of total electricity from renewable energy sources.

In the White Paper [9] states that alternative fuels are essential for both security of energy supply and reduction of negative environmental impact from transport sector.

In 2005, the European Commission issued a communiqué called "The Biomass Action Plan" in terms of:

- An increase in energy consumption in the transport sector, which does not allow for the reduction of greenhouse gas emissions;
- Undertaking by car manufacturers to commit to the introduction of new technologies in the car industry to reduce carbon dioxide emissions.

According to the National Security Strategy of the Republic of Bulgaria, the stability of the energy sector is a continuous process of providing vital public services for the functioning of society as a whole in the context of possible terrorist threats, natural disasters and major industrial accidents. The Republic of Bulgaria is interested in building a common EU energy policy. It supports the implementation of EU strategic initiatives to build the necessary infrastructure and diversify energy supply. Priority to ensure our

energy security is building and maintaining interconnections with neighboring countries networks as well as expanding the capacity of gas storage facilities.

The Republic of Bulgaria supports the development of international energy projects within the Southern Corridor, the first of which is the NABUCCO project, which is an EU priority. We also support the South Stream international energy project. Their implementation is accompany by security expertise - civil, public, environmental and national.

The development of nuclear energy is of strategic importance for our national security. The construction of new capacities is institutionally support, given that it is a promising resource for the production of emission-free electricity and due to the accumulated successful experience and professional capacity. Its development is strictly in line with the requirements for the management of nuclear waste and decommissioning and security measures.

Priority in energy security policy is to increase energy efficiency and promote energy savings. There is enormous energy saving potential in the country for its production, transmission and consumption. The energy security of the country and the improvement of the quality of the environment depend on the realization of the policy of the Republic of Bulgaria to increase the share in the energy production of renewable and alternative energy sources and the substitution of the electric energy with natural gas.

The country shall contribute to technological development in terms of efficiency in the production and deployment of clean coal technologies and to the application of technological achievements that are in line with European requirements and own economic capabilities. Our energy policy is based on a balanced approach to the integrated use of renewable energy sources, nuclear energy, natural gas, coal technologies and HPPs to ensure energy security and economic efficiency.

The Republic of Bulgaria carries out a clear and consistent regulatory policy to ensure the interests of national security, society and citizens in the operation and development of energy capacities, transmission and distribution networks. [11]

As a result of main sources of greenhouse gas emissions, policy of the European Union is aimed at: enhancing security of supply; ensuring the competitiveness of European economies and the availability of affordable energy; supporting environmental sustainability and combating climate change.

The European Union seeks to ensure that biofuels are produce sustainably, do not endanger the production of food and do not lead to deforestation or loss of biodiversity. All of this has given us a reason to summarize that the Community is striving for a comprehensive energy and environmental policy based on clear targets and deadlines for moving to a low-carbon economy and saving energy.

4. Conclusion

Although we cannot prevent all natural disasters, our preparation and responses to human impacts, can and should be improved. The possible restriction or even interruption of access to vital energy resources will have a severe destabilizing effect on the economy and the security environment, respectively.

Improving the environmental situation is a long and continuous process, an important part of the life activities of people in each country. In order to improve the environmental situation and the management of environmental security, both legislative and legal knowledge and actions, as well as knowledge and actions on the organization of its management at state, regional and corporate level are need.

5. Bibliography

1. <http://www.nsi.bg>
2. <http://ec.europa.eu/eurostat>
3. Blajeva V., European policy on biofuel development, governance and sustainable development, 3-4/2010.
4. <http://eea.government.bg>
5. http://old.europe.bg/htmls/print_page.php?id=5997&category=8&print=yes&page=8
6. Cvetkova S., Minkov T., Analysis and assessment of the environmental impact of transport on cities, Economic and social alternatives, Issue 3, 2017
7. Padarev N., Anthropogenic accidents and catastrophes. PIC, V.T. 2016.
8. http://ec.europa.eu/environment/climat/campaign/actions/what_iseu_doing_bg.htm
9. White Book - Adapting to climate change: a challenge for European agriculture and rural areas, Commission of the European Communities, Brussels, COM, 2009.
10. Shah, A., Energy Security, Global Issues. 2011.
11. National Security Strategy of the Republic of Bulgaria, 2011.

BEST PRACTICES IN CBRN WASTE MANAGEMENT IN MILITARY OPERATIONS

Chief. Assist. Prof. Nikolay I. Padarev PhD
Land Forces Faculty - "Vasil Levski" NMU – V. Tarnovo, Republic of Bulgaria
nikolai_padarev@abv.bg

Abstract: *Dangerous wastes are solid, liquid or gaseous materials that may be lethal or dangerous to humans and the environment. Such wastes can be toxic chemicals and flammable or radioactive substances, including industrial waste from chemical plants or nuclear reactors, agricultural waste, pesticides, fertilizers, medical waste or hazardous household waste such as toxic dyes or solvents. CBRN waste should be safely recycled without harm to the environment. Toxic chemicals, radioactive substances or biological materials should be concentrated for final disposal.*

Keywords: CBRN, ENVIRONMENT

1. Introduction

CBRN waste management is perceived as a set of actions toward the achievement of certain organizational goals through impacts on people and available but limited resources. In order to provide more opportunities with fewer resources, environmental management systems should be built. In their work in the performance of their assigned tasks of defending the political and economic interests of NATO member states, they interact with each other as well as with a number of external factors of political, economic and environmental nature.

Chemical, biological, radiological and nuclear (CBRN) risks represent a new dimension of possible terrorist attacks, accidents and / or pandemics due to their transnational character and mass scale of damage. An appropriate response to such a threat involves not only follow-up programs, but starts much earlier - dealing with such materials, their proper storage, limited access, checks, and so on. At same time, the interference subsequently requires wide-ranging cooperation between the different national authorities in a Member State (civil protection, military, law enforcement, etc.) as well as between national authorities of different Member States and EU instances. Therefore, a coordinated approach covering all risks is needed. [19]

2. CBRN Waste Management

Radioactive Waste Generation:

- Military programmes;
- Hospitals and research laboratories;
- Nuclear Energy Industry
 - Mining and milling of uranium ores;
 - reprocessing of fuel discharged from reactors;
 - decommissioning;

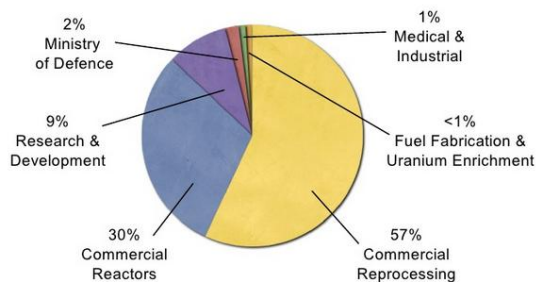


Fig. 1 Total conditioned waste volumes from each business activity⁵.

On fig. 1 there are a total conditioned nuclear waste volumes from each business activity. During the air strikes in 1999 NATO used ammunition with depleted uranium (DU) in FRY. It is known that the DU has a long time of semi-disintegration; actually its

effect is ever lasting. More than few years after the end of conflict, particles of DU dust can be detected in a soil samples, as well as in some air samples. Also DU was found in the sensitive bio-materials. In this material cytogenetic and clinical laboratory investigations in persons, who lived in Southern Serbia (Vranje) and on the Kosovo have been presented. The population of the contaminated regions should be subjected to annual screenings according to the program of the targeted examination aimed at detection of internal contamination in order to enable early diagnosis and treatment of the diseases. The particular attention should be paid to children and pregnant women, due to their increased radio-sensitivity. [1, 2, 20, 21]

In recent years, there has been growing concern that many of the most likely threats of chemical terrorism involve so - called "agents of opportunity." Both common and unusual industrial agents may pose a considerable threat as potential terrorist weapons. While an understanding of the traditional military chemical weapons (e.g. nerve agents) remains essential, an appreciation of the myriad of other potential toxic chemicals readily available in our society is crucial if we are to optimally prepare, identify and defend against chemical threats. Many toxic industrial chemicals are easily obtainable from multiple sources in our communities and pose a serious threat to health if accidentally released or intentionally disseminated. [3, 4]

In that context in military operations, everyone knows the pollution of environment with bio-waste. The environmental pollution is carried out during non-warfare, and even more so in combat operations. The management of bio-waste should not be overlooked for both radiological and chemical waste. The North Atlantic Treaty Organization (NATO) refers to "medical waste" as "healthcare waste." NATO's guidance on how such waste should be handled is contained in Annex C of NATO Standardization Agreement (STANAG) 2581 Environmental Protection (EP), Ed. 1, Allied Joint Environmental Protection Publication (AJEPP)-1 Environmental Protection Standards and Norms for Military Compounds in NATO Operations, 7 September 2011.

Planning environmental protection when managing CBRN waste should include: prevention, detection, preparedness and response. The importance recognizing of each of these four steps in dealing with CBRN materials is crucial to ensuring the proper implementation of risk assessment, response and countermeasures as a whole. It is also highlights need for a horizontal and cross-border approach to handling CBRN materials, resulting from the proper allocation of measurable objectives and actions in each of the three parts to which the action plan is divided.

It's should be emphasized that CBRN risks arise not only from countries but also from non-state actors, which is why the strengthening of the non-proliferation and disarmament regime is of the utmost importance through the universal and full implementation of all relevant treaties and international agreements, namely the Non-Proliferation Treaty, the Convention on Chemical

Weapons, the Convention on Biological Weapons, and by agreeing on a treaty banning the production of fissile materials for weapons of mass destruction.

In the conduct of military operations, it is influenced by various elements of the environment. To prevent the negative consequences of this impact, it is necessary to plan and implement a variety of procedures under the Alliance's policy in this area. Environmental protection activities should be organized in a way that does not interfere with the balance between the objectives of the operation and capabilities of the formations. The organization's policy requires commanders to provoke understanding of environmental issues in their subordinates and to organize the process effectively. The responsibilities of the Armed Forces to environmental issues are both the responsibility of society and of themselves.

Contemporary operations are they a peculiar challenge and radically different from the peacetime activities of troops. Although operational requirements are paramount in planning, it is imperative to take into account the need for nature conservation as it is important to ensure the health and well-being of the forces and the local population. Planning of environmental protection and subsequent management of the environmental risk of CBRN waste is essential to prevent damage to sites of natural, cultural or historical importance that will complicate the achievement of the mission's objective. Most military operations are characterized by clearly defined phases of varying lengths, depending on the nature of the operation, its intensity and complexity:

- Planning;
- Pre-deployment;
- Deployment involving task execution and rotation;
- Redirection;
- After conflicting recovery.

For the individual phases, applicability of the environmental protection standards that may effect on participants is determined. In this way, it is clarified how the extent of the deployment of the voices will affect performance of the CBRN events and how to best deal with the planning of the mission. It turns out that the degree of deployment has a direct impact on the applicability of environmental standards. [20]

Military environmental protection is not a stand-alone process, it is an integral part of operations. Inclusion in standard operating procedures also increases the level of force protection, and effective risk management can be seen as a factor in preserving the fighting potential of forces.

Releases of CBRN agents may negatively impact human health through respiratory exposure (breathing it in), contact with skin or mucous membranes (eyes or nose), or ingestion through food or liquids. Property can also be affected because if it is contaminated, it will not be available for use. Areas of the environment (for example wetlands, fishing areas, agriculture areas, or groundwater sources) can be contaminated from releases of waste. The commander is necessary to provide clearly defined environmental protection guidelines for conduct of a drill or operation as early as possible during planning. They are basis for defining the main purpose and specific tasks of environmental protection. They must comply with the requirements set out in regulatory documents and be defined as events before and after approval of the plan. They are regulate order of movement along the area, peculiarities of overcoming water basins, wetlands and water catchment areas, prohibited activities in disguising and engineering equipment of deployment areas and positions. The requirements for setting up field bearings, parks, food points and outposts, field stations for maintenance, repair and storage of armaments and equipment, fuel stations, ammunition storages and other types of property, as well as the order of action for the occurrence of accidents. Any restrictions

on the actions of the formation aiming at the protection of the environment are given on a map or scheme. [5]

NATO's joint doctrine on environmental protection and environmental protection during NATO-led military action provides guidance on the ecological planning of military activities. It sets out requirements for all commanders to effectively implement environmental events in organizing and conducting exercises and operations by NATO forces. It analyzes the operational activities to be carried out and their potential impact on environmental components, including various possibilities and contingencies.

3. CBRN Waste Management Capabilities

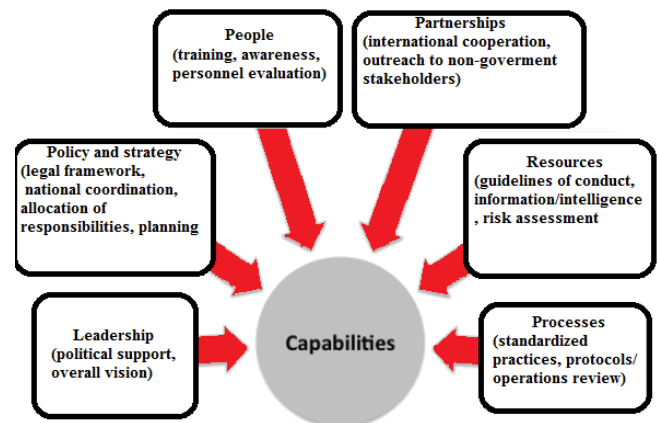


Fig. 2 Directions of developing capabilities for managing CBRN waste.

On the basis of an analysis of information related to waste management of radiological, chemical and biological origin there are on the Fig. 2.

4. Tasks in the CBRN Waste Management

Waste management is an integral part of environmental protection in the areas of operations. All waste is required to be managed in accordance with their hierarchy. Managing and handling is a logistical task. It requires pre-planning and appropriate financial support. To accomplish the task, all waste should be categorized. There must be places for storage of them by building temporary sites and equipping places for hazardous waste. Waste recycling opportunities are sought in local facilities.

The CBRN management plan can be part of an integrated waste management plan. Whether it is a stand-alone document or is part of an integrated plan covering the full range of wastes, the keys to a successful CBRN management plan are:

- Understanding what wastes are hazardous;
- Safeguarding waste throughout collection, transportation, and disposal;
- Assigning responsibilities and establishing procedures and standards for each aspect of the plan (segregate, collect, transport, recover, and dispose);
- Establishing the means to enforce standards through training, supervised execution, and inspections.

The CBRN waste management plan and standard operating procedures (SOP) must collectively address the proper characterization of CBRN waste as well as requirements for accumulation areas, container management, labeling, documentation, and recordkeeping instructions.

During operations, environmental specialists, medical staff and logistics specialists should consult the commander on a case-by-case basis. As before and during the deployment of NATO troops,

data on the ecological situation should be collected and documented. At the end of the military activities or during the re-appointment of the troops, the changes and the adverse consequences must be documented. [6, 9]

The commander bears all responsibility for the proper implementation of the waste activities. The aforementioned specialists must be assisted in assessing the situation when planning and conducting the training. Waste management plans and orders are drafted, indicating activities that prevent waste from spreading into the areas where the exercise is conducted. The plan reflects the order of organization of the interaction with the Regional Inspectorate of Environment and Waters and ensures full control of the waste management process.

At the waste management planning, account should be taken of the factors affecting CBRN waste such as geographic and topographic conditions, climate, population, waste management infrastructure, industry, industry and agriculture, as well as the quantity and nature of waste that would be the factors of the Environment were generated. The impact of specific ecological problems, the existence of risk areas and their adverse impact on the performance of the activities and the fulfillment of the tasks are also affected. [9]

Due to the nature of the combat operations and the CBRN environment, the forces must make efforts to collect, preserve, or otherwise dispose of the CBRN materials properly. Every effort can be made, but the situation may not allow that.

Recycling CBRN waste should be done in an appropriate and safe place to reduce the risk to the environment. If there is a CBRN waste, NATO operations must be reported to local authorities. The staff involved in managing CBRN waste must have sufficient knowledge and skills. They should be informed about the minimization of the harmful impact of the waste and its proper management. Suppliers of hazardous substances also play a role in waste minimization programs. On the regulations, it is permissible to assign functions of a radiation protection officer responsible for the storage, reporting and control of ionizing radiation and the accountability officer for incidents and accidents to an official such as the CBRN officer. He is assigned to act as a radiation protection officer. [18]

The ecologist of the formation is responsible for the waste management plan. He coordinates with:

- The lawyer of military formation;
- Logistics department;
- Engineers;
- The receiving nation;
- Different supporting countries;
- All services producing any kind of waste (for CBRN waste it would be a CBRN officer);
- Political leadership - on strategic waste management.

The ecological officer (EO) does not bear all these responsibilities unassisted. Examples of other officers and their responsibilities include the following:

- The health (medical) officer is responsible for medical waste management. The EO should coordinate closely with the health officer to ensure proper disposal of medical waste. (Note that a medical waste incinerator is included in the "disposal options" section of the solid waste technical module.)
- The logistics officer (who may be at a higher level rather than within the unit) is usually responsible for distributing, transporting, storing, and recovering (turning in) waste; the EO works with the logistics officer to ensure that subordinate units have the necessary equipment and materials needed to establish proper

hazardous waste accumulation points (HWAPs) and/or hazardous waste storage areas (HWSAs).

- The engineer staff officer, as the primary staff integrator for the environmental program which includes waste management, is responsible for integrating waste into the unit's overall waste management plan and incorporating the necessary tasks within operation orders and plans to ensure waste is effectively managed.

The CBRN Officer is responsible for the CBRN waste management process, which seeks assistance for the analysis of samples from a specialized CBRN Laboratory for Chemical, Dosimetric and Biological Analysis and Control or a link to the Military Medical Hospitals. In military operations, except for an active combat operation, all formations releasing CBRN waste are responsible for:

- Spill prevention;
- Proper collection of CBRN waste;
- Limiting the separation of CBRN waste;
- Locating / preserving containers storing CBRN waste;
- Control of leakage of CBRN waste;
- Marking of CBRN waste;
- Reporting when detecting the presence of CBRN waste;
- Transportation and disposal of CBRN waste as a logistical responsibility;
- Landfilling. [7, 8, 9]

The principle planning considerations for the location and storage of CBRN waste are:

- Being far enough away from sensitive environmental areas
- Avoiding areas that are subject to flooding
- Minimizing (or eliminating) adverse waste management operations risks

In making planning decisions about CBRN waste facilities, it is important to use all available information, such as the Environmental Baseline Survey (EBS), so that the necessary environmental information is taken into consideration.

The EO should coordinate with the safety officer so that there is ample space for expedient and unobstructed movement of personnel, material handling equipment, firefighting equipment, decontamination equipment, and spill control equipment.

The location, size, and number of hazardous waste accumulation points (HWAPs) within base camps and hazardous waste storage areas (HWSAs) within the theater will depend on: the amount of and location where waste is being generated; the availability of qualified contractors; and safety, security, terrain, and environmental considerations identified during the EBS. In terms of numbers, one HWAP will generally suffice for small base camps, depending on how much waste can be accumulated (based on final disposal procedures). In larger base camps with multiple large-sized units, there may need to be more than one HWAP. HWAPs are situated near where CBRN waste are generated in small quantities for a limited time, and are then moved to a consolidated HWSA as required.

As the EO, you have a responsibility to ensure that personnel are properly segregating different kinds of CBRN agents. He should know where to look for information about how substances should be segregated (such as SDSs), and ensure this information is conveyed to appropriate personnel, including training them on this issue. Segregation information can be found in a number of places. EO can obtain them from supply officer, the Safety Data Sheets (SDS), the manufacturer or from various websites, such as Internet.

SDSs list the hazardous characteristics for CBRN waste and are material- and manufacturer-specific. A Safety Data Sheet (SDS) is a document that provides information on the properties of hazardous chemicals/materials and how they affect health and safety in the workplace. They are material and manufacturer-specific. An SDS (also known as a material safety data sheet (MSDS), or product safety data sheet (PSDS)) is an important component of product stewardship and occupational safety and health. It is intended to provide workers and emergency personnel with procedures for handling or working with that substance in a safe manner, and includes information such as physical data (melting point, boiling point, flash point etc.), toxicity, health effects, first aid, reactivity, storage, disposal considerations, appropriate protective equipment, and spill-handling (emergency) procedures. It is important to have spill response plans in place, to have people trained in what to do in the event of a spill, and to ensure that these instructions are clearly posted in the storage areas. Even when people are well trained, having a poster that can quickly be reviewed in the event of an accident helps guarantee that proper procedures will be followed. [14, 15, 16]

The purpose of Allied Joint Environmental Protection Publication (AJEPP-2) is to provide NATO commanders and environmental protection (EP) officers with best EP practices and standards for military camps in NATO operations. The agreement of nations to use this publication is recorded in STANAG 2582.

Chemical, biological, radiological, and nuclear (CBRN) decontamination is the removal of CBRN material from equipment or humans. The objective of the decontamination is to reduce radiation burden, salvage equipment, and materials, remove loose CBRN contaminants, and fix the remaining in place in preparation for protective storage or permanent disposal work activities. Decontamination may be carried out using chemical, electrochemical, and mechanical means. Like materials, humans may also be contaminated with CBRN contamination. Changes in cellular function can occur at lower radiation doses and exposure to chemicals. At high dose, cell death may take place. Therefore, decontamination of humans at the time of emergency while generating bare minimum waste is an enormous task requiring dedication of large number of personnel and large amount of time. General principles of CBRN decontamination are discussed in this review with emphasis on radio decontamination. [10, 11, 12, 13]

5. Conclusion

Good CBRN waste management can be:

- Enhance mission accomplishment
- Contribute to force health protection by preventing
 - Direct health problems
 - Contamination of the environment
- Promote good relations with the host nation (HN)
- Free up resources for the mission (camp space, transportation, funds, etc.)

Military operations generate CBRN waste whose mismanagement can have people and environmental consequences. Although there are best practices have been found to present a health risk to personnel, they persist because they are viewed as expedient. Poor waste management practices on bases can lead to air and water pollution that affect communities living in proximity to installations, as well as military personnel and civilian contractors.

6. Bibliography

1. Sarap, N., M. Janković, D. Todorović, J. Nikolić, M. Kovačević, Environmental radioactivity in southern Serbia at locations where depleted uranium was used. US National Library of Medicine National Institutes of Health. 2014.

2. Federal Ministry for Development, Science and the Environment, FR Yugoslavia Report – The Consequences of NATO bombing for the Environment in FR Yugoslavia Belgrade. 2000.

3. Chemical Agents of opportunity for Terrorism: TICs and TIMs. Non-procedure participant guide. 2008.

4. Khan A., M. Sage, Biological and Chemical Terrorism: Strategic Plan for Preparedness and Response, Recommendations of the CDC Strategic Planning Workgroup. MMWR. 2000.

5. Medina, V., S. Waisner, Military Solid and Hazardous Waste - Assessment of Issues at Military Facilities and Base Camps. 2011. 358-376.

6. Velez, S., Ecological military aspects and protection of the environment. S. 2003.

7. AJEPP-1 Environmental protection standards and norms for military compounds in NATO operations. 2011.

8. AJEPP-2 Best environmental protection practices for military compounds in NATO operations. 2011.

9. AJEPP-3 Environmental management system in NATO operations. 2011.

10. Padarev, N., Danut-Eugeniu MOSTEANU, Decontamination of Hydrochloric and Nitric Acids. International Conference Knowledge-Based Organization. Vol. XXIV. Sibiu. Rom. 2018.

11. Padarev N., Peneva P., Tsvetkov D., Surface Activity of Solutions for Eliminating Radioactive Contamination, International Journal Machines, Technologies, Materials. Issue 5.2015.

12. Allied Joint Doctrine for NBC Defence – AJP-3.8. 2004.

13. Padarev, N., Selection on Nonionic Surfactants in the Decontamination Solution, International Journal Knowledge. Skopje. 2016.

14. <https://www.ncbi.nlm.nih.gov/books/NBK225528/> 20.11.2018.

15. https://osha.europa.eu/en/tools-and-publications/publications/reports/workers-participation-in-OSH_guide. 20.11.2018.

16. <http://www.hfscientific.com/MSDS>. 20.11.2018.

17. Roberts, J., Immobilisation and Storage of Nuclear Waste. Rough Guide to the Nuclear Industry. 2010.

18. Иванова, Г., Изисквания за радиационна защита в производствени обекти при дейности с уреди за технически контрол. НВУ том 5. В.Т. 2018. стр.156-164.

19. Лилов, И., Ж. Жеков, Г. Баев, Логистични методи и средства за сателитен мониторинг на околната среда. Международна научно-техническа конференция „Техника. Технологии. Образование. Сигурност“. В. Т. 2015.

20. Dolchinkov, N., B. Karaivanova-Dolchinkova, Radiation effect on human and living nature. International scientific journal: Science. Business. Society 5. 2016. стр. 59-61.

21. Dolchinkov, N., N. Nichev, Characteristics of radiation. Revista. Sibiu. Rumania. no.2 (82). 2016.

INFORMATION SECURITY AWARENESS IN CONTEMPORARY ORGANIZATIONS – CHALLENGES AND SOLUTIONS

Assoc. Prof. Popescu D. PhD
 “Alexandru Ioan Cuza” University, Iași, Romania
 rdaniela@uaic.ro

Abstract: Nowadays, we are witnessing a constant increase of cybersecurity-related threats and dangers. New trends such as monetization of attacks, their virulent propagation through social media channels, the abusive collection of data through interconnected smart things, with little concern for the privacy of the user, are expressed by the important security solutions providers around the world. In addition, the academic literature presents numerous real and proof-of-concept attacks and security problems that have a considerable impact in various domains. On the other side of the story, the organizations usually ignore privacy and security concerns, and there is a very low level of awareness regarding these issues. The need for related training programmes and educational curricula in this area remains almost unanswered. In this context, the paper analyses the security measures applied in contemporary organizations with the purpose of raising employees' cybersecurity awareness and discusses their effectiveness, using a sample of 25 small and medium Romanian enterprises, with the intention to identify the current and to propose future viable solutions for raising awareness and inducing ethical behaviour among employees.

Keywords: INFORMATION SECURITY AWARENESS, INSIDER THREATS, SECURITY TRAINING

1. Introduction

Today, the subject of information security (IS) has become very complex. Various types of tacit and explicit knowledge, from traditional fields as information and communication technologies (ICT), but also from business administration, human resources, psychology, finance and legislation, mix and mingle in this organizational area, transforming it in a very provocative one. The technical expertise of network administrators and other ICT specialists is no longer enough for protecting an organization, due to the complexity of human actions, organizational processes and regulatory policies associated with IS. Information assets' fragility and vulnerability increases steadily, as digital information can be easily copied, destroyed, or forged, as shown in [1] [2] [3]. New and ingenious threats occur in cyberspace every year, causing security breaches that determine financial and productivity losses, and forcing organizations to respond with updated security measures. In this context, is of utmost importance for organizations to be aware of the risks associated with the use of ICT in business processes and to positively address this issue by training employees in such a way that they understand the types of threats, risks and vulnerabilities specific to digital work environments and are able to apply appropriate security measures.

2. Literature review

The need for education in IS field has constantly been affirmed by academia, important security organizations [1] [4] [3] [5], and cybersecurity solutions providers [6]. In [7], creation of IS competencies is seen as a social and economic need, a critical cross-field outcome, a way to narrow the evident “information security gap” in universities and businesses. In order to prevent “a divide into Digital Elites and Analog Illiterates with dramatic consequences for societies”, in [8] and [9], cybersecurity education is considered an important step in assuring a sustainable development, a part of lifelong learning processes. Various solutions for active learning, with practical outcomes and useful hands-on experiences are proposed, e.g. gamification [10] [11], Web 3.0 ontologies [12] or cloud computing platforms that offer teaching staff and students (on-demand, elastic, dedicated, isolated, (virtually) unlimited, and easily configurable virtual machines [13]. Also, [14] highlights the need to ensure that employees are informed and aware of their obligations toward information security in organizations.

Our research question, based on the above formulated elements, is related to the extent in which users are aware of the IS threats and vulnerabilities in the organizations they work in, and what's their perception regarding the important security measures adopted and needed in organizations.

3. Methodology

The study was conducted in the framework of an elective course of *Information Security* taught at the Faculty of Economics and Business Administration of Alexandru Ioan Cuza University, Iasi, Romania to a group of up to 50 students enrolled in a non-ICT undergraduate programme. None of the students had prior experience in IS before the course and none of them attended any form of formal education in the field. The topics covered in the course are IS challenges brought about by computers and the Internet, importance of protecting information assets, key concepts in IS (e.g. information assets, risks, vulnerabilities, threats, confidentiality, integrity, availability, authentication, authorization), information classification, physical, logical and administrative access control measures, information security policies, data storage, backup and recovery, personnel security, encryption, steganography, systems security and some elements of network security, ethical and legal issues (software piracy, code of ethics, privacy law, copyright). After discussing the threats and vulnerabilities that may affect an organisation (based on ENISA framework) and the security measures recommended for a proper protection of data, information and knowledge during 4 meetings of 4 hours each, the students were asked to identify the most important threats and vulnerabilities recorded at their working place/in other known organisation, to present the security measures adopted by the organisation and to propose some new measures which they consider important for a better protection of information assets. Students were requested not to disclose any information or data that could possibly lead to the identification of the organisation. For this paper, the most comprehensive 25 reports were selected and analysed, with the intention to identify the most frequent threats and vulnerabilities the students became aware of after the class, the security measures they consider important, and their recommendations about possible improvements in IS in their immediate proximity.

4. Results and discussion

The most frequent threats identified by the amateur analysts can be categorized in insider threats (attacks and errors), malware, physical damage, and identity theft. Some example for insider threats, in students' own words, are the following:

“An IT employee, whose name was on the dismissal list, blocked the entire billing cycle, with the intention to persuade the manager in changing his mind and keep him in the company”

“Important documents were stolen and sold to interested third parties, due to the lack of passwords for each file”

"As the same laptop was used by many employees without any user accounts, so it happened that an employee deleted data of the others"

"Errors occurred in payrolls and order reports, caused by the insufficient ICT competencies of some older employees, who had problems in understanding the accounting software"

"Folders and files were deleted by mistake"

"A user did not check the ERP software' HASP protection key, which was not correctly entered into the computer. The employee worked on a demo version of the program, nothing was saved and the work had to be started over"

"By mistake, a folder with important documents was thrown away during a general cleaning period"

"During a faulty update of the accounting software, all existing data were deleted"

Also, disclosure of confidential information, as a consequence of missing non-disclosure agreements (NDAs), improper procedures and absence of IS trainings, and a laptop theft were noticed.

In many organisations, computer viruses caused „system malfunctions, data processing delays and financial losses“. In some cases, reinstallation of the operating system was necessary, in one organisation *"obscene messages were displayed in browser (title bar)"*. In a case, *"a fake antivirus software deceived an employee and, after he accepted to install it, the mouse and keyboard were blocked and the computer was repeatedly shut down"*. Other three cases of phishing were noticed, and four cases of ransomware – in one of those, the manager paid the reward for the decryption of organisational data, as no backup was available.

The physical damages were frequent enough. In two cases, *"a heavy rain damaged documents, cables, and computers"*. In another organisation, *"flood caused by a broken water pipe on the 1st floor deteriorated many documents and computers in the ground floor"*. Malfunctions in the power supply network are among the most important threats mentioned, *"because not all computers are protected by UPSs and information is lost"*. Due to the obsolete infrastructure, failures of the power supply are very common. They have a destructive effect on computer components, especially CPUs and hard drives. In some cases, data integrity was affected. In one enterprise, *"the accountant's laptop broke up due to a mechanical shock, and records for an entire month were lost"*.

Regarding the financial identity theft, *"there was an attempt to clone a card (manager's card), from Peru"*, and a successful money withdrawal from one company's account. Also, a situation in which usernames and passwords were stolen by a keylogger was identified.

Vulnerabilities observed by the students were related to:

- passwords: no, default or weak passwords, *"passwords placed on sticky notes and visible to any person who enters the room"*, *"access codes, passwords and keys are not changed after an employee leaves the organization for good"*;
- weak ISPs and procedures: software installation permitted to any employee; unrestricted access to Internet, *"making employees feel free to play games, watch online TV, use social media pages in their personal interest"*, unsecured portable computers (laptops), vulnerable to loss, theft and unauthorized data access, no backup policies/procedures, too lax BYOD (Bring Your Own Device) policies, *"USB sticks are used outside the organization, in unsecured computers, and then they become a malware access point in the organization's network"*; or, in the worst case, *"no policies/procedures at all"*;
- unaware, uninformed employees, due to the lack of proper ICT and IS knowledge and training: *"employees cannot distinguish between normal and spam messages"*, *"personal data are transmitted on unsecured channels"*;
- other vulnerabilities: untrustworthy employees, due to *"faulty recruiting and selection processes"*, unwary guardians, tired employees, dusty or humid environment, old computers etc.

Regarding the security measures in place, students mentioned firstly the obvious ones. The equipment (*"electric and non-electric fire extinguishers"*), materials and plans for fire intervention were noticed in all the organisations. Some organisations use gas detectors in archive and computer rooms, but only in one case, *"a quarterly training on fire extinguishing and work safety"* was mentioned. The usual physical access control measures observed were: fenced yard, keys (with some mentions that *"for spaces like organizations' archive or server room the key is doubled by a code"*), special attention to the main keys, video interphone, magnetic cards for employees (unique ID for each employee). In a case, the analyst mentioned that *"computer rooms are placed at a safe enough distance to production unit, because computers need to be protected from wastes generated by the fabrication of cotton clothing (especially lint, dust etc.)"*. Other noticed that *"the access of staff in certain areas of the unit is limited, based on a badge"*, and *"for some operations two people are needed because special information assets-related activities are done only in the presence of an authorized person"*. Many noticed that servers are located in special rooms, with restricted access, that the computer rooms have windows with bars, they are placed under video surveillance, and *"at night the buildings are secured by alarm systems"*.

Hardware protection measures noticed during the analysis referred to *"careful provision of spare parts and supplies for the computers"* and *"the periodical cleaning of the dust inside the CPUs"*. Students noticed that the organisations use licensed and updated software, antivirus software (but usually the basic, free version), they launch periodical scans for threats and they use firewalls for scanning the Internet traffic.

Identified backup procedures were diverse: weekly backup for accounting and financial data (with USB sticks and external hard disks as the most used supports), digital copies for the most important documents on paper (contracts, for example), periodic backups, *"with priority for data of the highest importance, such as: employee payroll, employee records (record of employment contracts and seniority)"*. In one company, *"periodic simulation of restoration from copies are made, together with logging of problematic events and defects, where possible, and permanent monitoring of critical equipment"*. In the event of maintenance or repair of the ICT equipment, a student noticed that *"all data is saved on external drives in order to avoid the access of unauthorized third parties, thus ensuring their confidentiality and integrity"*.

Passwords are used in various ways: passwords per employee and device, known by the user only – if a replacement is needed in an exceptional situation, a special authorization is issued, signed by an authorized person; complex password per device; username and password for financial and accounting software and for the wireless router. In three organisations, *"passwords are changed frequently (1 to 3 months) and every time after an employee leaves the organisation"*. In one case, *"digital fingerprint readers on manager's and accountant's laptops"* were signalled.

Correct document storage procedures were noticed in the majority of organisations. For example, in one company *"important documents are stored in cabinets equipped with locks, and only Human Resources and Financial Accounting departments' managers have the keys"*. In another, *"the documents are moved weekly in special boxes, which are then stored in a locked room"*. Most documents are properly archived – *"tagged, dated, placed in shelves on the edges of which the company name is written and moved in a separate room"*.

Digital signatures are largely identified in the analysed organisations, due to the fact that is mandatory for the accounting experts to submit the online statements on the website of the National Agency for Fiscal Administration (ANAF), using an electronic signature obtained through a digital certificate. It can also sign electronically and contracts, tax invoices, tax returns, reports and balance sheets. These electronically signed documents have the same legal value as paper documents signed and stamped. Moreover, being an electronically signed document with a digital certificate, they are much more difficult to fake than a stamp or a

hand signature. The electronic signature uses two security tokens and its PIN and cannot be forged, making it much safer than the handwritten signature. At the same time, the use of electronic documents is faster, cheaper and more efficient.

In the sphere of employees related measures, *"a careful personnel selection process was mentioned twice"*. In many organisation, at least a CV/resume and a verified recommendation from the latest workplace were requested. In one report was mentioned that, *"when elaborating the job description contract, security-related tasks are not skipped. Precisely to reduce the risks of human error, theft, fraud or abuse of trust, the implementation of security responsibilities starts from the recruitment stage. Personnel is also closely monitored"*. Other measures say that *"employees must have the necessary training for the job and comply with the internal regulations of the organisation and their job description"*; that *"they are required to keep important information confidential (in some cases through NDAs) and are not allowed to upload confidential data and information on external websites"*. When an employee leaves the job, for various reasons, *"he or she has to give back the mobile phone and the keys"*. In one organisation, the manager kept *"the workload in reasonable limits, as a way to help employees in working carefully, correctly and in an organized manner, providing accounting data on time and with a high level of integrity (as accurate as possible, in his words)"*. In another, ISPs are presented to every new employee, for the safe use of computing systems.

Only one mention was made about a specific training on ISP, probably on GDPR application. In the same enterprise, *"the manager periodically informs the personnel about malware, phishing, spam etc. The website uses a secured connection through https, digital certificate, restricted access at the administration page. In the organization there is a person in charge of maintenance of equipment and software and this specialist is responsible for training the personnel in the use of software. The loyalty of the employees is an important focus, in order to avoid the threats. Training occurs usually when new equipment or software is bought and installed. Registered threats are described and communicated to all the employees, they are also entered in a special register. The exchange of information and software between the different institutions with which there are collaborative relationships is monitored; the director of the organisation is following these exchanges to comply with the legislation in force; procedures and standards shall be established to protect data and information in transit which are initiated in Partnership Agreements."*

Other measures noted by analysts are computers' stand-by mode after a 20-minute period of inactivity, document shredders, supervised third-party access to computers.

The students came with recommendation for improvement of the IS in the analysed organisation, extracted from the course materials/inspired by discussions during the classes:

Proposed measures for access controls referred to *"the redefinition of access rights, especially for physical access in special-purpose rooms and offices (archive, server room etc.). The number of authorized persons in these special spaces should be reduced to a minimum value"*, *"digital fingerprint at the main entrance and other important rooms"*, *"no more default passwords for devices (routers or surveillance systems) and also for software"*, wireless surveillance system, movement sensors. Regarding the access to documents, *"a closed computer system that prevents the extraction / copying of documents, folders or any other confidential information from the computer and, when such an attempt occurs, the administrator is alerted"* was considered a good idea.

In many cases, *"the upgrade of the current antivirus to a better version, with anti-phishing, anti-ransomware, anti-spam protection"* was suggested.

In the personnel security area, following recommendations were made:

"Security courses regularly attended by employees, because everyone needs to know how to recognize a phishing message, know how to handle attached e-mail files, scan them and, very important,

report to the IT department any incident or situation that appears to be suspicious"

"Motivating and rewarding company employees with various bonuses or premiums to prevent them from leaving the company or disclosing important information to malicious outside people"

"Real and not formal communication between the staff responsible for organizational security and the rest of the employees"

"Raising employees' awareness of computer security, in order to prevent malware attacks"

together with *"a rigorous set of recruiting, selection, and hiring procedures"*, NDAs signing, *"adaptation of internal regulations to include rules on information security"*, and *"special training sessions for employees to prevent data loss"*.

Suggested ISPs revisions referred to *"no more BYOD"*, with a more focused advice, that *"employees who bring and use their own devices should be aware that a smart phone, tablet, laptop can be a big challenge for the company's IT department. It is important that every device that runs a different operating system has up-to-date security settings and is included in the company's secure network"*, and the monitoring of Internet activity for each employee.

In the communication area, students suggested *"a dedicated internal phone line and e-mail channel, to be used only inside the organisation when discussing confidential and secret information"*, and use of encryption.

Many references were made to backup procedures, as: *"investing in data backup and data recovery systems, as data in computing systems are vital to the firm"*, *"more frequent backup, for not-so-important documents also"*, *"a backup server/cloud solution"* or *"at least an UPS"*.

Other recommendations regarded *"written record of all services provided by the ICT Specialist, with date and signature on both sides, with all changes made to software and hardware"*, *"contracting cloud services for the future online store of the shop, as developing a home-based solution involves colossal costs to ensure the security of the information stored on it, compared to storing the site on an online platform where security and maintenance is ensured in a professional way by the hosting provider"*, and *"testing the reaction times of the security firm that has never been done since signing the contract with them."*

5. Conclusions

The threats, vulnerabilities, adopted and needed security measures identified by the students during the study were very ... earthly, unsophisticated and credible. Although the course largely presents sophisticated technical threats which are massively promoted in the media, such as Web Based Attacks, Web Application Attacks, Denial of Service, botnets, and adequate technical measures, these were ignored by analysts, as a result of their absence from the organizations under review. Their focus has been on the most common problems, frequently experienced in organisations, for which they have also selected the appropriate measures.

Beyond the modern and extremely interesting methods suggested by the literature, increasing the awareness of information security issues among SMEs' employees with a non-technical background can be done with modest means. The exercise we tried during the IS course had very good results: armed with minimal IS knowledge, the students analysed a familiar situation, in their immediate proximity, and presented the results using their own unsophisticated, natural language. The discussion which followed the analysis was in itself a good way to raise awareness at the level of our focus group. Good practices presented by each participant were saluted by the others, interesting questions arose, and some valuable lessons were learned during this workshop.

In conclusion, IS is rather a human problem than a technique one, and can be provided in a not very costly manner. Raising awareness amongst the employees and turning them into active

vectors, able to modify their own and their colleagues' behaviour regarding the IS are goals that can be achieved with a minimum investment in a basic IS course.

6. References

- [1] ENISA, *ENISA Threat Landscape Report 2017*, January 2018. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017>. [Accessed 1 February 2018].
- [2] DC, *DDC Reveals Worldwide Internet of Things Predictions for 2015*, 3 December 2014. [Online]. Available: <https://www.idc.com/getdoc.jsp?containerId=prUS25291514>. [Accessed 2 October 2016].
- [3] Royal Academy of Engineering, *Cyber safety. Strengthening the digital systems that support the modern economy*, Royal Academy of Engineering Prince Philip House, London, 2018.
- [4] ENISA, *The new users' guide: How to raise information security awareness*, European Network and Information Security Agency (ENISA), 2010.
- [5] Romanian National Computer Security Incident Response Team, *Awareness Guides*, 2018. [Online]. Available: <https://cert.ro/>. [Accessed 14 November 2018].
- [6] Bitdefender, *Whitepapers*, 2018. [Online]. Available: <https://www.bitdefender.com/>. [Accessed 14 November 2018].
- [7] L. A. Fitcher, C. Schroder and R. von Solms, *An Integrative Approach to Information Security Education: A South African Perspective*, Information Management & Computer Security, 2010, vol. 18, no. 5, pp. 366-374,.
- [8] B. Kooi and S. Hinduja, *Teaching Security Courses Experientially*, Journal of Criminal Justice Education, 2008, vol. 19, no. 2, pp. 290-307.
- [9] T. Osburg and C. Lohrmann, Eds., *Sustainability in a Digital World: New Opportunities Through New Technologies*, Springer, 2017.
- [10] A. Antonaci, R. Klemke, C. M. Stracke, M. Specht, M. Spatafora and K. Stefanova, *Gamification to Empower Information Security Education*, in GamiFIN Conference, Pori, Finland, 2017.
- [11] B. Endicott-Popovsky, *Information Security and Risk Management*, coursera.org, 2014. [Online]. Available: <https://www.coursera.org/course/inforiskman>. [Accessed 8 January 2015].
- [12] J. Van Niekerk and R. Goss, *Towards Information Security Education 3.0. A Call for Information Security Educational Ontologies*, in ISE 6, 7, and 8, IFIP AICT 406, IFIP International Federation for Information Processing, 2013, pp. 180-187.
- [13] K. Salah, M. Hammoud and S. Zeadally, *Teaching Cybersecurity using the Cloud*, IEEE Transactions on Learning Technologies, vol. 8, no. X, 2015.
- [14] Y. Alkhurayyif and G. R. S. Weir, *Evaluating Readability as a Factor in Information Security Policies*, in Proceedings of International Conference on Arts, Science & Technology, Dubai, 20-22 December 2017, 2017.

DEVELOPMENT AND IMPLEMENTATION A PLATFORM TO SECURE CYBER INFRASTRUCTURE AND OPERATION

PhD. Eng. Mircheska S.

Ministry of information society and administration, Skopje, Republic of Macedonia
mircheska.s@gmail.com,

Abstract: *Cyber security is a comprehensive area that covers the protection of assets from cyber crime which affect operations in organizations and is achieved through active monitoring, detection of interruptions or malicious activity and timely response to interference. Geo-spatial approach to cyber-security and technology development provides clear guidance and vision for contemporary data protection in the organization. The role of Geo-spatial technologies in support of physical security is well-known and intelligible and is used for situational information, multi-INT, synthesis, analysis and information exchange. Development of platforms enables organizations to implement these cyber defense concepts to quickly identify and prioritize cyber threats by creating a technical solution that integrates all existing data to reduce uncertainty.*

KEYWORDS: CYBERSPACE PROTECTION PLATFORM, GEO-SPATIAL SOLUTION, APPROACH AND CYBER-PROTECTION MODEL

Introduction:

Cyber security is importance part in any organizations such as business, records keeping, financial and so on. This information security will help the organizations to fulfill the needs of the customers in managing their personal information, data, and security information. There are a few challenges faced by the organizations in managing the information so that it would fall in hand of unauthorized person or hackers. Besides, an effective cyber security management system can reduces the risk of crisis in the organizations. All organizations must have their policies in secure their information so that the information can be kept safely. Cyber threats affect more than just the information technology (IT) infrastructure of a company or command. These threats cause disruptions to its entire network that can impact its principal business functions and mission. Cyber security should be assessed in terms of its direct contribution to the successful execution of an organization's primary mission. Organizations can no longer ignore cyber threats or delegate security to the information technology department. Cyber defense must be integrated into traditional security activities, such as physical and personnel security as part of an overarching effort to protect business operations from both external and internal threats. Cyber security activities must be prioritized and aligned to strategic business activities. With organizations increasing reliance on electronic communications comes the inherent risk of cyber attacks. The Government of USA issued an executive order that cyber systems (computers and related technology) be considered like critical infrastructure. The Department of Defense Joint Publication 1-02 defines Cyberspace as "The interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." The role of sophisticated technology in the support of physical security is well known and understood and it is used for situational awareness, data management, multiple intelligence (multi-INT) fusion, analysis, and information sharing. Physical security is interdisciplinary and relies on multiple sources of information. Cyber defense should be assessed in terms of its direct contribution to the successful execution of an organization's primary mission. Cyber security should be integrated with the various business functions it is protecting. However, in the past, this tight integration has been difficult to achieve. Arguably, the reason for its difficulty is the lack of a common framework that can align the activities of mission specialists with experts in all the other security-related activities required to provide full mission assurance. As businesses and individuals embrace technologies in their

everyday activities, software and technical solutions that try to protect us from cyber security threats have multiplied. Yet, despite awareness of cyber threats, advancements in cyber security technologies, and an increased number of national and organizational computer security incident response team to coordinate responses, both the frequency and costs of data breaches continue to rise. Humans remain the weakest link in the security chain, and investing in and developing cyber security cultures within organizations can decrease the human factor risk, imparting a positive impact on efficiencies and security while mitigating financial risks. Organizational leaders are increasingly concerned about the threat posed by cyber attacks and usually they aren't focused on the technical aspects of the event but they want to understand the impacts to their mission.

I. Security platforms important key to cyber security

Platforms are becoming a dominant force in business and software architecture. Platforms are increasingly becoming core features of the digital world and in different area like government, health or military/defense sectors. The platforms are at the center of digital systems. Today in the modern technological world, platforms have different technological structures and systems. They develop as highly specialized and expensive platforms that provide services. Platforms that are multinational provide multiple building blocks that accelerate growth and maintain systems. The deployment of a technology platform is cloud-based and software-defined. In addition, cloud infrastructure itself becomes a commodity. Highly virtualized cloud platforms dominate because of their huge advantages in automated, hyper-scale resource efficiency. The creation of platforms in organizations allows for solving important tasks that should previously be custom-built in any system or application as a cloud-based identity management system can meet the individual needs of hundreds of different services and systems that are or are available through this platform. Platforms encompass many of the cyber security roles that were previously implemented by separate systems or applications. The growing role of platforms requires adaptation of the system architecture and its offers significant improvements in cyber security.

Many authors define a platform as "a business based on enabling value-creating interactions between external producers and consumers." In the continually evolving digital era, platforms are causing some important shifts in focus. We are evolving from monetizing by selling a right-to-use license of a hard-to-make competitive service or capability towards extracting smaller pieces

of the recurring value from each of the massive numbers of interactions between producers and consumers in digital systems. The model for valuation of platforms becomes a function of the number of producers and consumers across a network provided the platform itself retains an ability to curate content and moderate network interactions. The focus thus shifts outwardly towards these interactions in a network effect between producers and consumers rather than inwardly on something being produced or licensed by the platform owner.

The requirements for security technology platform integration in organizations must include some minimal criteria:

- *Coverage from endpoints to data centers to clouds* - Platforms must provide comprehensive coverage that includes endpoints (i.e. PCs, mobile devices, IoT devices, etc.) and networks, as well as physical servers, virtual servers, and cloud-based workloads. The best platform offers strong integration with common threat vectors such as email security and web security. Many vendors or companies may not offer mobile or IoT device support in their security platforms today, but before purchasing from these companies, the responsible engineers should assess security technology platform to gauge schedules for future functionality and device support;
- *Prevention, detection, and response capabilities* - A security technology platform must greatly improve threat prevention when compared to today's point tools. Each individual tool should offer best-of-breed security efficacy, while the platform should provide incremental threat protection as more tools are glued together. Beyond threat prevention, each tool should also act as a sensor for collecting security telemetry. Platforms will be back-ended by some type of security analytics services that processes, analyzes, and acts upon this growing volume of security data. Security platforms must also offer well-defined and flexible options for responding to and mitigating threats, including automated and manual options. For example, the platform should be able to automatically find and block retrospectively installed files and IoCs when new threats (that include these files and IoCs) are detected in the wild or offer options for quarantining systems, deleting files, or restoring systems/workloads to a known good state;
- *Hybrid deployment options* - Today's security technology world includes ubiquitous cloud services, costly security operations, and data privacy concerns. Individual security tools and the platform management plane should be offered in on-premises and/or cloud-based form factors;
- *Cloud-based services* - Security technology platforms should include myriad cloud-based services for things like threat intelligence analysis/sharing, static/dynamic file analysis, reputation list compilation/distribution, machine learning modeling...;
- *Central management and reporting* - All individual tools must plug into a central management plane offering role-based access control that can be customized for different users, views, and functions. Management functionality must include policy management, configuration management, and detailed reporting from individual tools, from groups of tools, or across the entire architecture. Management data must also be easily exportable to other tools;
- *Openness* - Large organizations have established best practices around certain point tools and security technology platforms must be open for easy third-party technology integration by offering developer support, technology partnerships, and well-documented and standards-based APIs as a core part of their platform;

II. Developing a cyber security platform in organization

Developing a cyber security platform is the most important security for organizations. Cyber security is important to all businesses. The primary motivation for modern organizations to rely so heavily on cyberspace is that it allows them to efficiently, effectively, and economically coordinate activities across dispersed locations in near real time. Cyberspace is critically dependent on electromechanical devices and personnel that make up its components in the physical domain or layer. The benefits of cyber security are immense for not only companies but also their employees. No one organization wants to be a victim of a cyber attack so the role of cyber security in an organization is an extremely important one. The best way to ensure an organization will not become the victim of a cyber attack is to verify the organization has an effective security plan and security platform in place before any attack can happen. In organizations security breaches are constantly happening, sometimes multiple times a month, sometimes many times for a few days. A good security system protecting IT for businesses is the best defense a company can have against these cyber security threats. The importance of cyber security for a business is not just about their information being protected but also the information of their employees and customers. Companies have a lot of data and information on their systems. This fact adds to the importance of security, whether it is data security, information security or cyber security in general. Developing a security platform in organization is importance and there are many benefits of cyber security for a business organization. When it comes to cyber security, it is important for a company to not only train and inform the higher-ups but every employee, of the benefits of cyber security. When a company trains all of its employees about the benefits of cyber security, the company itself has less exposure to cyber security risks in the first place. A company will save money with cyber-related loss and severity of cyber security incidents when they offer their employees proper cyber security training. Another benefit of training employees is the time saved. When a company has fewer cyber security threats, the employees of that company will spend less time tracking down the treat, fixing it and possibly having to redo any affected work. When employees are properly trained, when it comes to cyber security, they develop a more positive company culture with regards to cyber and information security.

Cyber space consists of a complex mix of data, devices, and people and the virtual environment consists of four different types of network layers, each of which has nodes that are locatable in space-time. These include different type of data, device, network... Data layers are often assigned based on the type of node used, whether a person or device. However, it is useful to think of each node layer as being defined by its type of dataflow. For information to be exchanged at the social level, documents must flow in the device layer. For documents to be exchanged, packets must flow at the network layer. And for packets to be exchanged, electromagnetic energy flows between two specific points in space-time.

The technology and platform that can deliver these capabilities is available on many networks and from devices, providing personnel with access to information and data to support decisions for awareness, prevention, protection, response and recovery. Development platform can be quickly accessed, understood and shared to support coordinated actions. The platform combines location with cyber security activity and other data to better anticipate, detect, respond to and recover from threatening security incidents. The technology is easily integrated into an organization's existing command and control structure to ensure that leadership

has access to complete and accurate data for decision making. In fact, platforms are already widely used in national security agencies, including defense, national intelligence, critical infrastructure protection and emergency management. Integrating the power of location intelligence with cyber security data allows organizations to make better decisions before security is compromised, rather than when it is too late.

III. Implementing a platform and improving a cyber strategy in organization

The implementation of the security platform in organization is a complex process who involves more departments from the organization. The security platform includes more processes which are incorporated into the organization's security strategy; the platform represents part of the strategy and security policy. The team of IT security professionals who formed the organization after detecting that there has been a cyber attack on the organization, they must observe all aspects of the process. This team of specialists must find any device that has been compromised. Team members analyze malware and determine whether it affects all data or not.

PREVENTION - Identifying and mitigating vulnerabilities

Conventional defenses, including firewalls and antivirus software, remain an integral part of an organization's security lineup. They block the majority of standard attacks by hackers on IT systems, and curb the spread of malware. Additionally, educating employees on cyber security and potential threats is a key aspect of any prevention strategy. This added layer of protection is vital, as professional criminals can often exploit the human factor to pinpoint vulnerabilities and obtain network access. Furthermore, it is important to deploy products and IT solutions that are secure by design. And enterprises should determine what data is truly missioned critical – and ensure that robust defenses are in place for these key assets.

DETECTION - Simulating and analyzing attack patterns

Dissecting the tactics employed by hackers can help hone defenses, making them more effective. Companies should implement intelligent security management that aggregates information from a variety of sources – and analyzes it in real time to shield systems from novel attack vectors. The cyber security enterprise detects previously unknown, particularly dangerous vulnerabilities frequently encountered in popular programs. Furthermore, major corporations should analyze attacks in dedicated cyber security centers, and share their findings with others.

REACTION - Rapid response and robust recovery

There is no way to guarantee assets are 100 percent safe. Even when all available mechanisms are in place, criminals may still successfully infiltrate networks. Enterprises must be prepared for these scenarios – and have recovery plans ready, and cyber emergency response teams (CERTs) on standby. CERTs identify, verify and counter threats, detect and evaluate vulnerabilities, and manage security architectures.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 1: Function and Category Unique Identifier

Conclusion:

The role of cyber security in an organization is vital for the protection of its data and for ensuring that its services and projects will keep running without obstacles or delays. Modern organizations depend almost exclusively on computer systems for storing data, contacting customers and performing various tasks such as research, marketing and strategic planning. The financial success of an organization, as well as the successful implementation of its goals will depend on the health of its computer systems. It is vital that the systems remain free from intrusions from third parties who may attempt to gain unauthorized access.

- Charles, K. (2013). The C.I.A. triad or C.I.A. triangle and other security concepts. <http://www.securityorb.com/2013/10/c-i-a-triangle-security-concepts>
- Deutsch, W. (2014). 6 security policies you need: an introduction to creating effective security policies. http://bizsecurity.about.com/od/creatingpolicies/a/6_policies.htm
- ForeScout. (2014). Mobile security <https://www.forescout.com/solutions/mobile-security/>
- Garret, C. (2012). Importance of a security policy. <http://www.slideshare.net/charlesgarrett/importance-of-a-security-policy-11380022>
- Information Security Handbook. (2009). What is Information Security?. <http://ishandbook.bsewall.com/risk/Methodology/IS.html>
- Johnson, M. E. & Goetz, E. (2007). Managing Organizational Security: Embedding Information Security into the Organization. IEEE Security & Privacy, 2, 16-24. <https://www.computer.org/security/>
- Mellado, D. & Rosado, D. G. (2012). An Overview of Current Information Systems Security Challenges and Innovations. Journal of Universal Computer Science, 18, 1598-1607.

http://www.jucs.org/jucs_18_12/an_overview_of_current/jucs_18_12_1598_1607_editorial.pdf

8. MindfulSecurity.com. (2014). Why is Information Security Important? <http://mindfulsecurity.com/2009/07/01/why-is-information-security-important/>
9. OpenLearn. (2014). an introduction to information security. <http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-3>
10. Rossouw von Solms. (1998). Information security management (1): why information security is so important. Information Management & Computer Security, 6, 174-177. <http://www.emeraldinsight.com.ezaccess.library.uitm.edu.my/journals.htm?issn=09685227&volume=6&issue=4&articleid=862722&show=pdf>
11. Schneider, L. (2014). Information security: learn about information security. <http://jobsearchtech.about.com/od/historyoftechindustry/g/InfoSecurity>.
12. Slade, E. (2009). Top 3 Reasons Why Information Security & IT Maintenance is Important. http://www.howardcounty.com/Top_3_Reasons_Why_Information_Security__IT_Maintenance_is_Important-a-1224.html

MATERIAL MODEL PARAMETERS IDENTIFICATION OF BLAST ENVIRONMENT

M.Sc. Dubec B.¹, M.Sc. Stonis P.²
University of Defence in Brno, the Czech Republic ^{1,2}

branislav.dubec@unob.cz¹
patrik.stonis@unob.cz²

Abstract: In terms of designing or building new protective and security structures or equipment as a physical component of force protection, experimental verification of analytical or numerical calculations and vice versa becomes necessary. While the experiment can be performed on individual components, complex assessment of more complex variants or performing a parametric study is becoming more and more relevant in modelling and simulation domain. For this reason, there is a clear necessity to find the right connection between numerical simulation and experiment.

Fast, nonlinear processes require nonlinear material models to capture the rate of deformation and material behaviour under extreme loads such as the effect of explosions or the impact of a projectile, i.e. the effects, which the theories and practices of protection of the population and troops are trying to minimize. The important part of the accuracy of computational models is the correct identification of the parameters of material models used in the simulations.

This paper deals with the simulation of explosion and its effects and identification and optimization of material parameters of the environment in which the explosion and the shockwave propagates, with a focus on the soil material model. The inverse identification method is based on a combination of the experimental measurement data and the computational methods implemented in the finite element solvers and optimization programs. The simulation proceed from experimental measurement curves of blast effects. For measured parameter in the air overpressure at specific measuring points was chosen, while ground-propagating shock wave was evaluated by measuring acceleration values. The numerical simulation took place in the LS-Dyna software environment interconnected with the Optislang optimization program.

Keywords: LS-DYNA, INVERSE IDENTIFICATION, FEM, NUMERICAL SIMULATION, SHOCK WAVE PROPAGATION, SOIL MATERIAL MODEL

1 Introduction

1.1 Motivation

In present day, protection against the destructive effects of the explosion is in the spotlight. List of these effects is broad and, for this reason, the principles and methods of protection extend to different fields of technical sciences. Among the most important are the direct effects of the increased pressure present near the epicentre of the explosion [1], followed by the accelerated fragments and, last but not least, the shock wave propagated in the air in the event of the above-ground explosion but also through the material, into which the waves step in or in which the explosion itself occurred. For force protection and the ability to assess the protective properties and level of resistance of buildings and other protective structures, it is essential to know and evaluate the magnitude of the destructive factors. In case of the possibility of damage to both, protective structures and critical infrastructure due to intentional or accidental explosion, it is advisable to investigate the shock waves themselves as well as the pressure and acceleration values that this wave is causing [2].

Unlike the propagation of the shock wave in air, the propagation of waves through the soil is more difficult to assess due to great variety of soil and rock types, as well as is the assessment of its effects due to variety of types of construction and buildings and its foundations. This thesis aims to show the methods for a correct and effective way to correctly identify and evaluate the parameters of the soil affecting the propagation of the shock wave in the soil and contribute to improve numerical simulation possibilities. The simulation and parameter identification present in this paper is based on the field test result of [3] and aims to further extend the possibilities of prediction, evaluation and assessment of dynamic loading effects on infrastructure [4].

1.2 Blast Pressure and Acceleration in Soils

Soils are generally a three-phase air-water-rigid matrix system. The mechanical properties of this environment depend on the macrostructure, which is difficult to accurately describe as it can be described, for example, in isotropic homogenous materials like

steel. The plastic part of the material response plays an essential role. This is the main difference in soil and rock behaviour.

Another important loading response classification differentiate whether it is cohesive or incoherent soil.

Rock rocks can be considered to be a homogeneous, linearly elastic substance [5]. For soil, the mechanism of the deformation consist of two steps, which are being realized gradually. In the first phase, the solid component is deformed until the bond is broken. In the subsequent step, individual grains are shifted, compressed, and all soil components starting to work as one. This way the dry soils are damaged. In the case of soils with substantial contain of water under the shock loading, the loading is mainly transmits by the liquid component. The solid phase is applied only in units of hundreds to thousands of MPa or at a slower rate of loading when the water is pushed out of the pores [5].

In the case of shock loading caused by explosion, in the vicinity of the epicentre, the plastic deformations of the soils are far beyond the applicability of the Hook Law. Subsequently, a stable shock wave is formed that quickly loses energy and passes into elastic-plastic waves, which can be mathematically described. The effect and evaluation of such earth-waves on structures is the subject of discussion and various approaches, where most standards use a velocity amplitude value, after which the real possibility of a certain damage to the building and the categorization of the foundation soil is exceeded.

As the representative of the analytical prediction, opposite to widespread numerical simulations, the most used source of analytical assessment equations of the ground shock parameters The US Army Corps of Engineers Manual [1] can be mentioned. Working with the cube root scaled distance, two equations of the ground shock destructive effects, peak values of pressure and acceleration can be obtained as:

$$P_p = 0.407 f \rho_c \left(\frac{R}{W^{1/3}} \right)^{-n} \quad (1)$$

$$a_p = \frac{39.8fc}{W^{1/3}} \left(\frac{R}{W^{1/3}} \right)^{-(n+1)} \quad (2)$$

where P_p is the peak pressure (Pa), f is a coupling factor, which is dependent on the scaled depth of the explosion - $d/W^{1/3}$, where d is the depth of the centroid of the explosive charge, ρ_c is the acoustic impedance, c is the seismic velocity, R is the distance from the source, W is the charge weight; n is an attenuation coefficient, and a_p is the peak acceleration. Manual provides classification of 5 type of soils with corresponding material parameters for the equations (Table 1) [1].

Table 1: Mechanical properties of selected powder materials [1].

Soil type	Density, ρ (kg/m ³)	Seismic velocity, c (m/s)	Acoustic impedance, ρ_c (Pa · s/m)	Attenuation coefficient n
(1) Heavy saturated clays and clay shale	1920-2080	>1524	3,9-40,68	1,5
2) Saturated sandy clays and sands with air voids < 1 %	760-1984	1524	29,38	2,25-2,5
3) Dense sand with high relative density, wet sandy clay with air voids > 4 %	1744 1920-000	487,68 548,64	9,944 10,848	2,5 2,5
(4) Sandy loam, loess, dry sands and backfills	1984	304,8	4,972	2,75
(5) Loose, dry sands and gravels with low relative density	1440-1600	182,88	4,972	2,75

2 Experimental data

In order to perform the numerical simulation and a material model identification of the soil, experimental data has to be obtained and analysed. For this purpose, and experimental data acquired from the field blast tests performed by [3] were used. By the usage of buried accelerometers situated in one line in defined distanced positions from the explosive charge, a time-acceleration curves were obtained together with the velocity of the shock wave computed from the data. Simulation and identification is focused on the two peak values of acceleration. The setup of the experiment is described through the computational model, which accurately depicts the experiment (Fig. 1).

Table. 2 shows the setup of experiment and its results, where the explosive charge of equivalent of 15 kg TNT was situated 1.6 m under the surface together with minimal and maximal values of acceleration measured with two accelerometers situated in the distance of 13 and 23 meters from the explosive charge.

Table 2: Setup description and results of the experiment [3]

#	Weight of charge	Distance [m]		Acceleration min/max [m/s ²]	
		1	2	1	2
12	15	13	23	4.4/-5,43	0.89/-1,36

3 Computational model

The aim of this phase was to create a computational model and to perform a numerical simulation of the explosion shock wave propagation in the soil environment. The simulation in substantial parts copies the experimental layout, i.e. a setup where the aim is to measure the peak acceleration given to the shock wave loaded sensors.

The computation model was prepared as a 2D problem with one axis of symmetry [6], resulting into significant savings of the computing time. For discretization of the soil occupied space, the Multimaterial 2D ALE elements were used with elements of the edge length of 2 mm, where, after the initial calculation, the mapping values from 2D to 2D was performed on elements with a diameter of 5 mm. Subsequently, a material model from the LS-DYNA library with the number 147 MAT_FHWA_SOIL [7] was assigned to this part of the mesh.

The elastic properties of this soil are isotropic. The model is extended to include excess pore-water effects, strain softening, kinematic hardening, strain-rate effects, and element deletion [7].

The modified yield surface is a hyperbola fitted to the Mohr-Coulomb surface. At the crossing of the pressure axis (zero shear strength), the modified surface is a smooth surface and it is perpendicular to the pressure axis. The yield surface is given as:

$$F = -P \sin \phi + \sqrt{J_2 K(\theta)^2 + a_{hyp} p^2 \sin^2 \phi} - c \cos \phi = 0 \quad (3)$$

where P is pressure, ϕ is internal friction angle, $K(\theta)$ is function of the angle in the deviatoric plane, $\sqrt{J_2}$ is a square root of the second invariant of the stress deviator, c is amount of cohesion, J_2 is the third invariant of the stress deviator, a_{hyp} is parameter for determining how close to the standard Mohr-Coulomb yield surface the modified surface is fitted.

To generalize the shape in the deviatoric plane, the standard Mohr-Coulomb $K(\theta)$ function was changed to a function:

$$K(\theta) = \frac{4(1 - e^2) \cos^2 \theta + (2e - 1)^2}{2(1 - e^2) \cos \theta + (2e - 1)[4(1 - e^2) \cos^2 \theta + 5e^2 - 4e]^{\frac{1}{2}}} \quad (4)$$

where $\cos 3\theta = \frac{3\sqrt{J_3}}{J_2}$, J_3 is the third invariant of the stress deviator, $J_2^{\frac{1}{2}}$

e is the material parameter describing the ratio of triaxial extension strength to triaxial compression strength. The whole description of the model can be found in [7].

Creators of this model provide a comprehensive manual of the model together with filled Ls-Dyna material card in the manual, which is a great advantage and reason for usage of this model in numerical simulations, because in complex models many parameter values are unknown or are difficult to obtain from experiments, tests or other sources (Table 3). This set represented a starting point in the simulation and reverse identification process.

Table 3: Soil material parameters according to the manual, values for shear tests [7] (mm, kg, ms, GPa, kN).

*MAT_FHWA_SOIL							
MID	RO	NPL OT	SPGR AV	RHO WAT	VN	GAM MAR	INTR MX
222	2.350 E-06	3	2.79	1.00E -06	1.1	0.0	10
K	G	PHI MAX	AHYP	COH	ECC EN	AN	ET
0.003 250	0.001 300	1.1	1.00E -07	6.200 E-06	0.7	0.0	0.0
MCO NT	PWD	PWK SK	PWD	PHIR ES	DINT	VDF M	DAM LEV
0.034	0.00	0.00E -05	0.00	0.001	1E-05	6.0E- 08	0.99
EPS MAX							
0.80							

To simulate the explosion itself, an explicit approach to air and explosive modelling was used using multimaterial ALE formulation [6] of elements with assignment of the proper equation of state (EOS) to the used materials. In the initialization phase, the entire

ALE network was filled with air (EOS_Linear_Polynomial, Mat_Null, Table 4. and Table 5.).

Table 4: Air material model parameters (mm, kg, ms, GPa, kN),

*MAT_NULL							
MID	RO	PC	MU	TEROD	CEROD	YM	PR
555	1.235E-09	-1.235E-09	-1.0E-00	1.844E-11			

Table 5: Equation of state parameters for the air (mm, kg, ms, GPa, kN),

*EOS_LINEAR_POLYNOMIAL							
EOSID	C0	C1	C2	C3	C4	C5	C6
2	0.0	0.0	0.0	0.0	0.4	0.4	0.
E0	V0						
2.533E-04	1						

After the beginning of the simulation, the volumetric part of the soil elements were filled with explosive charge (EOS_Wilkinson_Lee, Mat_High_Explosive_Burn). (Table 6. and Table 7.)

Table 6: Explosive material parameters (mm, kg, ms, GPa, kN),

*MAT_HIGH_EXPLOSIVE_BURN							
MID	R0	D	PCJ	BETA	K	G	SI G Y
444	1.650e-06	6930.0	21.0	0.0	0.0	0.0	0.0

Table 7: Equation of state parameters for the explosive charge (mm, kg, ms, GPa, kN),

*EOS_JWL							
EOSID	A	B	R1	R2	OMEG	E0	V0
3	371.2	3.23	4.15	0.95	0.30	7.0	1.0

A 15kg TNT equivalent defined cylindrical charge was placed 1.6 m under the surface (Fig.1) [8]. For a more detailed record of the acceleration values at nodes distanced 13 m and 23 m from the charge, a database command was added for recording the peak values of acceleration. Both nodes were situated 1.6 m underground.

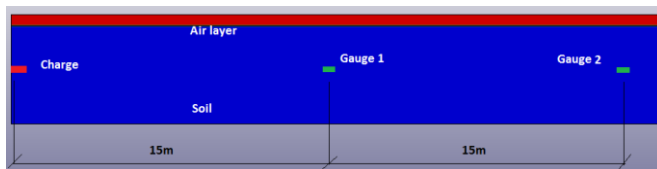


Fig 1. Computational model - setup

For the first step of the simulation, the simulation was launched on the fine meshed soil part to enhance the accuracy of the simulation. After that phase, the result were mapped [9] on more coarse mesh representing the whole setup due to significant computational time savings (Fig 2).

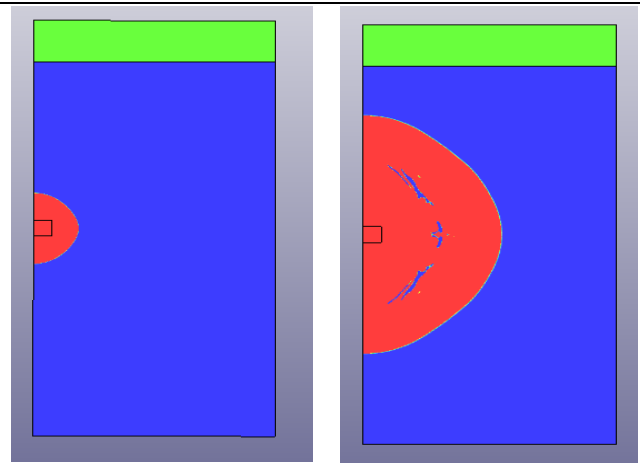


Fig 2. Propagation of wave – Initial step before mapping

On the Fig. 3 it can be seen the propagating wave has reached the final gauge point. At this time, the simulation was stopped and it was able to advance to the next step.

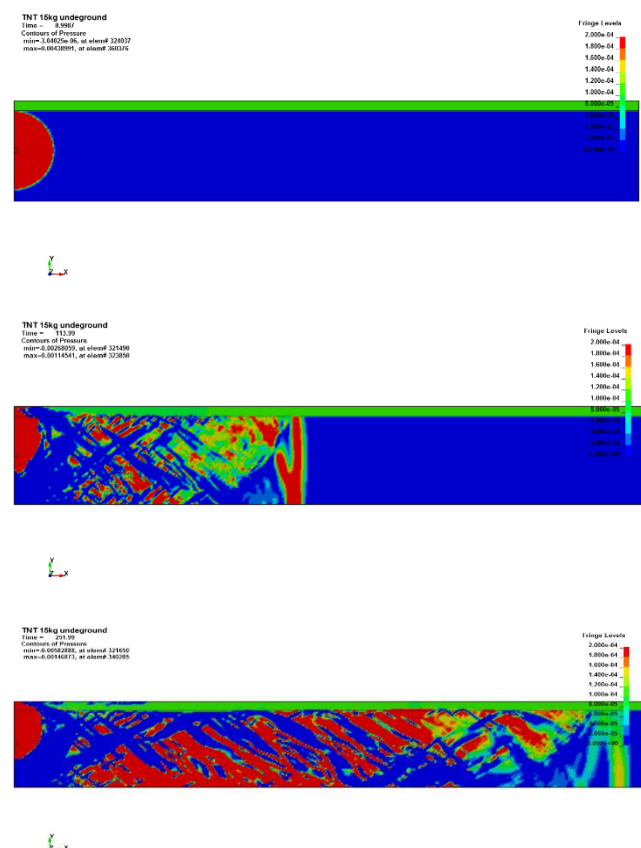


Fig 3. Propagating shock wave – pressure contours

Table 8 show the extracted peak values of acceleration in the gauge nodes.

Table 8: Setup description and results of the experiment and simulation

#	Weight of charge [kg]	Distance of gauges [m]		Acceleration min/max [m/s^2]	
		1	2	1	2
12	15	13	23	4.4/-5,43	0.89/-1,36
Simulation	15	13	23	4,8/-5,8	1,5/-1,4

4 Parameter identification

Inverse parameter identification is a set of methods and procedures used to find parameters in the material computational model used in the software environment of programs working on the finite element principle. Since only the exact values of the input parameters lead to the desired match of the simulation results with the experiment, finding them is a key part of the computational model creation. Inversion Parameter Identification of Maternal Model 147 MAT_FHWA_SOIL was used for text based interconnection of LS-Dyna and optimization software Optislang [9].

To simplify and reduced the computational time, four parameters of interest were chosen. Besides K - bulk modulus and G - shear modulus, $Dint$ - Volumetric strain at initial damage threshold and $Vdfm$ - Void formation energy, parameters connected with high strain effect and values of pressure, effects presented in the blast loading, were chosen for parameter identification with corresponding ranges of variability. $Damlev$ - Level of damage that will cause element deletion and $Epsmac$ - Maximum principal failure strain were set to values of 1 due to necessity of conservation of energy and ability to secure the propagation of the wave [7].

The objective function was set simply as the sum of squares of differences between the numerically-simulated maximal values of nodal acceleration obtained from text output database and corresponding experimentally measured maximal acceleration values from the field test. To minimize those function, and evolutionary algorithm was chosen [10].

A comparison of the values of acceleration and together with the newly found material parameter card in LS-Dyna can be seen in Table 9. and Table 10. It can be seen, that in order to increase the values of nodal accelerations in gauge points, it was necessary to increase the values of input parameters. Some of them in the order magnitudes compared to the initial values.

Table 9: Setup description and results of the experiment and simulation, and parameter identification

#	Weight of charge [kg]	Distance of gauges [m]		Acceleration min/max [m/s^2]	
		1	2	1	2
12	15	13	23	4.4/-5,43	0.89/-1,36
Simulation	15	13	23	3.51/-3.6	0,42/-0,83
Simulation - optimized	15	13	23	4,8/-5,8	1,3/-1,4

Table 20: Soil material parameters after the inverse parameter identifications (mm, kg, ms, GPa, kN)

*MAT_FHWA_SOIL							
MID	RO	NPL OT	SPGR AV	RHO WAT	VN	GAM MAR	INTR MX
222	2.35 - 06	3	2.79	1.00E -06	1.1	0.0	10
K	G	PHI MAX	AHYP	COH	ECC EN	AN	ET
0.01750	0.00822	1.1	1.0E-07	6.200E-06	0.7	0.0	0.0
MCO NT	PWD 1	PWK SK	PWD 2	PHIR ES	DINT	VDF M	DAM LEV
0.034	0.00	0.00	0.00	0.001	1.9E-03	5.0E-02	1.0
EPS MAX							
1.00							

5 Conclusion

Inverse parameter identification of material model parameters of soil were performed in this paper. The problem of wave propagation in the soils is very complex and with combination of extreme loading caused by explosion pose a challenge for material modelling. The more complex the model is, the more stand o necessity to exclude the some parameters from the identification process to secure reasonable computing time. Another restricting condition for the accuracy of the results of the simulation is the computational model and its complexity together with refinement of the finite element mesh. More complex field tests and parameter identification is necessary for other cases of blast loading [11]. Identified values of the parameters of the soil model represent a way how to simulate effects of blasts in the soil and can be used to assess the damage of the facilities and infrastructure buried or in contact with the soil ground [12, 13]. To assess the effects of blast loading on the laid critical infrastructure is the goal of the next simulation and experimental study of the authors.

6 References

- [1] Department of the Army, Fundamentals of Protective Design for Conventional Weapons, Technical Manual TM 5-855-1, November 1986.
- [2] Hejmal, Z., Mañas, P., Štoller, J., 2016. „Measurement and numerical simulation of the effects of an explosion on HPFRC slab". Pp. 881-884 in Proceedings of 20th International Scientific Conference Transport Means 2016, Part III. Kaunas, Lithuania: Kaunas University of Technology.
- [3] Moravcik, M.: Návrh pracovního postupu měření a výpočtu šíření tlaku v zeminách (Master's thesis). University of defence in Brno, Faculty of military engineering, 62p, Retrieved from (Accession No 20d7aade-ab41-4648-acba-ac86ab380e98 / 6894)
- [4] Štoller, J., Dvorak, P., Turo, T., Zezulova, E.: Basic Principles of Critical Infrastructure Protection. In: PROCEEDINGS OF THE 22nd INTERNATIONAL SCIENTIFIC CONFERENCE. Kaunas, Lithuania: Kaunas University of Technology, 2018, p. 267-271. ISSN 2351-7034.
- [5] Henrych, J. Dynamika výbuchu a její využití. 1. vyd. Praha: Academia, 1973.
- [6] LS-DYNA, Theory Manual, Livemore Software Technology Corporation, Livemore, California, 2015
- [7] Lewis, B.A. (2004) Manual for LS-DYNA Soil Material Model 147. No. FHWA-HRT-04-095, FHWA, Washington DC.
- [8] ANSYS, ANSYS Mechanical Theory Reference Release 15.0, 2014
- [9] LS-DYNA, Keyword User's Manual, Livemore Software Technology Corporation, Livemore, California, 2015
- [10] optiSLang, Methods for multi-disciplinary optimization and robustness analysis, Dynardo, Weimar, Germany, 2014.
- [11] NATO Standardization Agency. STANAG 2280 *Design threat levels and handover procedures for temporary protective structures*. Brussels, Belgium, 2008.
- [12] Davison, L., *Shock physics in solids an introduction*. Online-Ausg. New York: Springer, 2008. ISBN 978-354-0745-693
- [13] Albert, D., Taherzadeh, S., Attenborough, K., Boulanger, P., Decato S. Ground vibrations produced by surface and nearsurface explosions. Applied Acoustics. 2013, 74(11), 1279-1296. DOI: <https://doi.org/10.1016/j.apacoust.2013.03.006>. ISSN 0003-682X.

FAST PROTOTYPING IN THE MANUFACTURING OF COMPLEX ARMAMENT PARTS

БЪРЗО ПРОТОТИПИРАНЕ ПРИ ПРОИЗВОДСТВОТО НА СЛОЖНИ ДЕТАЙЛИ ОТ ВЪОРЪЖЕНИЕТО

Assoc. Prof. Ing. Ganev V. PhD.*, M.Sc. Ing. Dimitrova Ya.**; M.Sc. Ing. Antonov S.***

Faculty of "Artillery, air defense and CIS" – National Military University "Vasil Levski", Veliko Tarnovo, the Bulgarian Republic

* vvganev@abv.bg, ** dimitrovax2yana@gmail.com, *** stamantonov@abv.bg

Abstract: Virtual prototypes or virtual 3D models of complex armament parts reduce costs and production time with minimal risk of hidden flaws, testing and analyzing the construction before creating real physical prototypes or optimizing parameters in parallel with the physical prototypes. The report presents the possibility of rapid prototyping through the virtual 3D model of the SPG-9 breech and using additive manufacturing to obtain a functioning physical prototype.

Keywords: FAST PROTOTYPING, 3D MODELING, ADDITIVE MANUFACTURING.

1. Introduction

Reduction in cost for the production of complex armament elements (special elements) can be achieved by making prototypes of the needed elements, increasing the quality of the production process and reducing the costs, design and implementation times of the products as a whole.

Prototypes can be both physical and virtual. Virtual prototyping as a technology involves the creation and use of virtual models for presentation, testing and analyzing of particular details before creating the real physical models or optimizing parameters in parallel with physical prototypes. Physical prototyping involves the creation of element models including functional ones in small quantities compared to the manufacturing ones. When a combination of the two technologies is possible significant reduction in costs and production time can be achieved with minimal risk of hidden deficiencies occurring in series production.

Suitable platforms for the creation of virtual models are CAD / CAM systems for designing and manufacturing of special products.

2. Research

2.1. Purpose: Exploring the possibilities for rapid prototyping of special complicated armament components manufacturing.

2.2. Tasks:

- Analyzing types of rapid prototyping;
- Researching the possibilities of rapid prototyping for special manufactured products.

For the purpose of the study the mechanical processing and the equipment necessary for manufacturing the breech of the SPG-9 anti-tank grenade launcher will be reviewed.

Steel with the designation OXN3MFA is used for manufacturing the detail for the SPG-9 breech. Required output dimensions of the material for a single breech are $\varnothing 195 \times 230$ mm at a mass of 51,190 kg.

The manufacturing technological process includes a total of 23 machining operations - 11 mechanical processing, 5 tuning operations, 1 heat treatment, 1 galvanic processing and 5 control operations performed on 7 specialized and universal machines using 10 fittings and over 60 tools.

Different and various questions arise in the implementation of various stages a quick and effective solution is to design a prototype of the product through Virtual Engineering without making a physical prototype. Whereupon design and validation activities are carried out jointly to ensure optimization and testing of products prior to their actual realization.

The virtual prototype is a computer model that allows simulation with a functional realism similar to that of the physical object.

Virtual prototypes allow: research and verification of functionality and performance with the help of specialized software and hardware; Finite Element Analysis; Computational Fluid Dynamics; Kinematic and dynamic analyzes; Reliability Analysis and Failure Mode and Effect Analysis; Planning and simulation of production; Manufacturability; Assembly Analysis; Manufacturing Management; Human Factor Analysis.

The natural environment of the virtual prototype is Virtual Reality. The virtual prototype is the core of the Virtual Reality. Virtual Reality is an artificial computer-generated environment that simulates to a great extent and with extreme credibility the real world around us and gives the user the ability to manipulate and interact with virtual models that behave like real objects. Depending on the degree of human involvement the virtual reality is Desktop VR, Projection VR or Immersive VR.

The advantages of virtual prototypes and models are the reduced cost in initial design stages, increased possibilities for alternative design in the virtual environment and rapid accumulation of design experience.

Physical prototyping involves the creation of a functional product model in small quantities compared to the final product quantities in its industrialization and commercialization.

Once created physical prototypes are difficult to change. If changes are necessary, this will lead to the development of new models i.e. requires extra time and investment.

Rapid prototyping technology (RP) is a sophisticated manufacturing technology that creates material models from CAD data through 3D printers. Different types of rapid prototyping systems have different molding principles and system characteristics due to different molding materials. Different systems can directly receive product design (CAD) data without having to prepare tools and tooling and quickly make samples, matrices or new product models. Therefore, applying RP technology can significantly shorten the product development cycle, the cost of developing and improving the quality of development. Most prototypes require three to seventy-two hours depending on the size and complexity of the product which is much faster than a few weeks or months to produce a prototype through machine production.

Adaptive manufacturing (AM) is a technology that allows for three-dimensional layer detail manufacturing by a layer of material based on polymer or metal. The design of the detail in the form of a CAD model file is loaded into the adaptive manufacturing machine (or 3D printer), which then produces the component.

The adaptive manufacturing technology used by most 3D printers is based on modeling by depositing plastic material such as Stereo Lithography-SLA, Digital Light Processing, 3D Printing, Polyjet technology, Inkjet and Fused Deposition Modeling is not suitable for the creation of the SPG-9 breech.

The main methods for direct 3D production of metal details are: Selective laser melting - SLM (Figure 1) and Laser Engineered Net Shaping - L.E.N.S. (Figure 2) both applicable for manufacturing the SPG-9 breech.

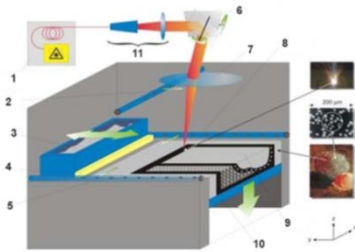


Fig. 1 Selective laser melting –SLM

1 - Laser; 2 -Processing gas jet; 3 –Material tank; 4 - Roller; 5 - Inlet of gas; 6 - Mirror; 7 - lens; 8 - Output gas; 9 - Layer material; 10 - Mass; 11 - Direction of the beam.

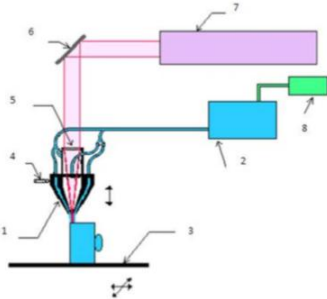


Fig. 2 Laser Engineered Net Shaping –L.E.N.S.

1 - Extruding head; 2 -Powder material; 3-table; 4-Inlet shielded gas; 5 - lenses; 6 - Mirror; 7 - Laser; 8 - Transportable gas.

3D models are created with computer aided design (CAD) via a 3D scanner or a simple camera with specialized software to measure the distance and size of the subjects in the picture. Regardless of the object modeling software used the model must be converted to .STL or .OBJ format. In order for the software responsible for printing the model to process the information.

Then the STL file is processed by software that converts the model into very thin layers and creates a G-code file containing specific instructions for the type of 3D printer used and the detail can be printed. In accordance with the instructions given the printer sequentially applies the material layer by layer. In this way, the pattern is created by the overlay of multiple layers. These layers represent the sections of the object from the CAD model connected to each other to form the shape of the final object. Depending on the size and complexity of the object this process may take from minutes to days. The advantage of this way of printing is that almost every possible form can be created.

The resolution of the printer determines how thin each layer and the detail of the object can be. Typically, 1 layer is about 100 μm (250 DPI) although some printers can reach up to 16 μm (1600 DPI). Which is comparable to the resolution of a laser printer.

3D принтирането предлага значителни предимства пред традиционните производствени процеси, като CNC механична обработка и леење, като позволява на производителите да консолидират в един единствен процес различни производствени операции, които преди са изисквали сложни и скъпи производствени процеси.

3D printing offers significant advantages over traditional manufacturing processes such as CNC machining and casting.

Allowing manufacturers to consolidate a variety of manufacturing operations in a single process that previously required complex and costly manufacturing processes.

In material-like production unlike traditional production only as much material as it is actually needed for the object itself can be used. With good design and architecture, the loss of material can be reduced to a really negligible minimum often as few as couple of grams.

The new printing materials are far lighter, stronger and more durable than conventional ones. There are high-performance printers that can be used directly for manufacturing details.

3D printers printing with metal offer direct production for details with great complexity removing costly tooling and shortening the time required for preparation and subsequent processing.

The main advantages of 3D printed metal models are: freedom in details design, fewer joints, reduction of workpiece weight by merging, greatly shortened production time, reduction in the cost of prototypes and small detail series, high metal density of the parts - 96-100%, a great variety of metals and alloys, high repeatability and precision of workmanship and handling of biocompatible materials - cobalt / chromium and titanium.

The creation of a physical prototype of the SPG-9 breech can be achieved by the use of additive manufacturing for metal parts.

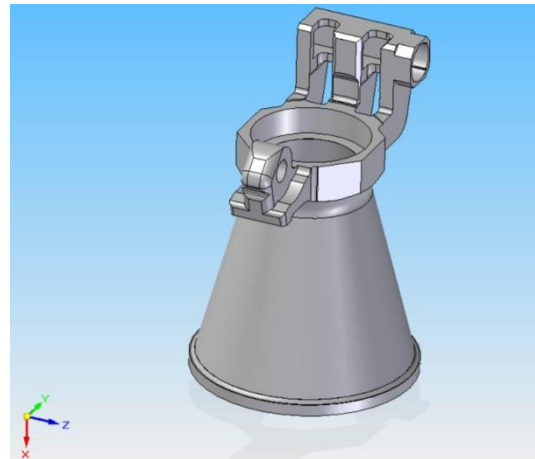


Fig. 3 Model of the SPG-9 breech.

Continuous technology development for additive manufacturing allows for the creation of finished details (including almost 100% dense fully functional constructions) through a one-step process. Additive manufacturing systems are becoming more and more reliable and efficient and the range of suitable materials has grown considerably compared to the first truly applicable manufacturing practices in the field.

Powder bed and direct powder-like layer processing technologies, known as laser melting systems are commercially available under various trade names such as: systems for selective laser melting (SLM), laser mixing and direct metal laser sintering (DMLS). The only exception from this principle is the electron-beam melting process (EBM), during which an electron beam is used under a vacuum.

The variety of available materials for additive metal manufacturing is constantly expanding. Stainless steels, aluminum, nickel, cobalt-chromium and titanium alloys are most often used, and a number of AM manufacturers also offer their own proprietary materials.

Research institutes, universities and AM systems manufacturers are already developing and offering customized materials tailored to the needs of client applications. Not all existing metal materials can be used for the additive production of parts but in most cases, and in the presence of suitable equipment, a metal powder can be created

for each model - a raw material for manufacturing the necessary products.

The wide variety of materials offers users a great deal of choice for the right material to meet the desired product specifications.

Common properties of metal powders suitable for AM are the spherical geometry of particles obtained from gas atomization and particle size distribution depending on the thickness of the layer, typically between 10-50 μm .

Material properties such as tensile strength, hardness, and elongation coefficient are used as reference points for deciding the suitability of the material.

In order to achieve the required specifications or to improve the properties of the manufactured parts, such as surface quality, geometrical accuracy and mechanical properties, additional processing is often required after the additive process.

The high quality of the metal products produced by additive manufacturing allows the application of different finishing technologies for metal surfaces to meet the surface quality and geometry requirements.

After removing the supporting structures and separating the obtained parts from the construction platform they can be milled, perforated, polished, etc. Heat treatment is often included in the process chain as well as the "shot peening" technology (a high-tech adhesion process carried out by a stream of solid particles). These techniques are used to improve the mechanical and tactile properties of the surfaces of the additively manufactured parts.

Electropolishing significantly improves the surface quality of AM produced parts during the finishing treatments. Its main purpose is to minimize the micro roughness thereby reducing the risk of them retaining dirt and debris and material leftovers on the surface of the detail and improving its cleanliness.

Electroplating can also be used for degreasing, coloring and passivation, especially for surfaces exposed to abrasion. Since electroplating does not involve mechanical, thermal or chemical action, small and mechanically fragile parts can be processed.

The process of designing metal parts produced through AM typically involves the use of topology optimization software to determine the place of deposition of the material and the areas from which it can be removed. From the low stress areas, material is removed until the finalized construction is created and optimized for load-bearing parts.

Because of the limited size of modern AM systems, the production of large-dimensional structural elements with them is also somewhat limited. The dimensions of the chambers of the typical industrial AM metal machines are approximately 630 x 400 x 500 mm.

A suitable equipment for the manufacture of a SPG-9 breech using the additive manufacturing method of metal details is the 3D Systems ProX Direct Metal – printers for direct printing of metal models.



Fig. 4 3D Systems ProX Direct Metal.

The 3D printers ProX Direct Metal of 3D Systems produce metal parts and high density metal casts from a wide range of materials with proven mechanical properties.

The ProX DMP 100, 200 and 300 printers include flexible settings for parameter control. These open systems offer users the ability to develop parameters and are able to use any material in addition to the ready-to-use alloys of 3D Systems. The ProX DMP 320 printer, with replaceable production modules, allows for fast material change according to the printer configuration.

	DMP Flex 100	ProX DMP 200	ProX DMP 300	ProX DMP 320
Build volume (W x D x H) ¹	3.94 x 3.94 x 3.15 in (100 x 100 x 80 mm)	5.51 x 5.51 x 3.94 in (140 x 140 x 100 mm)	9.84 x 9.84 x 12.01 in (250 x 250 x 305 mm)	10.82 x 10.82 x 14.96 in (275 x 275 x 380 mm)
Metal alloy choices with developed print parameters	LaserForm CoCr (B) LaserForm 17-4PH (B) LaserForm CoCr (C)	LaserForm CoCr (B) LaserForm 17-4PH (B) LaserForm Maraging Steel (B) LaserForm AlSi12 (B)	LaserForm CoCr (B) LaserForm 17-4PH (B) LaserForm Maraging Steel (B) LaserForm AlSi12 (B)	LaserForm Ti Gr1 (A) ² LaserForm Ti Gr5 (A) ² LaserForm Ti Gr23 (A) ² LaserForm AlSi10Mg (A) ² LaserForm Ni625 (A) ³ LaserForm Ni718 (A) ³ LaserForm 17-4PH (A) ³ LaserForm CoCrF75 (A) ³ LaserForm 316L (A) ³ LaserForm Maraging Steel (A) ³
Layer thickness	10 µm - 100 µm Preset: 30 µm			10 µm - 100 µm Preset: 30 and 60 µm
Repeatability	x=20 µm, y=20 µm, z=20 µm			
Min. feature size	x=100 µm, y=100 µm, z=20 µm			100 µm
Min. wall thickness	150 µm	150 µm	150 µm	150 µm
Typical accuracy	± 0.1-0.2% with ± 50 µm minimum	± 0.1-0.2% with ± 50 µm minimum	± 0.1-0.2% with ± 50 µm minimum	± 0.1-0.2% with ± 50 µm minimum
Material loading	Manual	Semiautomatic	Automatic	Manual
Recycling system	Optional external system	Optional external system	Automatic	Optional external system
Interchangeable build modules	No	No	No	Yes
Real-time monitoring	No	No	No	DMP Monitoring

¹Maximum available part size using standard build plate ²Set up A ³Set up B Complete specifications available at www.3dsystems.com

¹Maximum available part size using standard build plate ²Set up A ³Set up B Complete specifications available at www.3dsystems.com

Fig. 5 Specifications of the 3D Systems ProX Direct Metal.

3. Conclusions

The methods of virtual prototyping in the CAD / CAM / CAE environment are applied in the design of a special device - a SPG-9 breech, to improve the production technology and reduce the cost of manufacturing the part. The designed virtual 3D model gives a better idea of the part design and is easier to correct than conventional 2D drafts.

The machining process used to create the part requires 7 machines in 23 processing stages and over 10 devices as well as over 60 tools to be used which are reduced to one machine for additive manufacturing - 3D Systems ProX Direct Metal for the production of high-density metal parts from a large wide range of materials with proven mechanical properties.

Using 3D prototyping in the design a special SPG-9 breech reduces costs, whether it is used for the creation of a prototype or in serial production.

REFERENCES

1. Григоров, Б. Проектиране и дизайн със Solidworks, София, 2003.
2. Марчевски, П. Цончев, К. Механична обработка на затвор, Кирилфарево, 2017. с.37.
3. Тодоров, Г. Софронов, Й. Технологии за 3D печат ефективност и тенденции, София, с.47.
4. <http://www.engineering-review.bg/bg/aditivno-proizvodstvo-na-metalni-detaili/2/3664/>
5. <http://www.spacecad.bg/printeri-za-metal>

EXPERIMENTAL DEVELOPMENT OF A SMART FUZE DETONATION ALGORITHM

Cad. Dimitrov M.*, Assoc. Prof. Ing. Ganev V. PhD.** M.Sc. Ing. Dimitrova Ya.***.

Faculty of "Artillery, air defense and CIS" – National Military University "Vasil Levski", Veliko Tarnovo, the Bulgarian Republic

* amirodimitrov@abv.bg, ** vvganev@abv.bg, *** dimitrovax2yana@gmail.com

Abstract: Today's battlefield is ever-changing in terms of weaponry demands and engagement criteria. Demands for additional capabilities of current ordnance are constantly growing. An easy yet cheap and effective way to increase existing and also add additional capabilities of current ordnance is by introducing a smart fuze that incorporates electronic components. In this report, a smart fuze software algorithm is created that is customizable, gathers and analyzes data from different sensors and provides different fuze functions. Introducing, as well as, upgrading existing fuze functions making them precise and accurate.

Keywords: DETONATION ALGORITHM, SMART FUZE, FUZE CAPABILITIES.

1. Introduction.

Although maneuver warfare is valid under certain circumstances, the nature of war and the realities of the modern battlefield call for a much more flexible weaponry [1]. Current ordnance faces an increased demand in capabilities and efficiency in order to fulfill its battlefield role efficiently [1].

In this report a smart fuze algorithm is created that gathers and analyzes data from different sensors, offering advanced control for next generation smart weapons. In order for all the electronic components inside the fuze to work as intended a creation of software is needed to initiate control over different sensors to collect data and execute commands given by the operator. The software is capable of introducing new fuze capabilities and increasing existing ones by making the smart fuze a highly customizable and versatile weapon of the modern day battlefield. The algorithm and software researched in this paper are created for a smart fuze project developed and researched in the report: "Experimental development of a smart artillery and mine fuze based on the Arduino microcontroller platform". The smart fuze is a project that aims to enhance and increase current capabilities of artillery projectiles. The smart fuze incorporates different electronic components. In order for all the electronic component inside the fuze to work as intended a creation of software is needed. The software created uses a function algorithm that will be explained in this paper.

The main function of the created algorithm is to control the smart fuze. The algorithm and therefore the software created provide the operator with the freedom to choose how the ammunition detonates. With these options being timed detonation, proximity detonation and heat sensing detonation.

The software created falls under the System Software category [2]. System software directly operates the hardware, to provide basic functionality needed by users and other software, and to provide a platform for running application software [2]. System software includes an operating system, device drivers and utilities which are essential collections of software that manage resources and provides common services for other software that runs "on top" of them [2].

In this paper the working principle of this software is explained via the help of an algorithm diagram.

2. Developing the smart fuze detonation algorithm

2.1. Objective: Developing the smart fuze detonation algorithm.

2.2. Tasks:

- 1 Creation of a block diagram;
- 2 Algorithm explanation.

In (Fig 1) the algorithm block diagram is created.

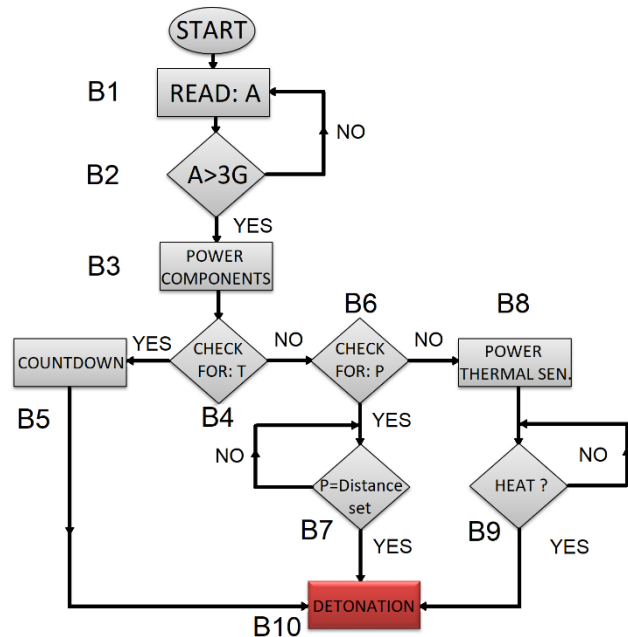


Figure 1: Block diagram of the algorithm.

Before powering on the fuze with the Start button if the operator wants to utilize the fuze proximity or time fuze capabilities he needs to set variables T and D in the software in order for the algorithm to determine the fuze function. The function of the algorithm is explained in detail below.

The algorithm starts when power is supplied to the Arduino board via the power source through a switch. The functions of the software are initiated and the algorithm starts functioning (START).

B1: The algorithm commands the fuze's safety mechanism. The safety mechanism is designed to prohibit any unwanted fuze detonation and to ensure fuze handling safety. When the board is initialized it starts running the uploaded fuze software. The software is designed via the algorithm to first read the value "A" which is the value that the microcontroller reads from the accelerometer chip. The sensor inside the chip measures acceleration in gravitational force – g-force. The acceleration value is designated with "A" in the algorithm. In the presented algorithm diagram the value "A" is presented in the B1 block.

In order for safe handling and transportation to be ensured the algorithm needs reliable way to detect when the ordnance has been fired and initiate the detonation function. This process is shown by the B2 block in the algorithm diagram.

The value read in B1 is checked in B2 as the block condition is $A > 3G$. If the value is higher than 3g the algorithm proceeds to B3. If value A is lower than 3g the algorithm is looped back to B1. This way the algorithm ensures that only after an accelerating force higher than 3g is registered by the accelerometer the ordnance can

be detonated. Only after the needed acceleration value is registered by the accelerometer the algorithm proceeds to B3.

B3 power the fuze's sensor components after which they start processing data. B3 is initiated only after the fuze has been fired and therefore needs to function with a predetermined pattern or detect potential targets and detonate at the best possible moment to ensure optimal destructive capabilities.

At B4 the algorithm checks for the variable "T". The "T" variable is the time set by the operator before the ordnance is fired. It is noted that giving a value to T is optional as the algorithm will still continue to function even when the "T" variable has no value. If the operator wants the fuze to function as a time-fuze before installing it on the ordnance, he needs to set the required time after which he wants the fuze to detonate the ordnance - "T". If the operator does not set any value to the T variable the algorithm starts reading data from the other sensor components and moves on to B6.

B5 initiates the countdown timer of the fuze and after the countdown is complete activates block detonate - B 10. In (fig.1) the timer code command is shown where the operator can input the count down time for the fuze - "T".

```
int 1 // Time variable
Serial.begin(9600); //establishes connection with the arduino
Serial.print(); //count down print
Serial.println() //

delay(1000); //wait 1 second
i= i-1; // loop countdown
if(i< )//if i is less than some number
```

Figure 2: Setting the countdown time.

(Int 1) is the T variable that is set by the operator in seconds. The variable is then looped in a countdown timer that counts one time per second (Figure 3).

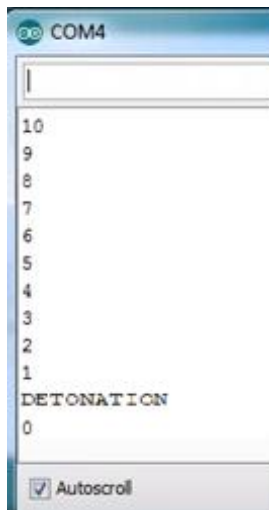


Figure 3: Countdown presented by the graphical compiler.

Detonation is initiated by providing voltage to the Pin connected to the detonator. The detonation code is shown in Figure 4.

```
{
  pinMode(8, OUTPUT);
}

void loop()
  digitalWrite(8,HIGH); // Sends detonation impulse
  delay (100);
  digitalWrite(8,LOW); // Resends detonation impulse
  delay(100);
```

Figure 4: Structure of the detonation code in the compiler.

The detonation Pin is Pin8 on the microcontroller. After the countdown is complete the voltage on Pin8 is set to (HIGH) which means that the software applies voltage to that pin. Detonation is initiated therefore the algorithm ends at B10.

When the T variable is not set the algorithm moves to B6 and checks if the P variable has been set by the operator. When the proximity sensor is powered the sensor constantly feeds the microcontroller with input data. Figure.5:

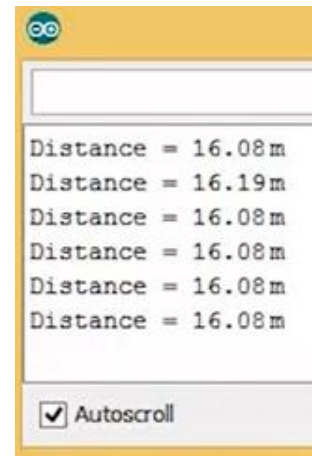


Figure 5: Measured distance displayed by the graphic compiler.

If the operator wants the fuze to function as a proximity-fuze before firing he needs to set a value for the P variable in meters. This value is then read by the microcontroller. The P variable is set in the software in (figure 5).

```
}
setDistance = distance;
if (setDistance <= 5){
  digitalWrite(8,HIGH); // Sends detonation impulse
  delay (100);
  digitalWrite(8,LOW); // Resends detonation impulse
  delay(100);
}
```

Figure 6: Setting the distance at which the fuze will activate.

In this example the detonation distance is set to 5 m. When the distance is less than 5 meters from the sensor to the object the microcontroller applies voltage to (Pin8) therefore initiating detonation B10 ending the algorithm. If the variable P is not set therefore it has no value. The algorithm continues to B8 and powers the thermal sensor and the fuze starts to function as a detection fuze.

After the thermal sensor has been powered in B8 the algorithm starts checking for heat sources in B9 and if a heat signature in the range of the sensor is detected the fuze detonation module is initiated therefore resulting in an ordnance detonation in close proximity to the target. If no heat sources are detected the algorithm is looped.

3.Conclusion:

In this report an algorithm was created and explained. The listed algorithm functions are sufficient for the functioning purposes of the smart fuze prototype researched in the paper: "Experimental development of a smart artillery and mine fuze based on Arduino microcontroller platform". Further experimentation and algorithm complication is possible that can further increase the flexibility and functionality of the algorithm. The addition of new algorithm elements is also possible if the demands for the algorithm change. The created algorithm is a valuable way to replace existing fuze mechanical components with faster electronics and micro components governed by software.

References:

1. <https://www.globalsecurity.org/military/library/report/1991/WAD.htm> .
2. "System Software". The University of Mississippi. Archived from the original on 30 May 2001.
3. <https://howtomechatronics.com/tutorials/arduino/ultrasonic-sensor-hc-sr04/>