

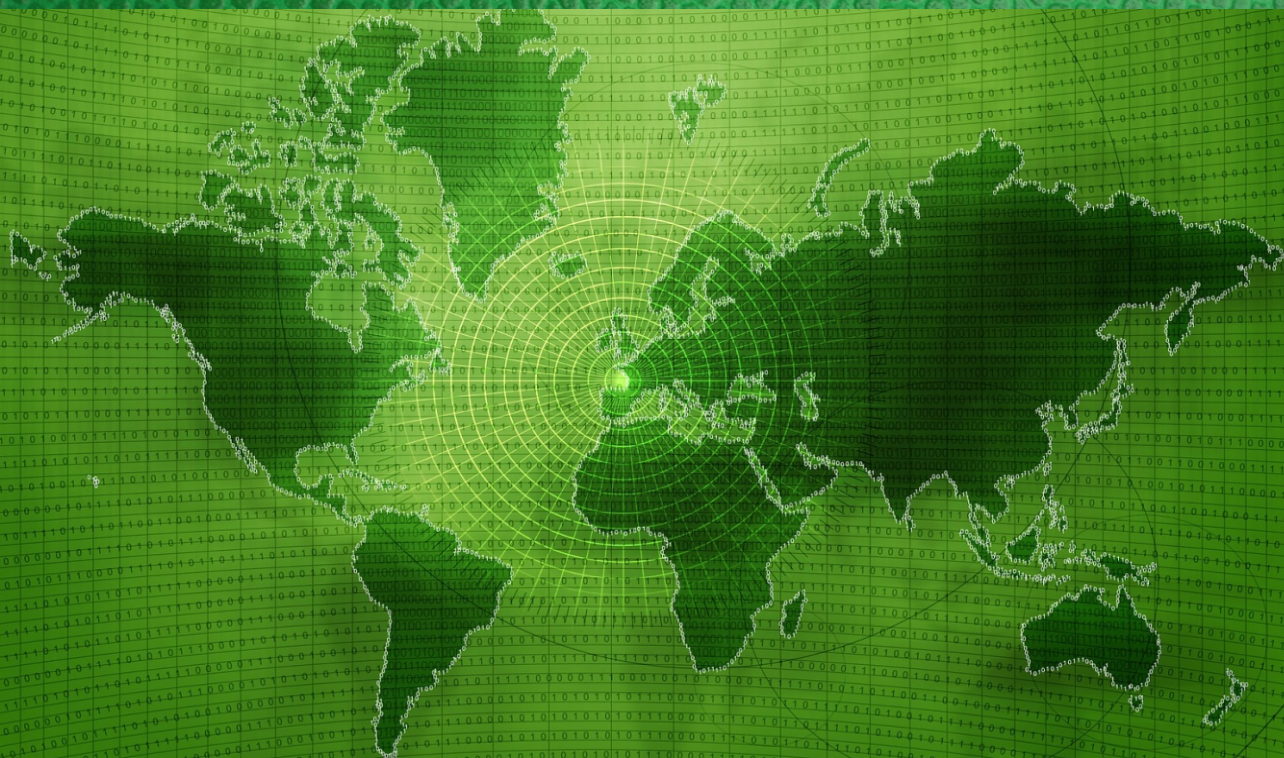
INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

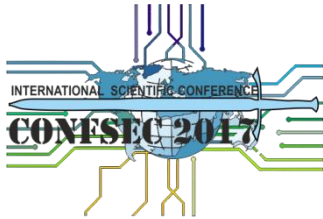
ISSN: (PRINT) 2535-0668

ISSN: (ONLINE) 2535-082X

YEAR II ISSUE 1/2018



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 1 / 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

INTEGRATED CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT

Chief Assistant Dr. Eng. Panevski V.S. 3

CRITICAL INFRASTRUCTURES RESILIENCE EVALUATION - RESILIENCE APPROACH, RESILIENCE MODEL AND RESILIENCE INDICATORS

Associate professor Dimitrov D.L., Ph.D. 7

SECURITY STUDIES IN SERBIAN HIGHER EDUCATION SYSTEM

Želimir Kešetović, Ivan Dimitrijević, Nenad Stekić 11

NATIONAL AND INTERNATIONAL SECURITY

MARITIME PIRACY AND ARMED ROBBERY EVOLUTION IN 2008-2017

Assistant-Professor Dr. Eng. Adelina Tumbarska 18

MODEL OF TACTICAL POLICE ACTION WHEN USING PHYSICAL FORCE

Assoc. Prof. Dr. Jonche Ivanovski, Assist. Prof. Dr. Aljosha Nedev 22

THE ATTITUDES OF THE EUROPEAN UNION ON THE DEVELOPMENT OF THE COMMON SECURITY AND DEFENSE POLICY

Colonel PhD. Eng. Angelov I. 26

ANALYSIS OF THE RELATIONSHIP BETWEEN ENERGY DEPENDENCE AND NATIONAL SECURITY

Chief. Assist. Prof. N. I. Padarev PhD 29

HISTORY AND DEVELOPMENT OF NUCLEAR WEAPONS

Chief Assistant Professor PhD eng. Dolchinkov N. T. 32

MAIN ASPECTS OF THE ECOLOGICAL POLICY OF THE EUROPEAN UNION AND ENERGY RESOURCES IN BULGARIA

Assoc.prof. Galina Todorova, PhD 36

TECHNICAL FACILITIES FOR ENSURING SECURITY

INNOVATIVE INVESTIGATIONS OF THE CRIME SCENE USING 3D SCANNERS

Prof. Wieczorek T., PhD., DSc 39

TYPES OF BULLETPROOF VEST. CLASSIFICATION

Assist. Prof. Eng. Yaneva S. PhD, Assist. Prof. Eng. Tumbarska A. PhD, Prof. Eng. Petkov S. PhD 43

SPATIAL TECHNOLOGIES FOR CRISIS MANAGEMENT

Assos. Prof. Milen Ivanov PhD, Ivailo Neshev PhD 46

MAINTENANCE OF TECHNICAL SYSTEMS IN THE FUNCTION OF SAFETY AT WORK

Veljanovski D. MSc. , Jovanovska V. PhD. 51

INTEGRATED CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT

Chief Assistant Dr. Eng. Panevski V.S.

Bulgarian Academy of Sciences, Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre
 "Acad. A Balevski", Sofia, Bulgaria
 panevski@ims.bas.bg

Abstract: *Integrated management should be seen as synonymous with good management, which means that it is necessary to manage the organization's activities, resources, personnel, impact on its functioning and countless risks that can cause a lot of problems if it is allowed to be happen than if they being avoided.*

The best way to define the parameters of integrated security implies the use of a simple, clear and comprehensive approach and format that allows the senior management of the organization to focus on the key elements that need to be planned, implemented and managed to fulfill the mission of the organization.

Keywords: INTEGRATED SECURITY; CRITICAL INFRASTRUCTURE; MANAGEMENT

1. Introduction

Critical Infrastructures (CI) are organizational units whose functionality if compromised could have led to unpredictable breaches in security, economy, public health and lifestyle of the population not only of one, but also in neighboring countries. While it is unlikely disruptions can be prevented completely, an effective analysis of CI can minimize their impact by improving assessments of vulnerability and protection planning strategies for response and recovery. The analysis aims to give an idea of the CI behavior in terms of occurrence and impact of possible risk events, which will increase the efficiency of protection plans and operations for response and recovery. The end result of the analysis is the presentation of a decision to ensure the Business Continuity of the CI, namely the establishment of an Integrated Security.

It is necessary to understand that "...we should not perceive critical infrastructure protection as an isolated and independently-functioning structure, because security aspects penetrate all, even seemingly irrelevant spheres of the operation of the organization". [1]

In the most general case, in modern theory and practice, under the integrated security of CIs is meant the deployment of intelligent protection, including both the identification of specific threats and vulnerabilities and the inclusion of the best adapted solutions, namely:

- External perimeter solutions, including radars, motion detectors, microwave, infrared, acoustic, vibration and CCTV;
- Inside perimeter technologies and solutions ranging from access control to video analysis;
- Integration Platforms (command centers of business management solutions for security of outer and inner perimeters).

But is this integrated security?

Presented in this way, Integrated CI Security provides a partial picture of the nature of the challenge. It should be pointed out that the creation of integrated security covers all the elements (systems and subsystems) of the CI management as a business organization: external and internal security; staff; finance; environment; quality; information security, business continuity management; corporate social responsibility and etc. Precisely in this direction, the following text will present the views and practical results of the activity to ensure integrated CI security.

2. Interactions between Business Continuity Management System and Business Organization Management System

In order to identify these interrelations, it is necessary to point out the *similarities* and *differences* with regard to the requirements for the establishment of the Business Continuity Management (BCM) System and the management systems for: quality assurance, environmental protection, health and safety at work, finance, human resources, information technologies and data protection, corporate social responsibility, risk management. [2]

Similarities

The construction of the above-mentioned systems requires the creation of documents specific to the individual area of activity of the business organization or the carrying out of actions such as: policy; a strategy for the implementation of key policy directions for development; risk analysis; a detailed plan for the implementation of the strategic objectives and objectives; updating, maintaining and testing the plan; training of the personnel for the implementation of the individual modules and tasks of the plan; conducting preventive and corrective actions, regular monitoring of changes in the business environment and audit of activities, related to achieving the objectives of the policy and strategy.

The methodology used is either the same (quality, environment, health and safety at work), or similar and very similar (finance, human resources), which creates conditions for understanding the general and specific problems of the organization by most of its employees and employees.

Differences

The significant difference between them is the conduct of *Business Impact Analysis* (BIA) in the course of building a Business Continuity Management System.

The purpose of BIA for each action, process, product, or service is to:

- document the impacts that may arise as a result of loss or interruption of the organization / system activity;
- determine the time required for recovery of the function;
- determine the conditions (internal and external) needed to operate the system / organization effectively.

This is the *basis of the difference* between BIA and Risk Analysis, namely that first explores the events that led to major disruptions of operations, while the second examines all potential events that may affect the business of the organization. [2] Considering the fact that BCM is in close relation with all other subsystems of the

Organization Management System, and that it only lays down specific requirements for all of them we can, with a sufficient degree of conviction, declare that it is the connecting link in the management of the organization.

3. Integrated model for security and protection of critical infrastructure protection

In the period 2011 ÷ 2013, under the leadership of the Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Center "Academician Angel Balevski", Bulgarian Academy of Sciences, an Integrated Model for Security and Protection of CI was developed and successfully tested. This result was achieved during the implementation of the European project "Development of tools needed to coordinate inter-sectoral power and transport activities at a situation of multilateral terrorist threat. Increase of the capacity of key CIP objects in Bulgaria", reg. № HOME / 2010 / CIPS / AG / 019. The model outlined and described the characteristics of the integrated security and protection management of the CI and, on the other hand, gave the specialists in this field a starting point for discussion and improvement of the system characteristics.

Essence of the model

Good practice so far has shown that the starting point for the development of the security and protection models (CPM) of CI is the adopted uniform terminology. For example, the following definition was used to describe the content of the term "Security and Defense System": "The Security and Protection System is a set of elements operating under a unified security concept, purposefully managed in a common information environment to provide the processes, aimed at timely detection of threats and a preventive response to prevent side effects". [3] As far as the term "Critical Infrastructure" is concerned, the natural definition of Council Directive 2008/114 / EC, namely: "means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".

On the other hand, the creation of CPM was taken to apply the methodology of the schematic description of the site and the activities of security and defense, who perform them and what are the interrelationships and consequences of these activities.

The Functions of the Model:

- Detection of terrorist attacks, recognition and reaction;
- Standby keeping for reaction;
- Provide continuous and normal operation of CI.

The purpose of CPM is to identify threats, to provide an answer and a response to prevent unauthorized access to the protected area of CI [3] through organizational and technical activities, offering the following characteristics:

- Organizational part;
- Technical part;
- Procedures for the implementation of policies, strategies and plans.

Organizational part

The organizational part can be composed of multiple elements, in this case, their structures consist of risk analysis and risk assessment and develop: security and protection policy; security and protection

strategy; security and protection plan; corrective and preventive activities and training programs.

Of course, risks analysis and risks assessment can be done using different methodologies. The essential point is to link the results of this process with follow-up by the authorities involved, aimed at enhancing the security and protection of the CI. Thus, without claiming completeness, the process may include the following elements [4]:

- Evaluating risk factors, such as the following groups of threats: natural; against machinery, equipment and buildings; against staff; against technology; against operations and social.
- Vulnerability assessment of the elements of CI;
- Sustainability Assessment of personnel and population.

In turn, vulnerability assessment of the structural elements of CI can be done in terms of the effect of external influences, the result of which is a map of vulnerabilities and their interconnections. It involves evaluating each item with the following parameters:

- Constructive reliability - measures the extent and ability of site elements to protect technology, machines, and those working with them from the actions of terrorists;
- Accessibility for external impact - measured under conditions of relative ease, serenity, or difficulty in moving terrorists to or within the protected object;
- Recognition of an external observer - characterizes the difficulty in determining the functions and significance of the object or machines and the technological lines located therein.

On the basis of this assessment and in order to identify the responsiveness to a particular threat, the level of the most effective implementation of the security and protection activities of the CI should be determined.

The assessment of the sustainability of personnel and the population with the impact of risk factors can be done by using the numerous human resource management methodologies.

Based on the analysis and risk assessment, it is necessary to develop the conceptual framework that will direct our efforts in the right direction, i.e. to formulate a security and protection policy for the CI.

Security policy is a set of documented solutions adopted by the organization's management and aimed at ensuring security and protection of the object of CI. [5]

The policy defines the principles and responsibilities for interrupting technical processes as a result of a terrorist threat in a way that ensures the maintenance or timely recovery of critical functions (processes), while minimizing the impact on critical functions and equipment. It should be directed to:

- ensuring the continuity of the critical functions (processes) of the CI;
- allocation, between management and response forces, of the roles and responsibilities of management in the event of a terrorist threat;
- ensuring a consistent approach to building security and protection in line with international and national standards;
- integration of the system to ensure the security and protection within and processes for risk management of the CI.

Meanwhile, Security and Protection Strategy defines the basic framework of rules and instructions for operation of the Security and Defense System. It regulates the determination of the means and procedures as well as the responsibilities of all participants in the process. The result of the implementation of the Strategy is to

achieve support from senior management to overall Security and Protection System.

The development of the Security and Protection Plan describes the processes and resources needed to achieve the objective - ensuring the continuity of the CI work. It should contain, but is not limited to, the following information [6]:

- Strategy to overcome the incident (in this case the realization of a terrorist threat);
- Minimum Requirements to Recover Continuous Action;
- List of team members, rights and responsibilities, and contact details;
- List of materials delivered outside the site;
- Activities organized by phases.

Technical part

In the technical part, three secondary models can be identified - a model of the site for the location of the site, a model of the risks and threats and a model of the equipment of the site. [5] They define parameters depending on the possible means of action by terrorists, characteristics of the technical means of monitoring and warning of the reaction forces - transport, communication-information systems, armament, and assessment of the territory and determination of the times for reaching critical.

The **Model of the site** for the location of the site is done in order to present the security and protection of the CI with a digital analogue for the mathematical processing of the data. To solve this problem, the site model for site deployment is described by a peripheral area, lanes and segments.

Through the **Risk and Threat Model**, the following tasks can be solved:

- identification the most likely areas for committing terrorist attacks;
- determining the forces and means that will impact on the CI.

The **Model of the Equipment** is built to determine the types of tools and systems depending on the potential of terrorists to influence the CI (including security, containment and alarm security (sensors)).

Procedures for the implementation of policies, strategies and plans

In order to implement the established policies, strategies and plans to ensure the security and protection of CIs, management must create the necessary conditions for a detailed description of the activities to be performed, bound by time, place and responsibilities. The allegation that this is done within the sections / phases of the security and defense plan is incorrect and one of the most common cases of failure in the implementation of the plans is the lack of clear and streamlined procedures for their implementation.

4. Integrated security management system

„The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures.“ [7]

Following this approach, the CI security levels that may be at the core of building an Integrated Security Management System are as follows [2]:

- 1st level – Risk Assessment (1) and Internal Security (2);
- 2nd level - Risk Assessment (1); Internal Security (2) and External Security (3);

- 3rd level - Risk Assessment (1); Internal Security (2); External Security (3), Quality Assurance (4) and Safety (5);
- 4th level - Risk Assessment (1); Internal Security (2); External Security (3), Quality Assurance (4) and Safety (5); Information Security (6); Human Resources (7) and Financial Security (8);
- 5th level - Risk Assessment (1); Internal Security (2); External Security (3), Quality Assurance (4) and Safety (5); Information Security (6); Human Resources (7); Financial Security (8); Environmental Security (9) and Corporate Social Responsibility (10);
- 6th level – All listed above and Business Continuity Management (11).

Of course, this is only a conceptual proposal. The structure and content of these levels is discussed and scientific and professional communities will determine their ultimate configuration. It is essential that, after defining the final levels of security for organizations, a practical and applied mechanism for their creation and assessment of their readiness to use has to be established, i.e. to assess the degree of security of the organization.

This mechanism may be covered by an international standard describing requirement for individual security levels. As for the assessment of their readiness for use and overall assessment of the security of the organization it is also necessary to create a unified methodology applied by individual standardization or other document to unify efforts in this direction. Only in this way will we have an objective assessment and a tool for comparing the security systems in place in different organizations.

Here it may be noted that the creation of CI security levels is not an end in itself. The ultimate result of their construction and operation should be the formation of an integrated security management system for organizations (Fig. 1).

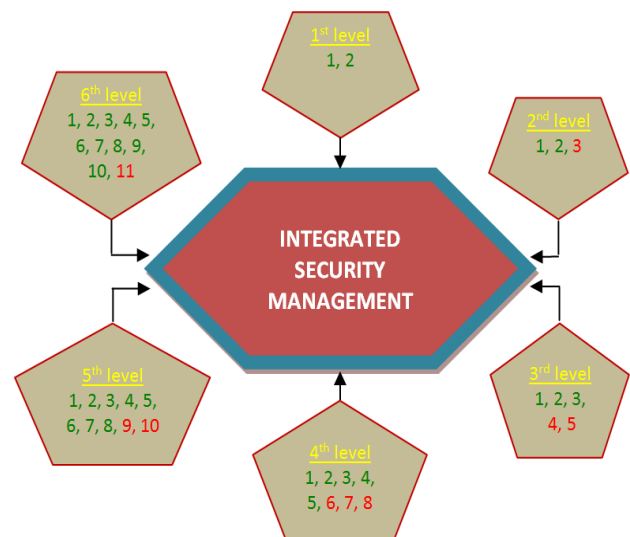


Figure 1: Integrated security management system – security levels.

It is true that there is a document that includes regulations for creation of such system, namely the ISO / DISSES 34001 Security Management System. However, the methodology described in this standard covers the processes of risk assessment and risk management. These two tools are the first and indispensable condition for creating and safeguarding the organization's security, but they are by no means the only.

The proposed approach to building an Integrated Security Management System takes into account the underlying nature of risk assessment and risk management, while covering all security-related elements / subsystems of the organization's management system, and focuses on detailing the individual requirements as well

in relation to these elements, and on the levels of security built on them.

Conclusion

The proposed model for integrated security and protection of CI covers the following basic directions: presentation of the structural framework of the integrated model, covering the organizational part, the technical part and the realization procedures; understanding business continuity management as an integrating link both between the individual subsystems of the business organization management system and between the elements of security and protection levels; definition of the security and protection levels of CIs, determining the creation of integrated systems in the area under consideration and last but not least, opportunity offering for choosing an alternative method for their construction, framing the methodology for the creation of integrated security and protection of CI.

Describing the integrity of security and protection, through the proposed levels of security, forms the framework of the integrated system. The security level elements correspond to the subsystems of business management system of the organization. This is precisely the uniqueness of the proposed approach - the mutual penetration of security within the overall CI management to ensure the fulfillment of its mission.

Literature:

[1] Dimitar Dimitrov, Valentina Nikolova, Martin Asenov, Petia Vasileva "TECHNICAL AND ORGANIZATIONAL ASPECTS OF THE APPROACHES, USED FOR ASSURING EFFECTIVE SECURITY AND PROTECTION OF CRITICAL INFRASTRUCTURE-GOOD PRACTICES AND RECOMMENDATIONS", Proceedings of the Sixth National Conference with international participation "Materials science, hydro- and aerodynamics and National Security '2017, ISSN 1313-8308, 210 ÷ 216;

[2] Kiril Stoichev, DMITAR Dimitrov, Valeri Panevski "Integrated Security and Critical Infrastructure Protection" Monograph, Chapter Two, ISSN 978-619-90310-6-3, 2016.;

[3] Yachev R. and Project team by NDA, Stoichev K. and Project team by IMSETHC-BAS, "Development of a security and protection model of the airport external perimeter", Collection of materials with the results of the project: "Development of tools needed to coordinate inter-sectoral power and transport CIP activities at a situation of multilateral terrorist threat. Increasing of the protection capacity of key CIP objects in BULGARIA – BULCIP", ISBN 978-954-92552-6-3, 2013;

[4] Vitanov L. and Project team by NDA, Stoichev K. and Project team by IMSETHC-BAS, "Modeling of advanced system for security and water channels protection of the NPP", Collection of materials with the results of the project: "Development of tools needed to coordinate inter-sectoral power and transport CIP activities at a situation of multilateral terrorist threat. Increasing of the protection capacity of key CIP objects in BULGARIA – BULCIP", ISBN 978-954-92552-6-3, 2013;

[5] Stoichev K., Business Continuity Model of the NPP' System for removing the heat, International Workshop: "Business Continuity Management of the Nuclear Power Plant System. Modeling and Procedures Development of Advanced System for Security and Water Channel Protection of the NPP", Kozloduy NPP, 05 of June, 2012;

[6] Stoichev K., (2014), The Role of Business Continuity Management in the Business Management System, Science Journal of Business and Management, 2(3), 97-102, DOI: 10.11648/j.sjbm.20140203.12, ISSN: 2331-0626 (Print); ISSN: 2331-0634 (Online);

[7] ISO/IEC 27002:2013 "Information technology - Security techniques - Code of practice for information security controls", "0 Introduction", "0.1 Background and context".

CRITICAL INFRASTRUCTURES RESILIENCE EVALUATION - RESILIENCE APPROACH, RESILIENCE MODEL AND RESILIENCE INDICATORS

ОЦЕНКА НА УСТОЙЧИВОСТТА НА КРИТИЧНИТЕ ИНФРАСТРУКТУРИ – ПОДХОД, МОДЕЛ И ПОКАЗАТЕЛИ ЗА ОЦЕНКА.

Associate professor Dimitrov D.L., Ph.D.

Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski" - Bulgarian Academy of Sciences, Sofia, Bulgaria

E-mail: ddimitrov@ims.bas.bg

Abstract: Aim of this report is to provide practical hints on how to evaluate the concept of Resilience in the domain of Critical Infrastructures (CI). The common understanding is that today best practices address cyber / physical protection of CI at the best they can, with traditional static and iterative solutions, trying to stop all possible known threats at the border of the single CI's assets or CI's full perimeter, ready to start with procedures of disaster recovery and business continuity in case of failure stopping external threats.

KEYWORDS: RESILIENCE; RESILIENCE APPROACH; RESILIENCE MODEL; RESILIENCE INDICATORS; SECURITY; SECURITY MANAGEMENT SYSTEM (SMS); INTEGRATED MANAGEMENT SYSTEMS FOR BUSINESS SECURITY.

1. Introduction

Nowadays, unfortunately, Infrastructure Operators have to deal with a landscape characterized by constantly evolving threats and vulnerabilities, in response to which we need dynamic and continuously adapted solutions. In addition to all the measures already in place for protection, resilience is intended to put in operation at physical and logical levels all possible status of the art measures, along with redundancy and fault tolerant mechanisms able to adapt the system to evolving threat landscape, to reduce the reaction time and increase the reconfiguration capabilities.

While at personal, organizational and cooperation levels is intended to put in operation the best practices for continuous training (aimed at reduce internal threats, environmental inertia and social engineering issues), communication within the same organization, among different organizations and with the external world, able to foster the solution of the crisis after a successful attack or natural disaster.

2. The resilience approach

Past and recent experiences have shown how likely is that protection policies, sooner or later, may fail.

For this reason, and being aware of the fact that the efforts put in place for protection of CIs can be easily bypassed, all of the stakeholders involved in the protection of such delicate and vital infrastructure have reached a level of awareness that strongly suggests putting more emphasis on critical infrastructure resilience [1].

What does resilience mean?

Though infrastructure protection and infrastructure resilience represent complementary elements of a comprehensive risk management strategy, the two concepts are distinct. Infrastructure protection is the ability to prevent or reduce the effect of an adverse event. Infrastructure resilience is the ability to reduce the magnitude, impact, or duration of a disruption. The spread in the continuous discovery of new threats that target CIs, stress the importance of a whole rethinking around the concept of protection. That's where resilience emerges from and becomes an important part of the playing field. A resilient approach is a holistic set of procedures and measures that encompasses the entire structure of an institution/business/infrastructure, from the physical parts to the management, to ensure the ability to prevent, absorb, adapt, and recover to an attack, either physical or cyber.

Very often there is the tendency to confuse the concepts of: resilience, security, business continuity, risk assessment/management, crisis and emergency management.



Figure 1 Resilience: A Multifaceted Problem

Difference between Business Continuity and Resilience

Some authors argue: "Business continuity has been focused upon a defensive resilience posture, consisting of three basic building blocks - recovery, hardening and redundancy – that are widely recognized as vital ingredients for successful business continuity plans. A defensive posture is useful in protecting the organization and its revenue streams but it does not help the bottom line. It is an insurance or bomb-shelter mentality; a static initiative that makes you feel more secure or protected, but rarely gets updated" [2].

The concept of the "static initiative that make you feel more protected" is exactly what makes the difference with Resilience that is a step ahead to Business Continuity. According to other authors, Resilience provide "a mixture of continuity, availability, security, recovery and scalability" enabling a dynamic, proactive and holistic dimension to the protection approach. Resilience enable organizations to rapidly "self" adapt to abnormal events, faults or disruption ensuring a seamless service [3].

Resilience Evaluation is the overall activities of modelling, and analysis of critical infrastructure system aimed to evaluate the ability to prevent, absorb, adapt, and recover from a disruptive event, either natural or man-made.

Resilience Engineering is the overall activities of design, construction, operation, and maintenance of critical infrastructure system aimed to ensure the ability to prevent, absorb, adapt, and recover from a disruptive event, either natural or man-made.

As said, this aspect is not included in this report and should be, whether applicable, the focus of a future investigation.

A Critical Infrastructure is not only made of technologies but especially of people, processes and organizations. Any Resilience Evaluation and Engineering activity must take in consideration all these components, including cultural background, in view to be complete and successful.

To be univocally applicable, infrastructure resilience evaluation and engineering require a precise definition of resilience that is applicable to all infrastructure systems. The model consists of a hierarchy of four system resilience dimensions that concur to realize the four system resilience capacities taken from the definition. Resilience features occupy the engineering level of the hierarchy and represent the current infrastructure design implementations that contribute to one or more of the system capacities, while resilience indicators are quantified properties of the dimensions, capacities and features characterizing the system subject to assessment [2].

2. Overall basic assumptions of the model

The following statements sum up the proposed model features and point out some relations among model entities:

- Resilience is a quality of the system. Being a system composed of several subsystems, the overall system's resilience will be achieved through assuring resilience to single subsystem, considering higher risk priorities, as well as dependencies from other systems. The primary difficulty often involves how to represent infrastructure dependencies.
- The model addresses resilience evaluation but is also applicable to resilience engineering.
- Resilience has four dimensions: technical (logical & physical), personal, organizational, cooperative.
- Resilience relies on four capacities: preventive, absorptive, adaptive, restorative.

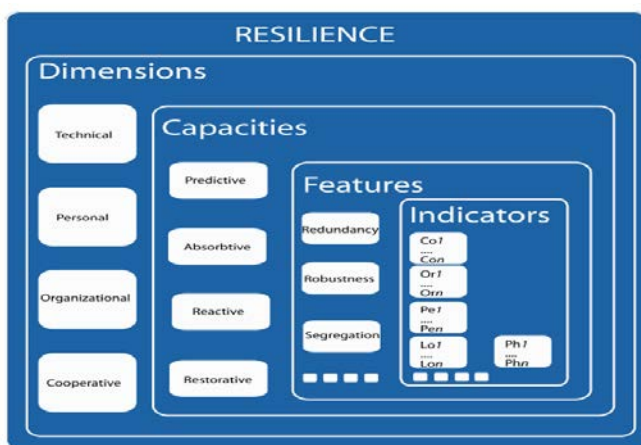


Figure 2 Hierarchical Representations of the Infrastructure Resilience Model and Indicators

- Each capacity is related to specific features (e. g. robustness, redundancy, segregation).
- Resilience indicators will be different for different application sectors (energy, transport, communications, and urban systems)
- Resilience indicators are physical and logical techniques, procedures, training activities, organizational solutions, etc. able to foster system capacities.
- Evaluating the system resilience may be downsized to evaluate the existence of resilience indicators, in the different features, capacities and dimensions of the system under evaluation.
- A software application based on the Resilience Model may be spun off the methodology [3].

Four system resilience dimensions:

The resilience dimensions derive from the assumption that a Critical Infrastructure is not only made of technologies but especially of people and organizations, and is dependent (or interdependent) from others infrastructures.

These dimensions may be stacked in an abstraction degree order from the highest abstraction level (Cooperative) to lowest abstraction degree level (Logical and Physical). Any Resilience Evaluation (and even Engineering) activity must take in consideration all these dimensions.

• *Logical & Physical dimension:* Individuate the most advisable technologies today available for the cyber and physical protection. Considering the best technologies to be used for sector specific applications. How to address the ever evolving threat and vulnerability landscape, with dynamic and continuously adapted technological solutions.

• *Personal dimension:* How to define the Profile of the people in charge for CI's resilience. How possibly certify the Resilience Skills of experts. Which should be the Training Program to prepare CI's resilient experts? In which way motivate the CI personnel not security specific to take part to the overall challenge of security.

• *Organizational dimension:* accordingly, with a proposed general logical model, how to define at organizational level a Resilience Management System and how to implement it. How to individuate the people to be involved. How to define the responsibilities and at which level.

• *Cooperative dimension:* How to promote the cooperation among different CI operators, both private and public. Who should have the responsibility of the initiative? Which is the state of the art and the best practices.

In building and evaluating resilience the contribution made by each of these four dimensions needs to be considered.

Four type of system resilience capacities

The resilience capacities are the intrinsic properties of the system infrastructure implemented into each one of the resilience dimensions, to make the system resilient.

- Preventive capacity: ability of a system to anticipate disruptive events.
- Absorptive capacity: degree to which a system can automatically absorb the impact of system perturbations and minimize consequences.
- Adaptive capacity: degree to which the system is capable of self-organization for recovery of system performance levels.
- Restorative capacity: the ability of a system to be quickly and easily repaired.

These capacities are represented in Figure 3. This figure has to be interpreted as that in case of disruptive event the four capacities will be activated from Preventive to Restorative, based on the real need

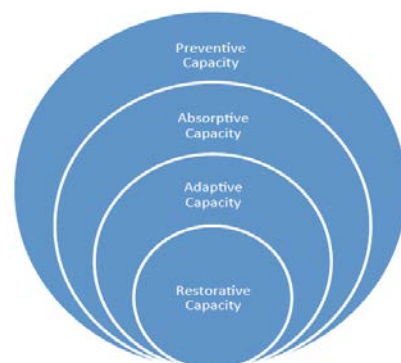


Figure 3 System Resilience Capacities

3. Resilience indicators

Resilience Indicators are quantified properties of the dimensions, capacities and features characterizing the system subject to assessment. Evaluating the resilience indicators means to evaluate the adoption of resilience solutions at the bottom level of the implementation used to implement features, enhancing capacities, acting in the four dimensions, with the goal to build a more resilient system. Resilience indicators are the basic tools for the evaluation process [4].

Resilience Indicator Name	Related code (Dimension related)
A - Description	Description of the specific Resilience Indicator of the sub-system/system subject to evaluation
B – Pertinent dimension(s)	To which dimension, sub-system / system, capacity it applies
C - CI Sector relevance	Relevance for the specific application sector (energy, transport, telecommunication, health care, etc.);
D - Evaluation method(s)	Method used to quantify this specific indicator while applying it to the sub-system / system subject to evaluation
E - Sources / References	References, if any, to authoritative sources from which card content is derived, totally or in part.

Figure 3 – Template for Resilience Indicator Cards

Validation Process for the Resilience Indicators

Resilience Indicators need to be validated for each specific sector or system of application by working together with Sector or System Experts. To this purpose, customization is essential to make the proposed methodology for engineering and evaluating resilience usable for CI operators and owners [5].

Today large organizations, such as most of the CI operators and owners, have a so called “silos” structures affected by the functions/roles assigned by the organization charts. This makes the process of resilience indicators validation still more difficult because of the necessity to interact with different key figures into the organization.

Here below is a suggestion about a potential approach towards the CI operators and owners: a matrix defining what to ask to the possible different key figures inside the organization. The rationale is to ask to quantify the magnitude of each resilience indicators to the key role in charge, respectively, of the logical, physical, personal, organizational and cooperative aspects.

4. Best practices to deploy a resilience management system

Tracking the knowledge path to resilience: how to take effectively the “as is” picture of the Organization Designing the organizational change posture for resilience.

It's important to gather good quality picture of all relevant assets of the organization and to estimate the overall exposure to business risk.

Let's say that organizations are required to perform a complex and knowledge intensive task that largely influences the “to be” project in terms of quality of results and effectiveness of the overall change effort. Specific knowledge management approach and techniques within organizations are available to face such a complex task.

From an operational point of view specific roles and responsibilities are a preliminary step along this path to use general or sector specific techniques. Strongly recommended here all the instruments

and techniques referred to the “learning organization” approach and related collaborative tools and techniques.

How to create and communicate a Resilience Intent Statement?

The presence of an “intent statement” is helpful to clearly make people aware of the targeted objective and direct their emotional, physical and intellectual resources to the objective.

Intent should be composed by at least by three statement: the indication of the purpose, the description the overall approach intended to be adopted (the “doing how”) and the desired end state.

An intent statement in “enacted” from the highest level of the organization and his function is to make clear and to commit all people of the organizations on the targeted objectives and the related expected behavior to be adopted.

The statement strongly upheld by top and diffused to all the organization must become the “motto” of every internal and external initiative to strengthen organizational resilience.

This approach has the twofold objective to make aware all the organization about the importance of the resilience and to definitely anchor the decision-making centers to the objective.

Creating a sound Resilience Policy

We suggest drafting a General Resilience Policy in which the organization recalls and details from the intent statement the main objectives, the methodology adopted by the organization to set up the resilience management system, the organization levels committed, the resources to be allocated, the expected results, and the envisaged control process.

Issue-specific policies will follow to grant details on the above mentioned topics or, if requested by the characteristics of the organization, or by sector-specific requirements, to provide a fine grain description of specific processes or sub-processes.

Building up an organization for Resilience and the “backpack of competences”

A definition of general and specific responsibilities for resilience needs to be allocated within the organization. This is not an “a priori” task but it's the results of the process flow design as provided by the resilience management system.

The responsibilities identified in the activity and process description need to be allocated to specific individuals and organizational units that take the commitment to carry out the envisaged assignments.

The ability to perform the related specific task needs a twofold set of competences: the knowledge of the process in which the subject is involved and the task-specific competence.

According to this requirement organization must provide an accurate “competence model” identifying a detailed competence/role matrix in order to set out the right competence “backpack” for individuals and providing specific programs for the related ongoing training.

5. Conclusion

Specific experience is needed to put in place a Resilience Management System. The design and the implementation approach although is strongly advisable to follow in any case the main steps of the overall model here introduced, largely depends on the characteristics of the organization such as the sector of operations, the size, the criticality of the business process and objectives; moreover internal factors (i.e. culture, characteristics of work processes, etc.) such as external factors (environmental, socio-political context, etc.) [6].

It follows that who has the burden to design and implement the system should pay particular attention to fit the system to the

specific organization. Here we provide some tips and advice in order to achieve the goal of placing the system under control, whatever the level of specify and/or complexity to deal with.

The operation of the system is the moment of truth: the intent statement must be accomplished, the general and specific policies need to be properly enforced and the targeted results must be achieved.

Since treating resilience everything goes well until organizations experiment a real the problem, it's really important never let your guard down and keep the focus on resilience always alive. Probably this is one of the toughest issue to manage to ensure resilience. Some basic practices will be here provided to set and maintain adequate levels of performance on this issue.

Measuring results and setting up a continuous improvement process for organization resilience - performance measurement is possible only if organization is capable to know and "read" what really happens inside itself. Several approaches are largely available on performance measurement and here we try to outline a specific one for resilience management.

Whatever the model adopted since the improvement is a step-by-step process, surveys on progress of the "maturity level" on resilience is recommended. Moreover, since resilience relates to mission critical objectives a "knowledge based" approach to performance analysis is also strongly recommended.

Literature:

[1] A. Boin and A. McConnell, "Preparing for critical infrastructure break- downs: the limits of crisis management and the need for resilience," *Journal of Contingencies and Crisis Management*, vol. 15, no. 1, pp. 50–59, 2007;

[2] P. H. Longstaff, "Security, resilience, and communication in unpredictable environments such as terrorism, natural disasters, and complex technology," *Center for Information Policy Research*, Harvard University, 2005;

[3] U. Rosenthal and B. Pijenburg, *Crisis management and decision making: simulation oriented scenarios*. Springer, 1991, no. 1;

[4] Tim Prior, "Measuring Critical Infrastructure Resilience: Possible Indicators", *Risk and Resilience Research Group*, Center for Security Studies (CSS), ETH, Zurich, 2015

[5] Birkmann J. "Risk and vulnerability indicators at different scales. Applicability, usefulness and policy implications" *Environmental Hazards*, 2007; 7(1): 20 – 31.

[6] George H. Baker III, Ph.D., "A Vulnerability Assessment Methodology for Critical Infrastructure Facilities", 05, 2007;

SECURITY STUDIES IN SERBIAN HIGHER EDUCATION SYSTEM

Želimir Kešetović, Ivan Dimitrijević, Nenad Stekić,
University of Belgrade
Faculty of Security Studies

Abstract: Academic programs of security studies in former Yugoslavia were organized within the Faculty of People's Defence in Belgrade and Faculty of Security in Skopje, as well as at colleges of professional police studies in Belgrade, Zagreb, and Ljubljana, all of them state-owned and aimed at schooling professionals in the national security sector. Following the Yugoslav dissolution, Western Balkan countries have continued development of their own higher education system synchronized with their European integration orientations. The cornerstones of European Union accession process in the area of higher education are mechanisms based on the Bologna Declaration, later institutionalized through the European Higher Education Area, which all the Western Balkan countries adopted and modified their higher education systems accordingly. The appearance of private higher education institutions was one of the first steps in the overall national reforms of these systems, where the Republic of Serbia is amongst regional countries with the biggest number of private universities, faculties, and colleges, especially in the social sciences and humanities. At the same time, the national security sectors went through the process of decentralization and privatization. These external and internal factors, combined with the global rise of importance of security-related phenomena, especially after the 9/11 events, brought the security studies in these countries in focus of interest of the existing and rising higher education institutions. Conflict heritage, the existing local security threats like extremism and terrorism, and a vast number of experienced national security officers with university titles, led to the appearance of various academic programs on terrorism, national security, national defence, and private security studies both on the existing state-owned and private universities and faculties. At the moment, the Republic of Serbia offers several dozens of higher education programs in security, on all the existing study cycles, within three different types of studies, and both for academic and professional levels. The paper will provide an overview of the existing higher education programs in the field of security and analyze the main discourses, directions and possible perspectives.

KEY WORDS: SECURITY STUDIES, HIGHER EDUCATION, REPUBLIC OF SERBIA, UNIVERSITY, EUROPEAN UNION, EHEA

Introduction

Serbian higher education system is relatively new in comparison to majority of Western universities, and it can be traced back to the beginning of the 19th century, when the first College was founded in 1808 by Dositej Obradović, Serbia's first Minister of Education. The College was a basis for establishment of the Lyceum, founded in 1838 in the city of Kragujevac, and later moved to Belgrade in 1841, where the Department of Law was established along with the existing Department of Philosophy. After the new Law on Founding Higher Education was adopted, in 1863 Lyceum became a Higher School, which had been recognized throughout Europe at the time, mainly because teaching staff consisted of professors schooled at the top European universities. In 1905, when the new Law on Universities was adopted, the University of Belgrade has been established as the first university in Serbia (University of Belgrade, 2018).

After the Second World War, the University of Belgrade influenced the establishment of other major universities in Serbia, Montenegro, Bosnia and Herzegovina, and Macedonia, then-republics in former Yugoslavia. The number of enrolled students increased rapidly after the war, with approximately 50,000 students in the early 1960s: "The influx of students was encouraged by the liberalisation of enrolment procedure and the possibility of part-time studies. Later on, the enrolment quotas became limited for each Faculty" (University of Belgrade, 2018). The influence of the University of Belgrade was not only limited to higher education, but also stretched to wider social and political movements. From demonstrations in 1968 to the ousting of the regime of Slobodan Milošević in 2000, the University of Belgrade, along with other universities in country and region, have had an important role for development and progress.

The turbulent history of Serbia marked with numerous wars, uprisings, turmoil, several economic decays, and continuity in authoritarianism, has put security in the centre of everyday life, especially in the last decades of the 20th century. The main pillars of the socialist-era political system, when Serbia was part of Yugoslavia, were three leading institutions of security sector, the armed forces (Yugoslav People's Army), the police, and several secret services with central, the State Security Service, as the most important one. The role of these security sector elements was to maintain the country safe from military attack, to provide comprehensive public security for its citizens, and to prevent any possible disruptions of the ruling ideology headed with the communist party. The result of such authoritarian system was a

centralization and non-transparency of education for security sector, especially in the higher education, which was understood as a "reserved domain" and exclusivity not appropriate for civilian education system.

A broader higher education programs aimed at academic security education started in early 1970s in former Yugoslavia, as a part of comprehensive education of all citizens with the goal of raising awareness and preparedness for wartime and peacetime threats during the Cold War (so-called *Concept of General People's Defence and Social Self-Protection*). Besides many study programs of General People's Defence that were founded within the existing university faculties across Yugoslavia (mostly within faculties of political science), the only independent faculty was established at the University of Belgrade. The Faculty of People's Defence of the University of Belgrade educated the future secondary school educators for the subject called *Defence and Protection* in Yugoslavia, which was an obligatory school subject at the time.

Along with the dissolution of the Yugoslavia, the Concept was abandoned as well, and in new conflict and authoritarian circumstances of the 1990s, the security studies remained a "reserved domain" for official state institutions only. Only after the democratic changes in 2000, security studies became a "public good" and provided on civilian universities and faculties, both state- and privately-owned. However, the sudden expansion of various curricula in security-related area showed that the quality did not manage to meet the quality of those studies. In this paper, we will firstly present a historical overview of the development of security-related higher education programs in Serbia, with special emphasis on civilian security studies programs. Then, we will give an explanation on what led to the expansion of security studies programs in Serbia after 2000, both on state-owned and private universities and faculties, while special focus will be put on higher education institutions within Serbian security sector. In the last part of the paper, we will provide an overview of security-related curricula in Serbia at the very moment, with their brief analysis.

Historical Overview of Security-related Programs in Serbia

The history of higher education study programs in the field of security in Serbia has its origins in the establishment of military education for commissioned officers in the Principality of Serbia in the first half of the 19th century, and police education for Ministry of Interior officers in the first half of the 20th century. After couple of attempts by several officials to found the Military

Academy, in 1850 the Artillery School has been officially established as "the first military degree-granting institution in Serbia" (Military Academy, 2018). In 1880 it changed the name into Military Academy, which had several breaks in work during the Balkan Wars of 1912, the First World War, and during the Second World War. At the end of 1944, the wartime Military Academy of Democratic Federal Republic of Yugoslavia has been established, and it became a main pillar of military education with several academies divided through branches, arms, and services. After the break-up of Yugoslavia, the Military Academy was organized within two academies (one for technical services and logistics), and from 2006 as one academy, from 2011 within the newly established University of Defence.

Modern police studies in the Republic of Serbia have been institutionally established aftermath the First World War, and date back to 1920 when the famous Gendarmerie School for Non-commissioned officers in Sremska Kamenica was founded. After the World War II, the whole system passed the heavy set of reforms on the long term, culminating with the enactment of the Police High School of Internal Affairs in Zemun in 1972. According to the contemporary demands and needs of the profession, the Academy of Criminalistic and Police Studies was established on 27th July 2006, by the decision of the Government of the Republic of Serbia. It is an independent higher education institution that provides academic and professional study programs of all levels for the purpose of police education, and police and security affairs (Academy of Criminalistic and Police Studies, 2018).

These higher education traditions are today implemented within two main security sector higher education institutions, the University of Defence, and the University of Criminalistic and Police Studies. Besides the official higher education for the purpose of the armed forces and public and state security institutions, until the second half of the 20th century there was no systematic university-level education in security area. The first institutionalized attempt to include security-related education into civilian higher education system had its roots in the so-called *Concept of General People's Defence and Social Self-Protection*. The Concept was introduced in Socialist Federal Republic of Yugoslavia (SFR Yugoslavia) as a part of comprehensive training and education of all Yugoslav citizens with the goal of raising awareness and preparedness for wartime and peacetime threats during the Cold War era.

After the Second World War, then-Yugoslav party leadership built around the Partisan wartime movement, focused on maintaining the preparedness for defence of the country in the peacetime as well. The obligation for taking part in defence was not only on behalf of conscripted citizens, but also on youth and wider population. Starting from 1947, the General Staff of the Yugoslav People's Army introduced the pre-military training for all citizens, with special focus on schools. This training soon became an official part of curricula in secondary schools, high schools and university faculties, and in mid-1950s the first textbooks for pre-military programs appeared. From 1948 to 1970 there were fifty different textbooks published for secondary schools and faculties, under various titles depending on the specialization of school or faculty (*Pre-military Training, Civil Protection, First Aid*, etc.) (Dimitrijević, 2014:231).

Goals and contents of these education and training curricula changed in the late 1960s, when the new Law on General People's Defence was introduced along with the new Strategy by the same name. The new security environment was attributed with a Cold War-induced change in the character of warfare, and fast industrialization and urbanization in Yugoslavia changed the character of emergency management. Thus, the pre-military training was abandoned with the new obligatory school and university subject taking its place – General People's Defence and Social Self-Protection (ONO and DSZ). It was introduced from 1969 to 1974, and after the Concept of ONO and DSZ was adopted, it became a

standardized System of Education and Training of Youth for ONO and DSZ, which was implemented in four different ways:

1. "Education for ONO and DSZ in pre-schools and first four years of elementary schools;
2. Education for 5- and 6-graders within other curriculum subjects, and within extracurricular activities;
3. Education of secondary school and university students within specialized subject called Defence and Protection, within other curriculum subjects, and within extracurricular activities;
4. Education of youth without secondary education, within special defence and protection programs" (Bešker, 1989:42-43).

At approximately the same time in Yugoslavia, in the late 1960s and early 1970s, in the period of vast industrialization and expansion of civil engineering, within the University of Niš the Faculty of Occupational Safety was founded. Initially, the Faculty of Occupational Safety offered study programs for civil engineering safety, but it soon started widening its curricula as the industries started spreading, and introduced programs for explosions and fire safety. Today, the Faculty of Occupational Safety organizes study programs in occupational safety, environment protection and management, fire protection, emergency management, and communal system management, on all three cycles of studies.¹

The key year for security studies in Yugoslavia was 1975. In five out of six capital cities of the former Yugoslav republics (Slovenia, Croatia, Bosnia and Herzegovina, Serbia, and Macedonia) at the same time new departments for ONO and DSZ were introduced within the existing universities (Katić, 2011):

- *Department for Defence Sciences* at the Faculty of Social Sciences in Ljubljana (Slovenia);
- *Division for General People's Defence* at the Faculty of Political Sciences in Zagreb (Croatia);
- *Department for General People's Defence* at the Faculty of Political Sciences in Sarajevo (Bosnia and Herzegovina);
- *Institute for People's Defence/Department for Social Sciences and People's Defence* at the Faculty of Sciences in Belgrade (Serbia);
- *Division for General People's Defence* at the Faculty of Philosophy in Skopje (Macedonia).

The idea behind the introduction of these departments and divisions was to transit the education for the Concept of General People's Defence and Social Self-Protection from the state security structures (primarily the Ministry of People's Defence) into the civilian higher education institutions. However, the fact that the military structures were behind the implementation of the Concept, caused a resistance at some universities. That was an argument for then-university officials to claim that "the introduction of such curricula in civilian universities could cause a militarization of civilian higher education" (Bric, 2004:12). This kind of resistance was the biggest in Belgrade, where the department ended at the sciences faculty, instead at the social sciences faculty. Reasons for that could be sought in the aftermath of the 1968 students' protests at the University of Belgrade, when the *tour de force* were humanities and social science faculties.

Soon, only in Belgrade the existing department for the study of General People's Defence evolved into the independent faculty, the Faculty of People's Defence, in 1978. From its early beginning, the Faculty implemented its curriculum along with logistical support from the defence system, and used the facilities at the Military Academy. Because of the nature of the Concept of

¹ Faculty of Occupational Safety is part of University of Niš. More details about the Faculty could be found at: <https://goo.gl/g7FRuK> (Accessed on: 29.04.2018. 14:34).

General People's Defence and Social Self-Protection, students had the appropriate military training which was implemented two-fold: 1) through military-professional schooling in the first three years of study (with elements of basic infantry training), and 2) through internship in the units of Yugoslav People's Army in the final year (Dimitrijević, 2014:235). Graduated students were completely prepared for the title of Professor of Defence and Protection in secondary schools across country. The Faculty itself changed the name couple of times², and in the beginning of 1990s it was called the Faculty of Civil Defence.

After the break-up of Yugoslavia, the Concept of General People's Defence was abandoned, together with the need for secondary school subject. Along with the shift in global security paradigm, the Faculty was adjusting its curricula for new security challenges, risks, and threats. Unfortunately, during the 1990s the Faculty of Civil Defence did not enrol regular students, but provided a higher degree for students of police colleges of professional studies from Serbia and from the region. Also, besides the existing Police College of Professional Studies, the Government of Serbia established the Police Academy in 1993, that soon introduced first subjects, and later complete study programs in the area of security studies.

Expansion of Security Study Programs in Serbia after 2000

In the early 2000s, the Faculty of Civil Defence started with the enrolment of regular students again, and introduced four new study modules: 1) Security Studies, 2) Civil and Environment Protection Studies, 3) Defence Studies, and 4) Human and Social Resources Studies. It was the first faculty in Serbia to name the Security Studies at the time.

In 2006, the faculty changed its name to the Faculty of Security Studies, and today it enrolls students on all three study cycles within four-module bachelor studies, two master studies programs, two vocational studies programs and one at the PhD level.³ During the same period after the break-up of Yugoslavia, and especially in the early 2000s, numerous state and privately-owned universities and faculties started introducing the study programs in security-related fields. The scope and types of these study programs varied from international security to safety in engineering, and they are implemented within different scientific disciplines, from social sciences to technology.

The introduction of various security-related study programs on universities and faculties in Serbia was influenced by two main processes: 1) the security sector reform process after the democratic changes of 2000, and 2) global security threat of international terrorism after the 9/11 terrorist attacks. The security sector reform process in Serbia after 2000 largely influenced the development of the existing and the establishment of new security-related study programs. Firstly, the reform of armed forces, police, and security services introduced the academic content related to comparative experiences from former Eastern Bloc countries (Kešetović, 2005; Radovanović & Dapčević-Marković, 2007). The role of civil society in this process also had a positive influence on the introduction of various informal education programs carried out with the support from academia (Glišić, 2007), which soon evolved into vocational postgraduate studies on several faculties, like the Faculty of Political Sciences which introduced an undergraduate subject of global and national security (2001), and vocational studies of global and national security (2004), which soon became master studies program of international security. The important part of the security sector reform process was a regulation of private security. In accordance with that trend, the Faculty of Security

Studies, besides bachelor studies of security management, introduced vocational studies in security management (2002), along with crisis management studies (2005) at the same study cycle. On the other side, the event from September 11, 2001 introduced a new topic to universities worldwide – terrorism and counterterrorism studies. Serbia was not an exception, especially with the legacy of domestic terrorism still active at the time. The Faculty of Civil Defence introduced vocational studies of defence from terrorism in 2003, and the Faculty of Political Sciences introduced vocational studies of terrorism and political violence at the same time (Dimitrijević, 2011).

Approximately at the same time, in 2006, private universities and faculties started introducing the study programs in security-related area. The Academy for Diplomacy and Security introduced the diplomacy and security undergraduate and master studies, and the Faculty of Law and Business Studies introduced the management in business and civilian security undergraduate and master studies. Soon, other state-owned universities and faculties started with programs in security studies, like faculties of law on the University of Novi Sad and University of Kragujevac, which introduced police and national security studies. In line with the trends, the Academy of Criminalistic and Police Studies, as well as the Military Academy, started with programs focused on security. The Academy of Criminalistic and Police Studies had introduced police and security studies on undergraduate and graduate studies (vocational and master studies), and the Military Academy introduced the defence management studies within all three study cycles.

During the 2000s and 2010s the number of state-owned and privately-owned universities, faculties and colleges offering degrees in security-related areas grew rapidly. Even some area-specific security-related programs were introduced, like the airport safety and security studies within management in civil aviation studies (Megatrend University), or many variations of environment security and protection studies, ranging from social sciences to technology-oriented faculties. At the moment, one of the most prominent privately-owned universities in Serbia, Educons University, has two faculties with security-related programs, the Faculty of Applied Security and the Faculty of Security Studies, both of which offering programs on all three study cycles.

Lastly, in 2013, the Government of Serbia established the National Security Academy within the central civilian intelligence service, the Security-Information Agency. The Government's Decision establishing the Academy stated that "the Academy is established for higher education purposes, and development of scientific and research and professional work in the national security area, within interdisciplinary science fields of social sciences and humanities, sciences and mathematics, and technology and engineering sciences. At the Academy the multidisciplinary areas are studied, and specific knowledge for tasks in the security area is earned." (Government Decision, 2013). It is still, however, unclear which security-related tasks are the subject of the higher education within the Academy, but it could be easily concluded that the education is aimed at professionals from intelligence services. Although it is stated that the National Security Academy is established under the provisions of the Law on Higher Education, their curriculum is still unknown, and the information about their finances, faculty and other requirements is not transparent.⁴ However, the Academy earned the accreditation from the Commission for Accreditation and Quality Assurance, for bachelor studies (2017), master studies (2017), and professional career studies (2015).

² Briefly it was called the Faculty of General People's Defence and Social Self-Protection, then the Faculty of Defence and Protection.

³ More details about the Faculty, available at: <https://goo.gl/3YUZxE> (Accessed: 29.04.2018. 13:43).

⁴ The National Security Academy is not even mentioned in yearly Information about the Work of the Security-Information Agency, although it exists for five years now.

There are different explanations of sudden expansion and quality of security studies in Serbia after 2000. Milosavljević (2007) claimed that "Serbia and other transition countries do not have developed academic study of security", and that "the experts who are practically dealing with security-related tasks are produced within the security structures" (Milosavljević, 2007:50). He noted that in the "humble academic dealing with the security the predominant are formal aspects of security, and what is missing is interdisciplinary study of the role of security structures and security phenomena themselves" (Milosavljević, 2007:50). Ejđus, on the other side, made a reflection on key deficiencies which prevent the education system in Serbia to create a new generation of security experts in a satisfying manner (Ejđus, 2007:55). One of his observations is related to the quality of security studies as an academic discipline in Serbia, where he sees no significant scientific contribution of local authors in relation to the quantity of security-related scientific papers published in Serbia (2007:60). However, in the last ten years there have been several research efforts related to the quality of security studies in higher education in Serbia.

During the expansion of security-related study programs, Serbia had difficulties in security sector reform process during the 2000s, with private security sector still being unregulated despite various initiatives for adoption of legal framework in this area. The number of study programs in security management area was larger than the market needed it, so the question arose if these programs were appropriate for the existing situation. One of the possible explanations for such a vast number of security-related higher education programs could be the fact that there are many retired security professionals from armed forces, police, and security services with appropriate degrees for professor titles, who are willing to continue their careers in higher education system. Another explanation could be that traditional, security sector higher education institutions, have limited number of students, rigorous selection process, and quotas, so civilian study programs are perceived as a bypass for later entry into the security sector structure with a university degree. No matter the exact cause, professionals in the field agree that the existing number of study programs largely exceeds the real needs for professionals in this field.

Overview and Analysis of the Existing Security Study Programs in Serbia

Modern study programs in security-related area in its broadest sense, within the higher education system of the Republic of Serbia, could be summarized with the following categories of studies available on all three levels of higher education:

1. Security Science/Studies and National Security
2. Defence Management and Military Studies

3. Police, Forensic and Internal Affairs Studies
4. Security Management, IT and Corporate Security
5. Emergency and Disaster Management and Fire Safety
6. Occupational Safety and Safety at Work
7. Environmental Protection and Ecology
8. Terrorism, Organized Crime and Political Violence
9. International Security/Politics, Peace and Diplomacy

The previous division into nine categories derives from the current state of art of higher education in security in the Republic of Serbia. Overall, 16 state faculties within six universities, offer programs in security-related fields on all study cycles (BA, MA & PhD):

- **University of Belgrade** (Security Studies, Civil Engineering, Political Sciences, Agriculture, Chemistry, Technology and Metallurgy faculties)
- **University of Novi Sad** (Technical Sciences, Law, Sciences faculties)
- **University of Kragujevac** (Law, Sciences faculties)
- **University of Niš** (Occupational Safety, Law, Sciences faculties)
- **University of Defence** (Military Academy)
- **University of Criminalistic and Police Studies** (Academy of Criminalistic and Police Studies)

Nine privately-owned faculties and four universities, offer study programs in safety & security on all three study cycles (KAPK, 2018):

- **Educons University** (Applied Security, Environment Protection studies)
- **Metropolitan University** (IT Security studies)
- **Singidunum University** (Faculty of Applied Ecology)
- **Megatrend University** (Faculty of Law, Public Administration and Security)
- **Union University** (Faculty of Law and Business Studies)
- **Union "Nikola Tesla" University** (International Security, Environment Protection studies, and four faculties)
- **University "Business Academy"** (Law, Economy and Management faculties)

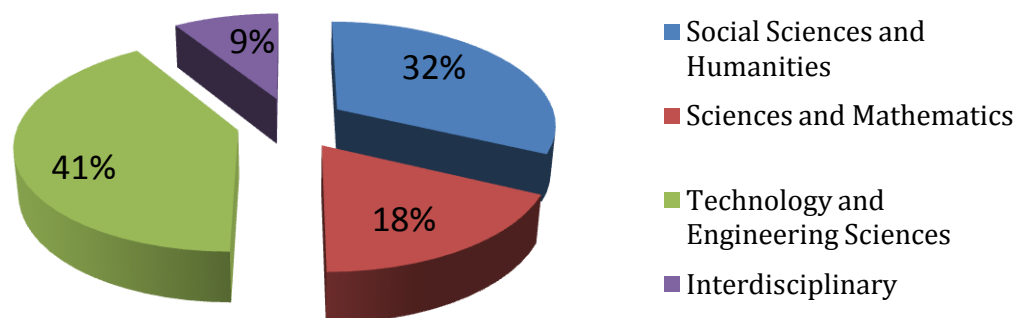
Existing study programs are offered on all higher education study cycles recognized by the Law on Higher Education and Accreditation Standards. There are academic study programs within universities and faculties. Also, there are professional/vocational study programs within universities, faculties and colleges of professional education.

Table 1. Programs in Safety & Security within the study cycles in the Republic of Serbia

ACADEMIC STUDIES	PROFESSIONAL STUDIES
1. Bachelor Studies (25%)	1. Professional Career Studies (13%)
2. Master Studies (35%)	2. Vocational Studies (13%)
3. Professional Academic Studies (12%)	
4. Doctoral Studies (2%)	

Source: Commission for Accreditation and Quality Assurance, 2018

Graph 1. Study programs in Safety & Security dispersion within the scientific areas



Source: Ibid.

There are six study programs in Serbian and English on state-owned faculties:

- **Civil Engineering** (Environmental Protection Studies, *PA studies*)
- **Political Sciences** (Peace Studies, *regional MA studies*)
- **Agriculture** (Environmental Protection, *MSc studies*)
- **Technology and Metallurgy** (Environmental Protection, *PhD studies*)
- **Technical Sciences** (Disaster Risk Management, *MSc studies*)
- **University of Defence** (Forensic Engineering, *MSc studies*)

There are four study programs in Serbian and English on privately-owned faculties:

- **Singidunum University** (Advanced Security Systems, *PhD studies*)
- **Educons University** (Environmental Protection, *BA studies*)
- **Educons University** (Environmental Protection, *MSc studies*)
- **Educons University** (Green Economy, *MA studies*)

Finally, there are four distance learning study programs within one state-owned and three privately-owned universities/faculties:

- **Civil Engineering** (Environmental Protection Studies, *PA studies*)
- **Metropolitan University** (IT Security, *MSc studies*)
- **Educons University** (Applied Security, *BA studies*)
- **Union "Nikola Tesla" University** (Security Studies, *BA studies*)

International joint programs in Serbia are organized within the fields of social Sciences and humanities (social work, business law, European integrations, Quantitative finance), natural sciences and mathematics, interdisciplinary Studies (cultural policy and management). There are 22 joint study programs in total, conducted with 15 partner institutions (University of Innsbruck, University of Salzburg, University of Rome, University of Trieste, University of Zagreb, University of Lion, University of Gottingen...). There is no single joint safety and security study programme. While there is none of doctoral joint studies at all, the distribution between joint MA and BA studies is vastly uneven. In total, 95% of the programs are dispersed into the master studies.

Referencing Mechanisms with the European Higher Education Area (EHEA)

National Serbian national qualification framework (NQF), law was adopted on Thursday, 5th of April, by Serbian Parliament. National Framework of Qualifications in Serbia (NQFS) is an integral part of the European integration process and the Chapter 26 – Education and Culture, with the planned referencing to European Qualifications Framework and mobility of workforce. The Law on NQFS shall envisage the establishment of a special Qualifications Agency, with the aim of providing quality on all levels of development and implementation of the National Qualifications Framework in the Republic of Serbia (NQFS).

The purpose of the referencing is to present transparently to other countries the way Serbia has connected its levels of qualifications with EQF and thus provided the fulfilment of appropriate procedures and criteria (ten) for the referencing. In order to be able to approach the process of referencing NQFS with EQF, it is necessary for Serbia to prepare a Report on Referencing, with the help of international experts, whose integral part shall be a Supplementary Report on the Self-assessment of NQFS in the field of higher education compared to Qualifications Framework in the European Higher Education Area (EHEA QF).

There are several referencing mechanisms on a disposal of non-EU member states. Even though some of them require full EU membership in order to be fully implemented, Serbia participates in most of them.

Youthpass is a tool to document and recognise learning outcomes from youth work activities. It is available for projects funded by Erasmus+: Youth in Action (2014-2020) and Youth in Action (2007-2013) programs. It is a part of the European Commission's strategy to foster the recognition of non-formal learning, putting policy into practice and practice into policy.⁵

Youthpass certificates are available for:

⁵ More information about the Youthpass system, available at: <https://www.youthpass.eu/da/about-youthpass> (20.04.2018. 14:43)

- Youth Exchanges, European Voluntary Service, Mobility of Youth
- Workers, Transnational Cooperation Activities (TCA)
- Structured Dialogue meetings

Europass is a European Union (Directorate General for Education and Culture) initiative to increase transparency of qualification and mobility of citizens in Europe. It aims to make a person's skills and qualifications clearly understood throughout Europe (including the European Union, European Economic Area and EU candidate countries).⁶ The five Europass documents are:

- Curriculum Vitae, Language Passport,
- Europass Mobility, Certificate Supplement,
- Diploma Supplement, sharing a common brand name and logo.

The European Association for Quality Assurance in Higher Education (ENQA) is an umbrella organisation which represents quality assurance organisations from the European Higher Education Area (EHEA) member states.

ENQA promotes European co-operation in the field of quality assurance in higher education and disseminates information and expertise among its members and towards stakeholders in order to develop and share good practice and to foster the European dimension of quality assurance.⁷

In most European countries, higher education institutions or study programs are subject to regular external review by a quality assurance agency. The European Quality Assurance Register for Higher Education (EQAR) is a register of such agencies, listing those that substantially comply with a common set of principles for quality assurance in Europe.

EQAVET is a community of practice that promotes European collaboration in developing and improving quality assurance in VET.

The European Credit System for Vocational Education and Training, often referred to as ECVET, is a technical framework for the transfer, recognition and (where appropriate) accumulation of individuals' learning outcomes with a view to achieving a qualification. Guided by a European-level Recommendation, ECVET relies on the description of qualifications in units of learning outcomes, on transfer, recognition and accumulation processes and on a series of complementary documents such as a Memorandum of Understanding and Learning Agreement.⁸

Table 2. Referencing Mechanisms and the Republic of Serbia status

MECHANISM	REPUBLIC OF SERBIA STATUS
Youthpass	Serbia is not formally member of the Youthpass system, even though, all the NGOs participating within Erasmus+ Youth in Action programs, could freely issue the Youthpass.
Europass	No membership existence. <i>De facto</i> all EHEA countries are implementing it.
ENQA	Serbia is a full member from 2013 (Commission for Accreditation and Quality Assurance) Self-evaluation report 2012-2015 available (SRB only): https://goo.gl/kGpnuw
EQAR	Formally Republic of Serbia is a full member from 2014; Serbian higher education institutions can't choose an EQAR-registered agency for their mandatory external quality assurance. Neither the European Approach is available to higher education institutions in Serbia.
EQUAVET	Serbia is not a member. Full EU membership required. EU Member States, European Economic Area countries and European Commission.
ECVET	Serbia does not have a local point. No further information applicable.

Source: Authors

⁶ More information about the Europass system, available at: <https://europass.cedefop.europa.eu/about> (20.04.2018. 14:47)

⁷ More information about the ENQA, available at: <http://www.enqa.eu/index.php/about-enqa> (20.04.2018. 14:50)

⁸ More information about the ECVET, available at: https://ec.europa.eu/education/policy/vocational-policy/ecvet_en (20.04.2018. 14:52)

Concluding remarks

Studying safety studies in modern circumstances is the pinnacle of an evolutionary course of development of security studies. Such a development was conditioned by various historical and social circumstances, phenomena and events that significantly influenced the change in the constellation of relations and forces within the international arena. There are several different determinants that "have enabled" in the longer run and contributed to the development of contemporary curricula and security study programs.

First, historical-political relations largely enabled the creation of two ideologically and militarily opposed blocs that served as the basis of what is modern in terms of studying security studies in general (and in Serbia). Then the so-called "broadening" and "deepening" of security studies reflected the need to create courses that examine a specific area in security studies. A typical institutional example of the contribution to the dissemination of the curriculum agenda is the 1994 United Nations Development Program Report, explicitly mentioning human security as a concept that (should) be prevalent in the development of modern humanity.

This has led to the development of entire departments and, of course, a multitude of different subjects at universities, not only at the levels of basic, but master, even doctoral studies. In addition to the institutional ones, examples of scientific contributions to the development of the curriculum are presented. The most typical is the contribution of the so-called critical schools, which indirectly initiated the education of a multitude of programs for master academic security studies.

The role of projects implemented by academic institutions in promoting and improving the system of higher education is extremely important. Project "Improving Academic and Professional Education Capacity in Serbia in the Area of Safety and Security - IMPRESS", is just one such project. It aims at creating a "knowledge union" in area of safety and security, promoting joint study programs in the field of security and protection, as well as enhancing the knowledge and capacity of stakeholders in order to increase the mobility of students, teachers, and non-teaching staff towards, and from the European Community Union. The project is funded by the European Commission within the Erasmus + program, and is conducted, among others, by the University of Belgrade, Faculty of Security Studies.

Although the processes that lead to the creation of joint study programs are extremely complicated due to various obstacles that may arise, the Republic of Serbia has a great starting point within which can benefit from membership in the European Higher Education Area. There are still no joint security programs at any level of academic studies, although there are many opportunities for short-term study stays in (primarily) the EU Member States. In the event of full EU membership, the Republic of Serbia will have the obligation to create joint study programs with at least 3 Member States in all scientific fields.

Literature

- Bešker, M. (1989). *Edukacija za obranu i zaštitu*. Zagreb: Fakultet prometnih znanosti.
- Bric, R. (2004). Ne verjamem, da se mladi na Primorskem manj zanimajo za vojaški poklic (the interview with prof. Anton Bebler from the Faculty of Social Sciences in Ljubljana), *Slovenska vojska*, XII(4), 12-15.
- Dimitrijević, I. (2011). *Akadske studije bezbednosti u Republici Srbiji od 2000. do 2008. godine (master rad)*. Beograd: Fakultet političkih nauka.
- Dimitrijević, I. (2014). Osnivanje i razvoj Fakulteta bezbednosti sa osvrtom na društvene promene i reformu visokog obrazovanja u Republici Srbiji. *Godišnjak Fakulteta bezbednosti 2014*, 229-243.
- Ejdus, F. (2007). *Saopštiti istinu moćnima: Da li obrazovna infrastruktura u Srbiji zadovoljava potrebe nove generacije stručnjaka za bezbednost?*, *Bezbednost Zapadnog Balkana*, 6, 55-62.
- Glišić, J. (2007). *Potreba postojanja nove generacije specijalista za bezbednost – Beogradska škola za studije bezbednosti*, *Bezbednost Zapadnog Balkana*, 6, 63-79.
- Katić, Lj. (2011). *Savremeni koncept nacionalne bezbednosti i profesionalno pripremanje kadrova (doktorska disertacija)*. Beograd: Fakultet bezbednosti.
- Kešetović, Ž. (2005). *Uporedni pregled modela obuke i školovanja policije (monografska studija)*. Beograd: Viša škola unutrašnjih poslova.
- Milosavljević, B. (2007). *Tri opšta problema studija bezbednosti u Srbiji i drugim tranzicionim zemljama*, *Bezbednost Zapadnog Balkana*, 6, 50-54.
- Radovanović, R. & Dapčević-Marković, Lj. (2007). *Visoko policijsko obrazovanje u Srbiji – stanje i nivo usklađenosti sa evropskim standardima*, *Nauka – bezbednost – policija*, 2, 147-168.
- Votkins, A. (2007). *Obrazovanje oficira u Srbiji: balansiranje tradicije i modernosti*, *Bezbednost Zapadnog Balkana*, br. 6, 91-99.

Legal sources

- Higher Education Strategy of the Republic of Serbia 2020*, Official Journal of the Republic of Serbia, No. 107/2012.
- Law on Higher Education*, Official Journal of the Republic of Serbia, No. 88/2017.
- Law on Military Schools and Scientific and Research Institutions*, Official Journal of the Republic of Serbia, No. 44/2005.
- Government Decision on the Establishment of the National Security Academy*, Official Journal of the Republic of Serbia, No. 39/2013, 70/2013.

Internet sources

- Commission for Accreditation and Quality Assurance (CAQA) (2018, February 9). *Guide through Accredited Study Programs in Serbia*. Available at: <http://www.kapk.org/en/home/> (Accessed on April 15th, 2018).
- ECVET (2018, April 20). *About the ECVET*. Available at: https://ec.europa.eu/education/policy/vocational-policy/ecvet_en (Accessed on April 20th, 2018).
- European Association for Quality Assurance – ENQA (2018, April 20). *About the ENQA*. Available at: <http://www.enqa.eu/index.php/about-enqa> (Accessed on April 20th, 2018).
- European Commission (2018, April 20). *The Europass*. Available at: <https://europass.cedefop.europa.eu/about> (Accessed on April 20th, 2018).
- European Commission (2018, April 20). *The Youthpass*. Available at: <https://www.youthpass.eu/da/about-youthpass> (Accessed on April 20th, 2018).
- The Academy of Criminalistic and Police Studies (2018, April 15). *History*. Available at: <http://kpa.edu.rs/en/academy/history-.html> (Accessed on April 15th, 2018).
- The Faculty of Security Studies (2018, April 29). *About the Faculty*. Available at: <https://goo.gl/3YUZxE> (Accessed on April 29th, 2018).
- The Military Academy (2018, April 15). *History*. Available at: <http://www.va.mod.gov.rs/cms/view.php?id=6581> (Accessed on April 15th, 2018).
- University of Belgrade (2018, April 15). *The History of the University*. Available at: <http://bg.ac.rs/en/university/history.php> (Accessed on April 15th, 2018).
- University of Niš, Faculty of Occupational Safety (2018, April 29). *About the Faculty*. Available at: <https://goo.gl/g7FRuK> (Accessed on April 29th, 2018).

MARITIME PIRACY AND ARMED ROBBERY EVOLUTION IN 2008-2017

Assistant-Professor Dr. Eng. Adelina Tumbarska

Institute of Metal Science, Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A. Balevski",
at the Bulgarian Academy of Sciences (IMSETHAC – BAS), Sofia, Bulgaria
E-mail: y.toumbarski@ims.bas.bg

Abstract: Maritime piracy and armed robbery against ships are one of the contemporary challenges to the shipping and have global impact on maritime trade and security. Following the boom of Somali piracy in 2009-2011, there has been a downward trend since 2012, resulting mostly from the international counter-piracy efforts, with reaching its lowest value for the last 20 years in 2017. However statistics show doubling the number of attacks in some other regions in the last several years accompanied by increased levels of violence. This report presents a survey of maritime piracy and armed robberies over the last ten years (2008-2017) by regions and countries, as well as by type of attacks on ships, personnel and cargo, with the purpose to outline the trends in contemporary marine crime.

Keywords: MARITIME PIRACY, MARITIME ARMED ROBBERY

1. Introduction

Maritime piracy is not a new phenomenon in the human history. With periods of peaks and relative lulls, piracy never ceased to exist. As a result of the increased activity in the beginning of 21st century, the piracy attracted considerable attention and was recognized as a modern transnational threat.

The world economy relies on the sea routes for 90% of its trade. Maritime piracy and armed robbery against ships are one of the contemporary challenges to the maritime industry and have a global impact on maritime trade and security. In addition to the economic losses, the pirate attacks also have a significant human cost for the captive sailors and their relatives.

Following the boom of Somali piracy attacks in 2009-2011, there has been a downward trend since 2012, with reaching its lowest value for the last 20 years in 2017. It is reassuring to see historically low piracy levels off Somalia and in the Indian Ocean, resulting from years of international counter-piracy efforts, however statistics show doubling number of attacks in some other regions, as well as increased levels of violence. "While pirate attacks have been on the decline off the Horn of Africa, piracy and armed robbery at sea in the Gulf of Guinea has been a cause of increasing international concern, as the attacks often involve great risk to the crew on the captured ships, whose lives are often secondary to the value of the cargo for the pirates". [1]

This report presents a survey of maritime piracy and armed robberies over the last 10 years (2008-2017) by regions, as well as by type of attacks on ships, personnel and cargo, with the purpose to outline the trends in their development in the coming years.

2. Definition and types of pirate attacks

The two sub-sets of maritime crime are armed robbery at sea, occurring within a nation's territorial sea, and piracy, which takes place in waters beyond the territorial sea. Various definitions of piracy can be found in different sources. One of the most common definitions describes piracy as the act of boarding any vessel with intent to commit theft or any other crime, and with an intent or capacity to use force in furtherance of that act. In other words piracy is an act of robbery or criminal violence at sea through illegal use of force by non-state actors known as "pirates".

According to the United Nations Convention on the Law of the Sea (UNCLOS), piracy is defined as any of the following acts: a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft; (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State; (b) any act

of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft; (c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b). *Armed robbery against ships*, according to the International Maritime Organization (IMO) definition, consists of any of the following acts: (a) any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against persons or property on board such a ship, within a State's internal waters, archipelagic waters and territorial sea; (b) any act of inciting or of intentionally facilitating an act described above". [2]

The term "piracy" encompasses two distinct sorts of offences: the first is robbery or hijacking, where the target of the attack is to steal a maritime vessel or its cargo; the second is kidnapping, where the vessel and crew are threatened until a ransom is paid. [3]

- *Maritime robbery* differs little from armed robbery on shore. A few men with knives can easily overpower an unarmed crew and take their belongings. Since the value of this booty is rather limited, these crimes are opportunistic, occurring when the vessel is at port or if the pirates' plans for a bigger venture go wrong. If hostages are taken, it is to ensure a clean escape, not to extort ransom.

- *Hijacking* is an attack intended to steal the vessel or the cargo. Such offence is a profitable, but in general difficult operation. The crew of the target vessel, rather than being the object of the attack, is simply an impediment, to be offloaded as quickly as possible. As a result, many of these attacks involve violence as the pirates need unobstructed withdrawal to repaint the abducted ship or unload the cargo. Finally, there must be a nearby market for either second-hand ships or cargo of questionable provenance.

- *Kidnapping* for ransom is usually the most profitable, but very difficult to carry off successfully. It requires intelligence to locate target vessels far out at sea; heavy armament, to subdue the vessel and deter rescue; long-term commitment and shore support, to weather the protracted negotiation process; money laundering, to allow the ransom (in international currency) to be digested. [3]

The incidents categorization in accordance to the effect on crew, vessel and cargo, proposed by the International Maritime Bureau (IMB), includes 3 levels:

- Level I: accidents which have direct impact on crew: crew being taken hostage, injured, kidnapped, killed, missing, threatened; hijacking where the command of the ship is taken over by those boarding; accidents where the crew retreats into the citadel.

- Level II: includes a vessel being fired upon, security team firing against approaching threat, robbers/pirates identified with weapons (violence is offered) whether boarding or otherwise.

- Level III: incidents which does not fall into either Level I or Level II.

3. Statistical data and methodology used

Statistical data used are taken from the annual piracy and armed robbery reports of the IMB¹ in the period 2008-2017 - [4-13].

Methodology of the study consists of the following. Initially, the statistics from the IMB annual reports for the 10-year period were collected and summarized. Then data concerning attacks by regions for the entire 10-years period were analyzed. The number of attacks by the countries having the big share in world maritime crime in periods 2008-2012 (the peak of piracy activity - during the boom of Somali piracy) and 2013-2017 (the period after the successful eradication of Somali piracy) were analyzed and compared to data for the same countries in the last 2 years (2016-2017). The character of attacks in regard to their effect on vessel, cargo and crew was examined for two 5-year periods: 2008-2012 and 2013-2017 in order to compare the character of attacks in these periods, and interpreted also by countries and regions. Special attention is paid to the last 2 years of the period of review in order to outline the trends in contemporary piracy.

4. Results and discussion

Attacks by regions and countries

In 2008-2012 pirate attacks were largely confined to four major areas: the Gulf of Aden, near Somalia and the southern entrance to the Red Sea; the Gulf of Guinea, near Nigeria and the Niger River delta; Malacca Strait between Indonesia and Malaysia; and off the Indian subcontinent, particularly between India and Sri Lanka. [14]

Unprecedented growth of pirate attacks off the coasts of Somalia (a country with a 3,300-kilometer coastline, Africa's longest) in 2009-2011 caused international concern over the new piracy due to its high cost to global trade. Multinational naval forces were formed to patrol in the region, which led to a steady drop in the number of incidents since 2012. The number of incidents in Southeast Asia, which demonstrated significant growth in 2012-2015, also declined in 2016-2017 compared to the previous 4 years. On the other hand, the West Africa, especially the Gulf of Guinea (a key gateway for oil shipments from Nigeria and Angola), has become the new piracy hotspot since 2014.

The number of pirate and armed robbery acts reported to IMB within the period 2008-2017 is presented by regions in Table 1 and Fig.1. The annual report of IMB for 2017 indicated 180 incidents - the lowest annual number since 1998 when 188 incidents were reported.

Table 1. Number of pirate and armed robbery attacks by regions

Region	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
SE Asia	54	45	70	80	104	128	141	147	68	76
East Asia	11	23	44	23	7	13	8	31	16	4
Indian Sub-cont.	23	29	28	16	19	26	34	24	17	15
South America	14	37	40	25	17	18	5	8	27	24
Africa	189	266	259	293	150	79	55	35	62	57
Rest of World	2	6	4	2	0	0	2	1	1	4
Total	293	406	445	439	297	264	245	246	191	180

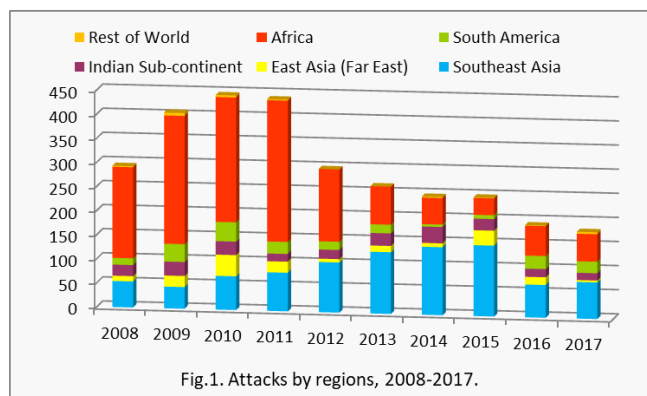


Fig.1. Attacks by regions, 2008-2017.

The share of attacks by countries on the total attacks over the world for the periods 2008-2012, 2013-2017 and 2016-2017, is shown in Fig.2.

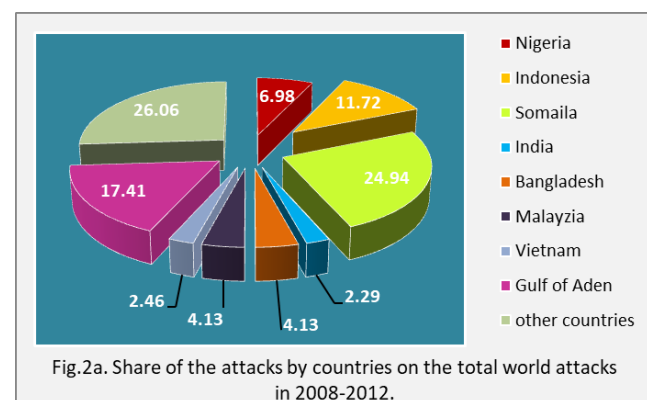


Fig.2a. Share of the attacks by countries on the total world attacks in 2008-2012.

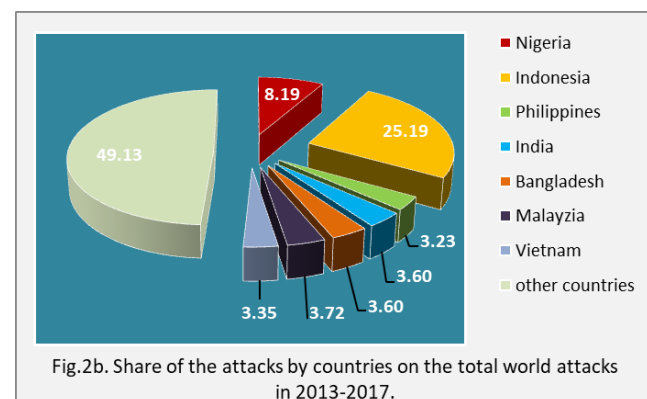


Fig.2b. Share of the attacks by countries on the total world attacks in 2013-2017.

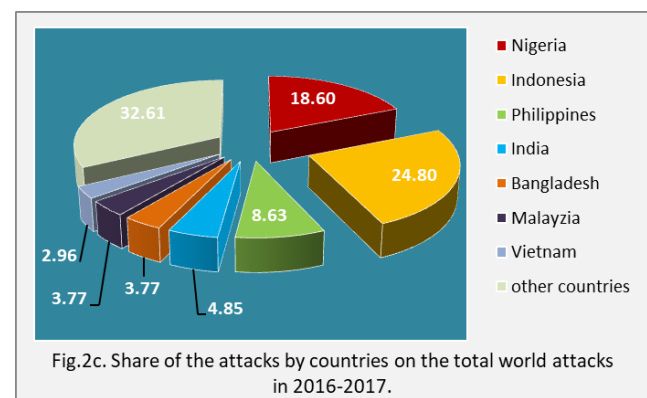


Fig.2c. Share of the attacks by countries on the total world attacks in 2016-2017.

¹ The International Maritime Bureau (IMB) is a division of the International Chamber of Commerce (ICC) established to act as a focal point in the fight against all type of maritime crime and malpractice. A key service of the IMB is reporting the piracy and armed robbery at sea incidents. IMB is publishing comprehensive quarterly and annual reports detailing piracy statistics.

The largest amount of pirate attacks in the 10 years surveyed was registered off Somalia and the Gulf of Aden, which represented almost half of the pirate attacks around the world in 2008-2012. After the peak in this period, a drastic decline has been observed in the region in the next period. Among the rest countries with the greatest number of pirate attacks, Indonesia was leading for the

entire period. In the last 5 years, Indonesia has invariably ranked first with 406 attacks (over 100 attacks yearly in 2013-2015, and twice decreased number in 2016-2017). Nigeria occupied the second place with 210 attacks in 2008-2012 and 132 in 2013-2017, regardless of significant decrease in 2014 (less number of attacks than Bangladesh and Malaysia) and 2015 (when it takes the third place after Indonesia and Vietnam). The Philippines appeared within the "top 5" of the list in 2016, and, with number of attacks doubled in 2017 compared to the previous two years, occupied the third place for 2016-2017 at the expense of India, where attacks have dropped significantly over the previous four years. The relative share for the other countries of the group having the greatest "contribution" to global piracy remained almost unchanged within the entire period. The number of attacks in Nigeria and Philippines, respectively their relative shares, has increased more than 2 times in 2016-2017 compared to the previous few years.

Types of attacks against vessels and crew

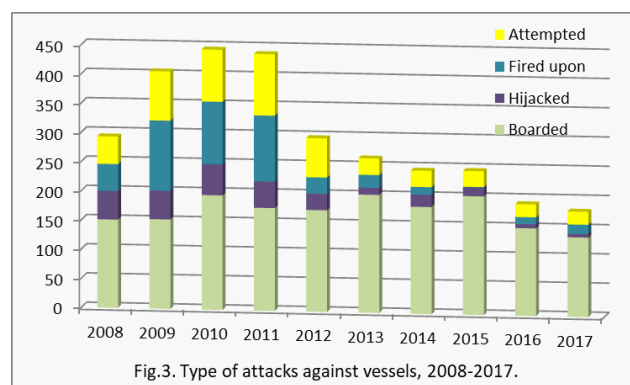
Modern pirates tend to attack and hijack cargo ships and fishing vessels, which have commodities readily sellable on the black market, and therefore rarely direct their attention towards cruise ships. "Smaller pirate gangs, who do not have the resources to seize the cargo being transported, instead often board a ship to steal substantial amounts of the cash ships carry for payroll and port fees, and the recent trend is more frequent kidnappings of crewmembers to be exchanged for ransom money". [15]

Globally, the number of boarded ships in the period 2008-2017 varies in relatively narrow boundaries on the background of the significant changes in overall attacks during the period, as is seen on Table 2 and Fig.3. The number of vessels hijacked and fired upon drastically falls in years following the peak of Somali pirates' activity, marking minimum values in 2016-2017. An interesting observation can be made concerning the ratio of unsuccessful attacks (attempted and firing upon ships) and actual attacks (boarded and hijacked ships): in 2009-2011 approximately half of attacks has been unsuccessful, while 79-89 % of the attacks in the years following 2012 have succeed. Most likely explanation for the more frequent failures of pirate attacks during their peak activity is the powerful international naval presence in the region with the highest concentration of pirate attacks, together with increased vigilance and security measures on vessels off Somalia coast. Besides, in the second half of the period under review, low-level (low-risk) attacks worldwide are prevalent.

The period 2008-2012, with the boom of Somali piracy, is characterized by a significant share of hijacking ships and keeping crew as hostages. The Somali piracy is unique in that almost all attacks involved hostage situations, which were often long lasting (an average 6 months to get large ransoms), with patience and strategy. "Somali piracy has been largely free of violent tactics because it is in the pirates' interest to keep their hostages alive". [14] In the Gulf of Guinea, pirates usually hijacked ships for several days and after stealing cargo, sailors were released. Preferred pirates' targets in this period were oil tankers. "Pirates conceal boats and stolen commodities in the thousands of inlets, rivers and mangroves that comprise Nigeria's coast. Crude oil is unloaded to criminal partners and resold on the local market through government and non-government facilitators". [16]. In Southeast Asia, piracy was focused on the ransacking cargo and fishing products from vessels like tugs, trawlers and passenger boats. Hijacking occurred mostly in Malaysia, Indonesia and Strait of Malacca. "In Southeast Asia, pirates are increasingly hijacking ships to steal oil from slow-moving tankers but rarely seek to ransom the crew. They capture tankers, sail them to a mother ship and siphon off the fuel, then release the boats with their equipment smashed and, at times, the crews badly hurt. (Because the crews are generally not ransomed, analysts say, they may be likelier targets for violence than was the case in East Africa.)". [17]

Table 2. Type of attacks against vessels

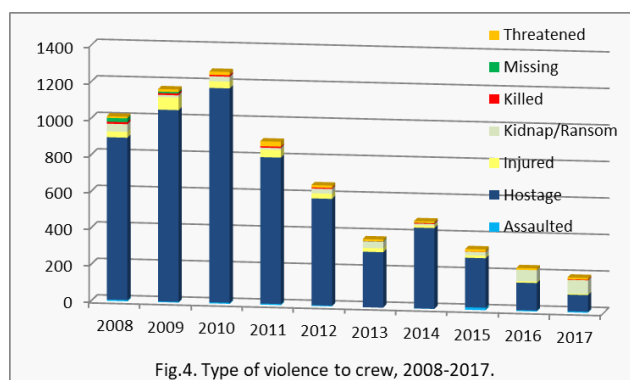
Vessels	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Boarded	151	153	196	176	174	202	183	203	150	136
Hijacked	49	49	53	45	28	12	21	15	7	6
Fired upon	46	120	107	113	28	22	13	1	12	16
Attempted	47	84	89	105	67	28	28	27	22	22
Total	293	406	445	439	297	264	245	246	191	180



Since 2013 the majority of incidents were low level attacks (robberies). Only a few incidents in the Somali pirates' area of activity were registered till 2016, but 3 vessels have been hijacked in 2017, demonstrating that Somali pirates still had willingness and capabilities to attacks. The rest 3 cases of hijacking in 2017 were in Malaysia and Indonesia. In the Gulf of Guinea, after the downturn in oil prices, pirates are expanding their hostage-taking to include off shore supply vessels and general cargo ships. Pirates of the West coast of Africa are often well armed and violent and have hijacked and robbed vessels, and kidnapped and injured crews along the coast, rivers, anchorages, ports and surrounding waters. The violence to crew is illustrated in Table 3 and Fig.4.

Table 3. Type of violence to crew

Crew	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Assaulted	7	4	6	6	4	0	1	14	5	6
Hostage	889	1050	1174	802	585	304	442	271	151	91
Injured	32	69	37	42	28	21	13	14	8	6
Kidnap/Ransom	42	12	27	10	26	36	9	19	62	75
Killed	11	10	8	8	6	1	4	1	0	3
Missing	21	8	0	0	0	1	1	0	0	0
Threatened	9	14	18	27	13	10	9	14	10	10
Total	1011	1167	1270	895	662	373	479	333	236	191



Statistical data show significant decrease of the number of crew held hostages in the last 5 years. On the other hand, since 2016 the

share of kidnapping has risen several times compared to previous 7 years. Pirates off Nigeria are leading in kidnappings with 29 crew members abducted in 2016 and 65 (of the world total 75) in 2017. The rest cases of kidnappings in 2016-2017 are in Malaysia (2016) and the Philippines (both years).

For the first months of 2018 (1 January – 31 March) the IMB reported 66 incidents of piracy and armed robbery against ships which is considerably higher value than that for the first quarter of 2016 (37 incidents) and 2017 (43 incidents). Worldwide 39 vessels are boarded and 4 are hijacked, 100 crew members taken hostages and 14 kidnapped. "As a region, the Gulf of Guinea accounts for 29 of the 2018 Q1 incidents and all four of the vessel hijackings. With the exception of one crew member, all crew kidnappings and hostages taken occurred in the Gulf of Guinea. As a country, Nigeria recorded 22 incidents". [18] Attacks in the Gulf of Guinea are against all vessels. Crews have been taken hostage and kidnapped from fishing and refrigerated cargo vessels as well as product tankers. In January-April 2018 two pirate attacks against tankers, which have been thwarted by the armed guards onboard, are registered in the Gulf of Aden.

5. Conclusion

In 2008-2012 pirate attacks were largely confined to four major regions: the Gulf of Aden, the Gulf of Guinea, the Malacca Strait and off the Indian subcontinent. Unprecedented number of attacks was registered off Somalia coast and the Gulf of Aden in 2009-2012, most often aimed hijacking ships and crew for ransom, with crew kept hostages for several months. Growing number of attacks was observed in Southeast Asia, especially in Indonesia. Most attacks over the world in this period, except the area of Somali pirates operations, were low-level incidents (robberies). Hijackings were targeted mostly at tankers and cargo ships with the intent to steal and sell the cargo, often with significant violence against crews. In 2012-2017, regardless the significant reduction of overall number of attacks after eliminating Somali piracy, the number of attacks in most of the other hot spots remained almost constant, with predominant low-level incidents. Since 2014 the Philippines appeared amongst countries having the biggest shares of the world piracy. In 2016-2017 the number of attacks in Indonesia has decreased compared to the previous several years, however in the Gulf of Guinea attacks increased more than twice. The number of hijacked ships and crew kept hostages over the world decreased significantly in the last two years. In result, 2017 is the year with the lowest level of maritime crime for 20 years. On the other hand, there is an alarming increase of attacks in the Gulf of Guinea near Nigeria, especially kidnapping crew for ransom, in the last two years and the beginning of 2018. The escalation of kidnapping and hijacking in West Africa since 2016 is a cause for serious concern and gives reason to conclude that piracy tends not only to increase, but to become more violent, and is likely to give a new impetus to piracy and armed robbery at sea across the globe.

6. References

- [1] Strategy for the Danish measures against piracy and armed robbery at sea 2015-2018, May 2015. <https://www.dma.dk/Documents/Publicationer/>
- [2] Piracy and armed robbery against ships. International Maritime Organization. <http://www.imo.org/en/OurWork/Security/PiracyArmedRobbery/Pages/Default.aspx>
- [3] Joubert, L. The Extent of Maritime Terrorism and Piracy: A Comparative Analysis. *Scientia Militaria, South African Journal of Military Studies*, Vol. 41, No 1, 2013, pp. 111-137. https://www.ajol.info/index.php/smsajms/article/...
- [4] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2008. ICC International Maritime Bureau, January 2009. http://www.rk-marine-kiel.de/files/piraterie/imb/imb_piracy_report_2008.pdf
- [5] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2009. ICC International Maritime Bureau, January 2010. http://www.rk-marine-kiel.de/files/piraterie/imb/imb_piracy_report_2009.pdf
- [6] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2010. ICC International Maritime Bureau, January 2011. http://www.rk-marine-kiel.de/files/piraterie/imb/imb_piracy_report_2010.pdf
- [7] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2011. ICC International Maritime Bureau, January 2012. http://psm.du.edu/media/documents/industry_initiatives/industry_reports/maritime_imb_annual-report-2011.pdf
- [8] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2012. ICC International Maritime Bureau, January 2013. <https://www.kvnr.nl/stream/2012-annual-imb-piracy-report>
- [9] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2013. ICC International Maritime Bureau, January 2014. http://www.ship.sh/attachment/files/2013_Annual_IMB_Piracy_Report.pdf
- [10] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2014. ICC International Maritime Bureau, January 2015. <https://www.hellenicshippingnews.com/wp-content/uploads/2015/01/2014-Annual-IMB-Piracy-Report-ABRIDGED.pdf>
- [11] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2015. ICC International Maritime Bureau, January 2016. <https://www.hellenicshippingnews.com/wp-content/uploads/2016/02/2015-Annual-IMB-Piracy-Report-ABRIDGED.pdf>
- [12] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2016. ICC International Maritime Bureau, January 2017. <http://www.allaboutshipping.co.uk/wp-content/uploads/2017/01/2016-Annual-IMB-Piracy-Report-ABRIDGED.pdf>
- [13] Piracy and Armed Robbery Against Ships. Report for the period 1 January - 31 December 2017. ICC International Maritime Bureau, January 2018. <https://www.hellenicshippingnews.com/wp-content/uploads/2018/01/2017-Annual-IMB-Piracy-Report-Abridged.pdf>
- [14] Christopher A. and S. Christopher. Combating Maritime Piracy. Council on Foreign Relations, March 2012. <https://www.cfr.org/backgrounder/combating-maritime-piracy>
- [15] Modern Day Pirate Attacks by Country. Worldatlas, January 2018. <https://www.worldatlas.com/articles/modern-day-pirates-countries-with-the-most-maritime-piracy-today.html>
- [16] Starr, S. Maritime Piracy on the Rise in West Africa. Combating Terrorism Center at West Point, USA, APRIL 2014, VOLUME 7, ISSUE 4, <https://ctc.usma.edu/maritime-piracy-on-the-rise-in-west-africa/>
- [17] Sjolín, S. Forget Somalia - this is the new sea piracy hot spot, Market Watch, October 2015. <https://www.marketwatch.com/story/forget-somalia-this-the-new-sea-piracy-hot-spot-2015-10-07>
- [18] ICC-IMB: World-Wide incidents of piracy and armed robbery against ships from January to March 2018. Maritime Cyprus, April 2018. <https://maritimecyprus.com/2018/04/11/icc-imb-world-wide-incidents-of-piracy-and-armed-robbery-against-ships-from-january-to-march-2018/>

MODEL OF TACTICAL POLICE ACTION WHEN USING PHYSICAL FORCE

Assoc. Prof. Dr. Jonche Ivanovski¹, Assist. Prof. Dr. Aljosha Nedev²,
University "St. Kliment Ohridski", Faculty of Security - Skopje, Republic of Macedonia
E-mail: jonche_i@yahoo.com; aljosanedev@yahoo.com

Abstract: *The police, as a public service, while performing its legal activities has at its disposal preventive and repressive forms of action. It is a rule that the preventive forms of action always have the priority, and only in specific circumstances the police is obliged to use repressive measures, such as: physical force, means of restraint, rubber baton, firearms, police dogs, etc. In this paper, only the use of physical force from tactical and security points of view is analyzed. This paper includes detailed analysis and elaboration of a model that refers to the most important phases of the police work. The structure of the model includes several tactical and security activities that determine the manner of tactical police actions during the whole procedure of performing police duties. The initial phase of the procedure includes: identification and evaluation of the seriousness of the threat, establishing verbal communication and maintaining optimally safe distance. The further phases, depending on the situation and according to the rules of self-defense, include using certain amount of physical force in order to reject the threat or to bring under control the resistance.*

Keywords: POLICE, PHYSICAL FORCE, TACTICAL PROCEDURE, DEFENSE TECHNIQUES, ACTIVE RESISTANCE, PASSIVE RESISTANCE, PHYSICAL ATTACK.

1. Introduction

In the Republic of Macedonia, the police are authorized and responsible for putting into practice the provisions of the Law on Police [18], as well as the other by-laws which are part of this Law [14, 17]. In order to execute their legal activities, the police dispose of the preventive and repressive forms of action. As a rule, the preventive forms of action have the priority, for example: rubber baton, firearms, handcuffs, etc. [7]. This paper focuses mostly on the physical force, which as a method of restraint can be applied in the following situations:

- to restrain the resistance of an individual who disturbs the public peace and order, and to restrain the resistance of an individual who needs to be detained, arrested or deprived of liberty;
- to restrain someone who is trying to attack the police or the facility which is safeguarded;
- to prevent the escape of an individual who has been found near or on the crime scene and who is suspected of committing the crime.

The use of physical force, which helps in putting under control the resistance of another person includes application of numerous defense and attack techniques, and for these reasons, it is very important to analyze all circumstances and events in regard to security, because the goal of the procedure is to apply only those defense techniques in achieving the goal of law which are least dangerous and cause little or no damage [2]. As a rule, physical force should only be applied during the defense or attack, because if it continues with the same intensity after the defense or attack, it can lead to authorization overstepping. In order to prevent this, police officers should tend to focus on those parts of the body which are less likely to be severely injured. Taking into consideration the different forms of physical force, it is extremely important to choose the most suitable method and to prevent the threat on time, because every prolongation increases the danger and risk of inadequate police actions.

2. Tactical and security procedure for the use of physical force

When police officers use physical force they should be well acquainted with the legal rules and regulations in order not to overstep their professionalism, ethic and human behavior [8]. Apart from taking into consideration and legal provisions, the police officers should work to provide conditions for adequate tactical action, mostly when it is known that physical force is used in specific circumstances that put into danger the safety and in which counterattack is prevented and disabled, and when resistance is being restrained or when escape is being prevented.

It is very difficult to establish strict tactical rules of action in cases when physical force is being used, but it is very important for the whole process to make suitable security evaluation and to make

decision for choosing the adequate techniques (ventures) which would help police officers to eliminate the danger on time and to put under control the assailant [15]. The tactical proceeding during the use of physical force includes several tactical and security activities which influence on the manner in which the individual should be brought under control before any physical contact is established, during the intervention and after the intervention [16].

2.1. Initial tactical activities when physical force is being used

The police officers, when starting any tactical procedure, in order to avoid physical contact with the individual and to exclude the possibility of using physical force, try to solve the conflict peacefully (preventively). In order to act tactically as best as possible on the beginning of the procedure, the threat is identified and assessment of its seriousness is conducted, and then, based on the information that was collected, a strategy for the further procedure is being made. When the threat is estimated, the seriousness of the danger and the possible reaction of the individual are being determined.

During the analysis of the risk factors, the police officers take into consideration every threat that has been manifested (verbal assaults, disobedience of the law, ignoring the warnings, provocative attitudes) and potential risks of assault (hiding the hands, change of facial skin color, suspicious facial expressions, widening of the pupils, fast breathing, change of moving direction, etc. When all direct and indirect danger indicators are being observed and perceived, visual control on the person is achieved by approaching him naturally, like trying to start a conversation - interview (figure 1) [10].



Figure 1. Initial tactical approach for verbal communication with an individual

During the establishment of this spatial position, the body is turned half-left or half-right from the face, the hands are alongside the body or put in front of the abdomen, the knees are slightly bent with equal weight distribution on both legs, and feet are shoulder width apart. With this posture, in order to provide safe

communication, the person is held at a distance of at least 1.5 meters. From tactical point of view, this distance is also called 'safety zone distance', because it allows police officers to timely react, withdraw, prevent attack, or to prevent the individual to use any sharp object or weapons [4].

During the time the police officers have this posture, they should be careful not to cause irritation and to provoke the individual with their posture, but it should only help them to provide tactical advantage and control of the whole situation. In order to maintain the necessary visual control on the person, it is necessary, by giving commands, to impose their will, in other words, to convince the individual to give up from their planned intentions. Controlling the situation, with the help of communication is of crucial importance for reducing the psychological and emotional tensions of the individual, but also in order to achieve their intentions, police officers must react quickly and to show that they are able to apply certain tactical and communication skills [5]. In such intense (insecure) situations, the verbal messages directed on the individual should be short, straightforward and unambiguous and reflect the security circumstances at the moment.

Regarding the types of the problem (impeding an attempt of taking objects that can cause bodily injuries, impeding an attempt of committing a crime, witnessing that someone is committing a crime, giving resistance by lying down, sitting, holding to some object, disobeying legal orders, trying to escape or escaping, etc), police officers, when addressing use the following phrases: 'stop every movement and stay there!', 'step back!', 'throw the object far away!', 'keep calm, we will try to solve the problem!', 'you must immediately leave this place!', etc.

In cases when the verbal advices, suggestions, warnings and orders will not give the expected results (preventive solution of the conflict), tactical actions for impeding the attack or bringing under control the resistance with the use of physical force is imminent. In order to react quickly and on time, the police officers put aside the abovementioned attitude of making conversation and engage into defensive attitude or prepare to fight (figure 2) [6]. In order to guarantee the needed stability and protection during the fight, the police officers bent down and go one step back or in front, while the hands are raised vertically to chest with the palms opened.



Figure 2. Taking fight position during the use of physical force

When the police officers take fighting position, if all specific elements which part of this process (diagonal position of the feet, elbows bent and parallel to the body, body weight equally distributed on both legs, head down) are properly applied, quality for timely and successful reaction and conduction of different tactical ideas will be guaranteed. Adequately taken fighting position is a starting point of the application of different technical and tactical elements (use of different techniques and blockades, hits, suffocations, falls and other fighting techniques), which are used by police officers during the fight in order to overcome the resistance and to stop (block) the attack [9].

In the first part of taking the fighting position, despite of the need to take suitable tactical position in space it is also very important to not allow the fighting position be a reason or motive 'act of provocation' for undertaking activities that will lead to physical confrontation, but it should help police officers to reduce the tension and exclude the possibility to solve the conflict with use of force. This mostly refers to those situations in which the

individual does not show much resistance, or shows minimal (not dangerous) intentions to attack. In order to bring the whole situation under control and to have the time to react if the following course of the action requires the use of physical force, the individual should not be allowed to approach very close, in other words, on a distance in which he/she can 'grab' the police officer [10, 16]. To maintain this distance and to prevent the individual to get very close so he can harm the police officer, it is necessary that the police officers know how to rationally manage the space. During the fight, and depending on the specificity of the security circumstances and the reactions of the individual, the police officers can move in every directions, in other words, to move the body walking in front, stepping back and moving left or right [9]. In order to maintain the body in a position optimal for fighting, it is necessary to keep the body in the previously taken fighting position. This means that police officers should not allow too much vertically directed oscillation from the center, transferring body weight only on one leg and crossing the legs.

While police officers try to maintain safe distance from the person when moving in fighting position, they must, within a short period of time, predict the further steps (intentions) of the person, and in accordance with the current situation, to plan the tactical activities during the use of physical force. Taking into consideration the complex and changeable circumstances in which they act, it is very difficult in a short period of time to evaluate all circumstances which are part of the situation and it is crucial to notice the most important elements that point out in which manner physical resistance or attack will proceed. Starting from the fact that the use of physical force is a collection of different combat activities, methods and procedures, police officers must quickly and efficiently choose the most suitable technique 'tool' that would be most adequate for the current situation and according to the rules of applying self-defense skills, to stop (disable) the person to achieve their goals (figure 3) [3].

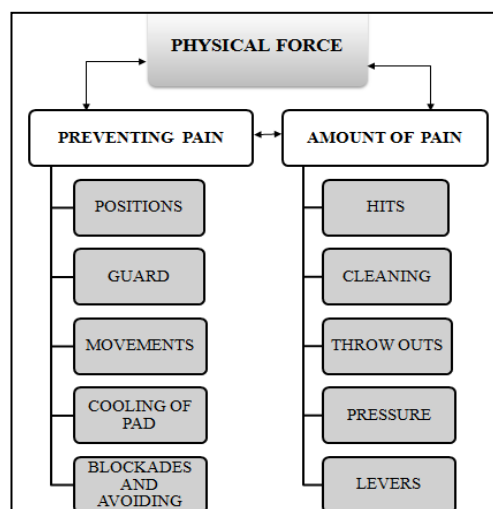


Figure 3. Types of self-defense techniques during use of physical force

Because the system of self-defense techniques that is used in the form of physical force includes numerous technical elements (positions, blockades, hits, throw outs, pressure, fixations, levers, avoiding, etc) which differ according to their structure, dynamics, intensity, time, it is very important to structure and combine them promptly during the performance of the tactical activities.

According to the already given classification, the first group of techniques that are applied during the use of force allows successful situational approach and space management without allowing the possibility certain dangers to arise which would cause physical injuries (preventing pain), while the second group of techniques is applied to control the person by causing him certain amount of pain on certain parts of the body.

2.2. Tactical phases of the use of physical force

Taking into consideration the wide spectrum of elements which are part of the groups of techniques, they are mostly applied during the conduction of the following tactical phases [1]:

- Tactical phase of use of physical force during defense;
- Tactical phase of use of physical force during an offensive (counter-attack);
- Tactical phase of use of physical force when preventing an attack.

When the tactical phase of defense is being carried out, the primary goal of the police officers is to establish suitable position in regard to the attacker, to move in space quickly, precisely and with good maneuvers and to use suitable blockade techniques. In cases when the attack has already started, the defensive tactic or the self-defense includes combined techniques which cover moving in fighting position and blockade techniques. Regarding the attack (hits with the fist, hits with an open palm, hit with an elbow, knee, leg, foot, using different objects) and the maneuver in which these are applied (directly, laterally, semicircular, from up to down and vice versa, backwards, combined, etc.), different types of defense movements are being carried out (stepping forward straightly or diagonally, stepping backwards, stepping left or right, rotating on one leg, etc) which block the attacks by rejecting them, using different body parts (avoiding) without allowing physical contact with the attacker (figure 4) [9].



Figure 4. Use of physical force during defense

When this tactical phase is being carried out, it is extremely important not to allow the attacker to use series of attacks that would unnecessary put into danger the personal security of the police officers. The tactical action should help police officers to provide conditions for transition from defensive to offensive attack or counter-attack.

Due to the time limitations which are typical for both tactical phases, police officers must quickly and energetically develop defense transformation and prepare a plan (action) for application of certain self-defense tactics during the further course of action. Because the process of planning and preparing offensive attack is timely limited, the choice of suitable techniques must be strictly coordinated to the behavior of the person, because it will reduce the possibility of increasing the resistance and police officers will gain time to bring the person under control.

When the offensive attack is launched, the elaboration of the information and the speed of the reaction after the defense are the elements which determine the structure of the attack and the selection (composition) of the techniques of self-defense which are applied as strategic methods during the attack. In such complex (uncertain) circumstances when the police officers determine the structure of the attack, two types of offensive attacks can be put into practice [12]:

- Attacks with simple (easy) structure, and
- Attacks with complex structure.

The simply structured offensive attacks contain limited number of techniques and methods (one to three defense techniques. These

techniques, even limited, can belong to different groups and subgroups of the different methods used in the form of physical force (figure 5). In this context, different groups (combinations) of techniques can be applied, such as: hits with the fists (direct punch with open or closed palm, semicircular punch with the fist, semicircular punch with the elbow), leg kicks (direct leg kick, roundhouse leg kick, lateral leg kick, knee kick), throws or flips (throwing some object, manual flips, leg flips), levers (levers with stretching out the ankle, levers with bending the ankle, levers with twisting the ankle, combined levers), grabbing techniques, suffocation techniques, etc [11].



Figure 5. Use of physical force during an offensive attack

Unlike the simple offensive techniques, the structure of the complex attacks includes more segments (techniques, group of techniques, compositions) which are significantly more numerous than the elements of the attack with simple structure. Most frequently, the attacks with complex structure are used when police officers fail to bring under control the resistance of the person by using attacks with simple structure.

The tactical stage of the use of physical force during prevention of attack is applied when the person has not still launched the attack or is starting to launch it (initial phase). In order to prevent this attack or to disable its further development, suitable tactical space positioning and the ability to quickly and timely approach the person is crucial for solving the conflict. The self-defense techniques that are used in order to prevent the attack are applied individually or combined with the other techniques, as well as in the previous tactical phases (figure 6).



Figure 6. Use of physical force during attack prevention

Taking into consideration all complex and changeable situations which require the use of physical force during the conduction of the tactical phases, it is impossible to previously establish strict sequence of actions, because these phases are mutually interrelated and connected to each other.

3. Conclusion

The legal obligation and duty of the police during the conduction of the regular and special actions is to act on a manner which would minimize the need of applying use of force when possible. Unfortunately, in reality, the police come more and more frequently in contact with citizens who express certain dissatisfaction which often impedes the possibility of peaceful solution of the conflict. The concept of applying persuasion, advice and warning which aim to deter, can only be achieved when the citizens who are communicating with the police at that given moment rationally understand the consequences of their actions. On the other hand, those citizens, who in most of the cases are

unpredictable or who manifest aggressive behavior are most frequently repressed, or physical force is applied on them. As a result of the many dynamic and uncontrolled variables which are result of the conflict between the police and citizens and which leads to the possibility of physical injury of one or both parties, it is extremely important that the police show that they are able to act professionally, rationally and tactically which is in accordance with the stipulated legal, security and ethic rules and norms.

3. References

1. Амановић, Ђ., Балтић, Р., Суботички, С. (2001). Тактика Специјалног физичког образовања и тактика поступања у примени овлашћења. Зборник радова наставника ВШУП, 4, р. 211-225.
2. Арлов, Д. (2003). Физичка сила као средство принуде у заштити безбедности припадника полиције. Зборник радова: Угрожавање безбедности припадника полиције - узроци, облици и мере заштите, р. 197-222.
3. Арлов, Д. (2006). Алати самоодбране. СИА, Нови Сад.
4. Defensive Tactics Training Manual. GitHub <https://www.whatdotheyknow.com/request/.../Full%202011%20UDT%Manual.pdf> [Accessed: 12.03.2018]
5. Дуковић, П., Суботички, С., Клисарић, М., (2009). Примена овлашћења полиције - Увод у полицијску тактику. Министарство унутрашњих послова, Београд.
6. Ghid de intervenție profesională - Editura MAI www.editura.mai.gov.ro/.../ghid%20de%20interventie%20profesionala.pdf [Accessed: 25.03.2018].
7. Ivanovski, J., Nedev, A. (2013). Usage of coercion means for protection of the personal safety of police officers. International Scientific Conference, The Balkans between Past and Future: Security, Conflict resolution and Euro-atlantic Integration, 1, p. 279-290.
8. Ivanovski, J., Nedev, A. (2017). Application of the model of use of force in the process of detaining persons. International Scientific Journal Security&Future, 1, p.11-16.
9. Јакимов, Ј. (2011). Специјално физичко образование, Факултет за безбедност, Скопје.
10. Kalem, D. (2011). Provera identiteta osoba. Policija, sigurnost, 1, p. 114-124.
11. Kosanović, B. (1988). Samoodbrana. Obrazovni centar za unutrašnje poslove SR Hrvatske.
12. Mudrić, R., Milošević, M., Jovanović, S. (2004). Napad u karateu - edukacija i trening. Viša škola unutrašnjih poslova, Beograd.
13. Praktični postopek (uporaba policiskih pooblasti, poenotenje policiskih postopkov), Ministerstvo za notarnje zadeve, Ljubljana, 1997.
14. Правилник за начинот на вршење на полициските работи, "Сл.Весник на Р.Македонија", 149/2007.
15. Ribičič, G., Svitlica, M. (2008). Taktika policijskog postupanja pri savladavanju fizičkog napada. IX slovenski dnevni varstvoslovja, Zbornik povzetkov, Bled.
16. Тактички пристап кон современата полициска обука, ОБСЕ Набљудувачка мисија во Скопје, 2006.
17. Уредба за употреба на средства за присила и огнено оружје, "Сл.Весник на Р.Македонија", 23/1998.
18. Закон за полиција."Сл.Весник на Р.Македонија", 114/2006.

THE ATTITUDES OF THE EUROPEAN UNION ON THE DEVELOPMENT OF THE COMMON SECURITY AND DEFENSE POLICY

Colonel PhD. Eng. Angelov I.

National Military University „Vasil Levski“ – Veliko Tarnovo, Republic of Bulgaria

ivailoaa@abv.bg

Abstract: *By asking the question of the creation of a single European army, we must say that the political will to integrate EU security and defense action is a primary factor. If Member States really want to guarantee the security of their citizens, to protect their humanitarian values in a global context, they have to have a huge political desire and not just "written documents".*

Keywords: SECURITY, DEFENCE, "BRUSSELIZATION", "EUROPEIZATION"

1. Introduction

Even at present, it is still difficult to find one uniform definition of the European Union because of its unique and complex character. Leading reference books give different definitions for the Union, and while some emphasize on the free market as one of its distinguishing features, others are focused on the political element, whereas the rest of them pinpoint its uniqueness. If we have to summarize, it could be said that the EU is a political and economic union without an equivalent, having its own internal logic associated with the gradual formation of a specific European identity based on universal values, shared by all European citizens, as well as, the formation and implementation of policies such as the Common Foreign Policy and Common Security and Defense Policy of the European Union.

2. European Union - The Common Security and Defense Policy

Despite the imperfections that the Union has today, in view of budgetary restrictions, military capabilities and historical overlaps, the EU has its uniqueness and potential for its rightful presence on the global stage. The development of this potential is a prerequisite for building a strategic vision for the future, supporting the European citizens, enhancing its political will and capabilities for its implementation, recognizing the fact that achievable security and defense solutions are increasingly associated with a renunciation of national sovereignty.

Its uniqueness lies also in the fact that it possesses the largest (non-military) capabilities to overcome crises and is the largest net contributor of funds to support the development of other countries¹. From institutional point of view, it should be noted that we have:

- on the one hand, a bureaucracy that is quite different from the classical bureaucracy, as the Brussels bureaucrats are historically a brand spanking new type of employees being the first ones to serve neither their sovereign nor their government, and the first ones to call into question the national bureaucracy and even sometimes to revise or reject the regulations and decisions of their own national governments;

- on the other hand, there is an attempt the concept of democracy to be institutionalized and a perception of political responsibility to be developed, a perception which will be able to peel itself away from the short term moods of the political majority.

In Eurobarometer 80 in a survey published in the autumn of 2013, European citizens say that after the free movement of people, goods and services, among the most positive results of the EU are: the peace among the member states of the Union (cited by 53% of respondents) and the political and diplomatic EU influence in the world (cited by 19% of respondents). On the question which of the values best represent the EU, the highest percentage of respondents point out - peace (37%), then human rights (34%) and democracy (30%)².

According to Prof. Ingrid Shikova, three are the fundamental pillars of the European project: First, the European Union is a political project and a common vision for its existence is necessary. What citizens expect from the present day leaders is the intellectual model of the future European political unification. This is not necessarily a federation or any of the already familiar models. It can and must be original and unique, as is the current European integration system. It is very important to provide a shared vision for creating and operating effective policies in important areas such as energy, infrastructure, including common foreign policy. Second, unity does not mean unification. This fundamental principle is very important because United Europe has different cultures, different languages, different sensitivities; each country has its own ambience and specific traits.

Individual differences can very well co-exist with the European and universal values. Thirdly, the shared vision for the future of the European project should be based upon the fact that in the conditions and characteristics of the world's 21st century development, in order to conquer a solid position and influence, for the sake of its voice to be heard, Europe must be really united, not only on paper. Probably, the most prominent example that could be given here is the Common Foreign and Security and Defense Policy Programs, which exist as an option in the Treaty of Lisbon, but are still not actively implemented in practice, and Member States often act differently and even quite contradictory³. Despite the significant changes introduced by the Lisbon Treaty in the CSDP decision-making procedures, the principle of intergovernmental cooperation and coordination is still applied.

The decision-making process within the EU is a complex combination of institutional interests and practices, governments' positions, binary democratic control, from national parliaments on one hand and from the citizens on the other. It is also a combination of leadership strategies, regulatory and bureaucratic procedures for reaching consensus and efforts to initiate and implement certain policies. The theory of rational choice has contributed to the explanation of the dynamics of intergovernmental relations and the decision making processes concerning important issues. The theory proposes two solutions that would help to boost the confidence among the member states that their duties and responsibilities will be respected:

- collecting and sharing sovereignty - when states strongly engaged in the management of supranational institutions agree to decide on mechanisms other than unanimity;

- delegated sovereignty - when supranational institutions attain the capability to take autonomous decisions without intervention by voting or one-sidedly imposed veto.

According to the rational choice theory, CSDP brings together the benefits of cooperation so that Member States can increase their influence on the world stage⁴.

There is also an additional logic for the "sharing" of sovereignty in the field of security and defense, based on the so-called "Two-

level games"⁵ according to which governments prefer to have the support of international organizations in order to be able to lay the blame on such organizations in the event of failure and to make it easier for them to justify the extended use of force as legitimate at national level. Having into consideration the opportunities provided by the Lisbon Treaty, there are still theoretical gaps in explaining the daily dynamics of policy making in the sector, "Brusselization" and "europeization", which also greatly influences the fundamental image of the CSDP. The process of brusselisation means the transfer of duties and functions from national capitals to the enlarging expertise capacity of the structures and institutions located in Brussels, thus aiming for greater efficiency.

Closely linked to the process of "brusselization" of the CSDP is the process of "Europeanisation" of the national policies, i.e. the expertise accumulated in Brussels, the processes and activities that take place there, have an impact on national policies⁶. Thus, the European institutions are currently developing both their political and military capabilities. Therefore, it seems possible for the EU to develop its strategic culture perception, despite the still persisting problem related to the reluctance to use hard power⁷. Institutions are part of the political processes in a given society and, in this respect; public opinion is a key factor in the process of institutional response to the changes in the security environment.

An interesting trend is observed in TNS opinion⁸ research and analysis, which examines citizens' attitudes to defense policy in Europe, whether it is a priority and whether it should be managed at national or European level. The study focuses on two dimensions - present and future. Empirical results show that "today" EU security and defense is important for citizens. On one hand, this is due to the possibility of receiving real-time information about emerging and existing conflicts and tensions in every part of the world, as well as problems in their own countries. On the other hand, this trend is due to the economic and financial crisis, which has grown into a social one, and this is what citizens consider a potential threat to increase tension between states and, respectively, it is linked to the defense policy. Although at present 74% of respondent EU citizens support the Common Security and Defense Policy, an interesting moment are the discrepancies in the results in terms of the future. Despite the strong support for the EU security and defense policy at present, in the future the citizens will prioritize social and public policies that will have an impact on their everyday lives.

As a result, the problems of defense and security rank an unenviable position in comparison to the problems of poverty and social exclusion, the economic, budgetary and fiscal coordination, the problems of improving further the consumer protection and public health. This shows the mixed feelings of Europeans on the topic. On one hand, they strongly support further integration into the CSDP and, at the same time, consider that defense expenditures should be kept at the current levels or reduced. The lack of unambiguous understanding on the side of public, which takes into account the challenges in the security environment yet still prioritizing other areas does not justify, but gives some explanation of the current situation in the security and defense sector. Under these attitudes, the Lisbon Treaty is an adequate response, providing a regulatory framework for the future security and defence policy of Europe.

However, the limited resources allocated to security and defense question the realistic assessment of the situation that should be underlain in a future Common European Strategy. The feasible level of integration of European security and defense policy is specified in Articles 42 to 46 of the specially developed section 2 of the Treaty of Lisbon but the real one depends on the level of political will and civil support for the application of the new provisions.

Over the past years, following the adoption of the Treaty of Lisbon in 2007, the EU has managed to implement practically a large part of the planned changes in the field of CFSP and CSDP. New structural units at political, military and administrative level have been established within the Union and are functioning. A High

Representative of the EU for Foreign and Security Policy was appointed and the External Relations Office was established. A Political and Security Committee has been established and functions as a permanent body. The established European Defense Agency fulfills its assigned missions and tasks. The EU carries out a number of operations, using military and civilian capabilities thus contributing to strengthen security in the world. Since 2003 under the auspices of the EU, dozens of missions have been carried out, such as: the military operations in the Republic of Macedonia (FYROM), the Democratic Republic of Congo and Bosnia and Herzegovina, the civilian-military supporting operation in Darfur, the Congolese defense reform mission, in Aceh (Indonesia), a border guard mission in Ukraine, Moldova and Rafah (Gaza Strip), police missions in Bosnia and Herzegovina, Republic of Macedonia (FYROM), Palestinian Territory and Congo, as well as missions in Georgia and Iraq.

A distinguishing characteristic of the CSDP is the focus on coordination rather than cooperation as a problematic element of collective action, given the nature that most European missions are sporadic and reactionary. CSDP is dominated by crisis management system which demands from the Member States to respond to regional and international crises in limited time. The scattered nature of these missions shows that the EU has no common vision of how it views the global environment and what image it wants to project on it⁹. Although the EU has been achieving significant progress in adopting and implementing a number of policies to respond to post-Lisbon challenges, it is still felt the need for new ways to be found to enhance integration in the area of foreign policy, security and defense.

The EU's ability to speak with one voice on economic matters enables it to influence the international scene. The transfer of this capability to foreign, security and defense policy would outline a power capacity that would earn the EU its corresponding position in the global system of international relations¹⁰. Economic and military interdependence is characterized by the fact that it is an integral part of traditional international politics and to a great extent is a consequence from social conditions and perceptions¹¹.

3. Conclusion

However, not the domestic political needs of the separate EU Member States, but the serious global challenges will most likely be the ones to incite the speeding up of the integration process in the field of security and defence policies. The Union undoubtedly needs its own strategy, a bold vision of a well-thought-out wholeness between high goals and means to achieve them.

With regard to European citizens' attitudes towards defense policy in Europe, the following two conclusions are to be drawn: firstly, in terms of overall influence, the EU sometimes finds it difficult to position itself on the international scene against the United States, China, even Russia. Therefore, having a European army capable of intervening quickly and effectively in a crisis situation would strengthen the voice of the Union among the international community.

Second, from an economic and budgetary point of view, defining European military needs and pooling defense spending, EU member states would avoid duplication and unnecessary costs. Member states should put aside their differences in the strategy and develop a common European strategy. This, in turn, would benefit not only member states but also non-EU members when they need assistance to improve their situation and resolve the crises they face.

The state and the traditional understanding of sovereignty are based on both approaches - supranational and intergovernmental. Differences arise from the final goal of whether to change the understanding of the currently existing concept for nation state or to create a new European super-state.

For some, the Lisbon Treaty is a step towards the European superstate, for others it invalidates the "federal vision" for the European Union.

In fact, the Lisbon's Treaty final evaluations by analysts, commentators and policymakers are at cross-purposes primarily due to differences in the perception of past and present expectations of the EU's future development. It can hardly be said that the Lisbon Treaty finds the right balance between supporters of deeper integration and radical Eurosceptics.

On the other hand, the Lisbon Treaty does not address a number of issues in the economic sphere: the further development of the Single Market and the Economy of Knowledge, increasing the competitiveness of the European economy, and last but not least, finding the most appropriate means to deal with the environmental and energy issues.

Solving these issues does not necessarily require new mechanisms, but rather a rigorous implementation of existing legislation, creativity, and new approaches to globalization. A good contract can be an important tool, but it cannot replace the need of political will and the determination to carry out particular tasks that correspond to the goals and ambitions set.

4. Reference

1 In 2012, net payments made by the European institutions to partner countries and multilateral organizations amounted to 17.57 billion dollars. <<http://www.oecd.org/dac/europeanunion.htm>>

2 Standard Eurobarometer 80. European citizenship report. November 2013
<http://ec.europa.eu/public_opinion/archives/eb/eb80/eb80_citizen_en.pdf>

3 Shikova, I. Policies of the European Union. University Publishing House St. Kliment Ohridski, 2011. pp. 331-334

4. Wagner, W. Why the EU's common foreign and security policy will remain intergovernmental: a rationalist institutional choice analysis of European crisis management policy. Journal of European Public Policy. August, 2003.p. 576–595

5. „Two-level games“, Putman (1988)

6 Breuer, F. Sociological Institutionalism, Socialisation and the Brusselisation of CSDP. Chapter 6

7 Matlary, J.H. When Soft Power Turns Hard: Is an EU Strategic Culture Possible?

8 TNS opinion. What place is there for defence in the context of crisis?,
<<http://www.tns-opinion.com/sites/default/files/Defence%20and%20security%20policy.pdf>>

9 Seselgyte, M. „A Grand Strategy for the EU: Top-down or Bottom-up Approach?“ EGS Towards a European Global Strategy 2013. 22 Feb 2013. <<http://www.euglobalstrategy.se/nyheter/opinions/a-grand-strategy-for-the-eu-top-down-or-bottom-upapproach>>

10 Pantev, P. Centers of Force in International Relations and the Problem of Polarity in the 21st Century. Sofia, 2014, p. 74

11 Nye, Josep Jr. Understanding International Conflicts An Introduction to Theory and History.,1993. p. 203

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_iseudoing_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.

HISTORY AND DEVELOPMENT OF NUCLEAR WEAPONS

ИСТОРИЯ И РАЗВИТИЕ НА ЯДРЕНОТО ОРЪЖИЕ

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: An overview of the emergence and development of nuclear weapons has been made since its creation to the present day. Described are the attempts and consequences of using this weapon. What are the accumulated capacities in the world and what is their prospect for mankind? Described are the parameters of the current nuclear abatement agreements.

Keywords: control monitoring, radiation control, radiological risk, radionuclides, radiometric measurements, gamma background

1. Introduction

The nuclear weapon is the main powerful weapon of mass destruction of the enemy.

The energy of explosion of the charge of the normal explosive substance (BB) is released as a result of a chemical reaction, during which the explosive molecules become more resistant molecules of the explosive products. In these explosions the atoms do not undergo any alteration. In the nuclear explosion, the source of energy is nuclear reactions, resulting in which atoms of some elements are transformed into atoms of other elements.

Nuclear blasts are used to:

- the critical reaction of the division of the core elements;
- the reaction to the synthesis of the light element nuclei (thermonuclear reaction).

Chain reaction of division

A chain reaction of nucleation is called a reaction which, starting with one or more cores, can continue in the substance without external action, i.e., self-sustaining.

The division of atomic nuclei into nuclear munitions is under the influence of non-drones.

The heavy nucleus, affecting the neutron, becomes unstable and is divided into two parts, representing nuclei of the atoms of the lighter elements (Figure 1).

The division of the core is accompanied by the release of a significant amount of nuclear energy and the release of the two or three neutrons called secondary. Secondary neutrons are capable of dividing two or three new cores, resulting in two to three neutrons from each split core, etc. If the number of secondary neutrons causing the nucleus division is increased, an accelerated nucleation response occurs in the substance in which the number of fission nuclei grows avalanche (Figure 2). This reaction runs in millions of seconds and represents a nuclear explosion.

If the number of neutrons causing the division of the nuclei remains constant during the reaction, an explosion will not be produced. These reactions are used in nuclear power plants.

When the number of secondary neutrons leading to division is reduced, the reaction subsides.

Under the influence of neutrons, the nucleus of many of the heavy elements can be divided, however, most of the releasing neutrons are insufficient for the next division of the other nuclei, and the chain separation process is not possible.

From the natural isotopes only in uranium-235, and from the artefacts - in uranium-233 and pluton-239, a nuclear fission chain reaction can develop. It is these three isotopes that are used today as a division into nuclear power.

Chain reaction can develop not in any amount of nuclear material. In a less mass substance, much of the secondary neutrons formed by the separation will take off beyond the boundaries of the universe without causing further divisions.

The smallest mass of the fissionable substance in which under certain conditions a chain reaction can be developed is called critical. The mass of the substance less than the critical mass is

called the mass, and the mass exceeding the critical mass over the critical mass.

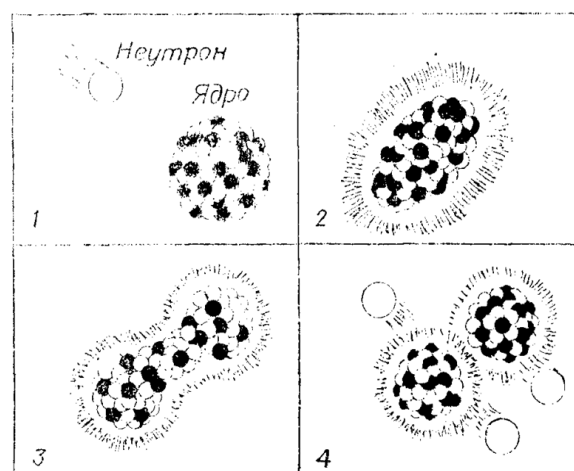


Figure 1. Core partition process:

1-core bombardment of neutron; 2 and 3 - the generation of an intermediate (excited) nucleus found in an unstable state; 4 - division of the core nucleus with particle formation - the nucleus of the new elements - n secondary neutrons

The magnitude of the critical mass depends mainly on the geometric shape, density and composition of the fissile material and the surrounding material.

The smallest critical mass at other equal conditions has the ball-shaped charges. In these charges, the number of secondary neutrons that take off beyond its boundaries is minimal. The critical mass for a uranium-235 ball is 40-60kg, and for a pluton-239-10-20kg ball.

The critical mass of the fissile is reduced as the density increases. This allows, by artificially raising (for example, by blasting a normal BB by means of an explosion), the density of the particle to reduce its critical mass.

The critical mass of the fissionable substance can be reduced by placing the charge in a reflector sheath that returns a portion of the neutrons to the reaction zone.

The division of all atomic nuclei contained in one gram of uranium or pluton releases approximately as much energy as the 20 tons of explosion.

In the reaction zone of blasting division the temperature reaches tens of millions of degrees and the pressure - tens of billions of atmospheres. Under the action of such a high temperature n pressure, most of the charge substance is sprayed and the reaction is quickly quenched.

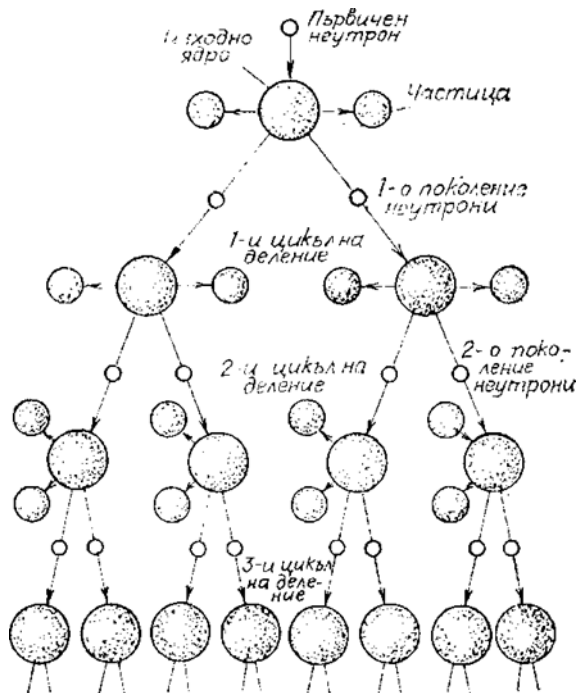


Fig. 2 - The development of a nuclear fission chain reaction

2. Synthesis reaction (thermonuclear reaction)

In the synthesis reaction, light cores are formed to form heavier ones. A mixture of hydrogen isotopes - deuterium and tritium, as well as lithium isotopes - is used to effect the synthesis of nuclear fuel.

The synthesis reaction is possible only at temperatures of several tens of millions of degrees. To create such temperature conditions a nuclear explosion based on the split reaction is used. Therefore, the thermonuclear explosions take place in two stages: the explosive reaction of the division of the nuclear charge, which is something like a detonator, then the synthesis reaction.

When joining all the cores contained in 1 g of deuterium-tritium mixture, approximately the same energy is released as in the 80 tons of explosion.

In the thermonuclear reactions neutrons with very high energy occur. They can cause a division of the nuclear atoms of uranium-238.

This feature has allowed us to use the comparatively cheap and most common in nature uranium-238 for nuclear fuel. In its use, the nuclear explosion takes place in three stages: the reaction of the division of uranium-235 or pluton-239 creates conditions for the synthesis reaction, and the synthesis of neutrons causes division of the uranium-238 nuclei.

2.2. Principles of Nuclear Munitions

Devices designed to carry out nuclear explosions are called nuclear charges. Nuclear charges are the nuclear explosive substance (sometimes referred to as nuclear fuel) in which the explosive splitting or synthesis reaction may take place.

Depending on the nature of the explosive reactions, we distinguish nuclear charges of division (or atomic charges), fusion-synthesis fusion charges, fission-synthesis-division fusion charges or combined thermonuclear charges.

The main elements of the nuclear charge divisions are: a fissionable substance (the nuclear charge itself), a neutron reflector, a charge of the ordinary explosive, and an artificial source of neutrons.

The formation of the overcritical mass of the particle in the nuclear divisions can be accomplished in different ways.

In the so-called "charge" charges, the formation of the overcritical mass occurs by increasing the density of the fissile by virtue of its non-uniform approximation by the explosion

pressure of the ordinary explosive. The fissile in these charges has a mass less than the critical mass and is charged in the charge of a normally explosive substance. At blasting of a normally explosive material is subject to high pressure, its density increases, the mass becomes overcritical (Figure 3) and a split response develops. The higher the pressure, the higher the supercritical the nuclear fuel and the higher the explosive power, respectively. When increasing the density of the dividable substance, for example twice the critical mass is reduced four times.

Other charging schemes are possible. For example, in the so-called gunnery charges, nuclear fuel is divided into two or more subcritical dimensions in order to initiate a self-sustaining chain reaction in each of them.

If nuclear fuel is divided into two parts, the supercritical mass is formed by joining the parts using the ejection charge of BB (Figure 4, a).

The speed of convergence of these parts to a large wall depends on the fullness of the reaction flow and, ultimately, on the explosive power. These charges are relatively simple in design, small in size, and can be used to shoot small-scale nuclear munitions. When splitting nuclear fuel into several parts (Figure 4, b), the overcritical mass is also created by blowing up the BB charges, resulting in all parts of the fissile being joined together in the center of the nuclear charge and converging. This fracture of the burst by explosion of ordinary BB increases the power of the nuclear explosion.

The neutron reflector provides a reduction in the critical mass of the charge and helps to increase the explosive power at the same amount of fissionable substance.

Artificial and non-tropical artefacts are used to excite the splitting chain reaction at the exact time to increase the number of concurrent starting divisions.

The fission-synthesis fusion charges (Figure 5) have in their composition a nuclear charge of fission and fusion fuel, lithium deuteride (a chemical compound of deuterium with the isotope of lithium-lithium-6), and in the case of the detonation of such charges the third is obtained directly in the blast process (when neutrons affect lithium-6).

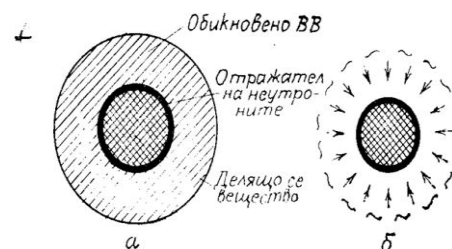


Fig. 3- Nuclear charge of the split-type implosives type: a - before the explosion (density of the divider - normal, mass less than the critical mass); b - in the moment of the explosion (density of the dispenser, higher than normal, mass greater than the critical mass)

In the case of explosion of a normally explosive substance, the fissile is subjected to high pressure, its density increases, the mass becomes overcritical (Figure 3) and a split response develops. The higher the pressure, the higher the supercritical the nuclear fuel and the higher the explosive power, respectively. When increasing the density of the dividable substance, for example twice the critical mass is reduced four times.

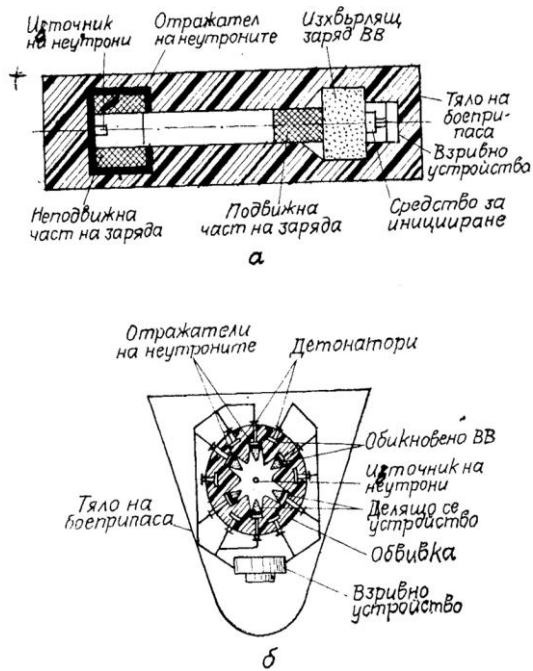


Fig. 4. Nuclear charge scheme:

a - the dispenser is divided into two parts; b - the divider is divided into several parts

Other charging schemes are possible. For example, in the so-called gunnery charges, nuclear fuel is divided into two or more subcritical dimensions in order to initiate a self-sustaining chain reaction in each of them.

If nuclear fuel is divided into two parts, the supercritical mass is formed by joining the parts using the ejection charge of BB (Figure 4, a).

The speed of convergence of these parts to a large wall depends on the fullness of the reaction flow and, ultimately, on the explosive power. These charges are relatively simple in design, small in size, and can be used to shoot small-scale nuclear munitions. When splitting nuclear fuel into several parts (Figure 4, b), the overcritical mass is also created by blowing up the BB charges, resulting in all parts of the fissile being joined together in the center of the nuclear charge and converging. This fracture of the burst by explosion of ordinary BB increases the power of the nuclear explosion.

The neutron reflector provides a reduction in the critical mass of the charge and helps to increase the explosive power at the same amount of fissionable substance.

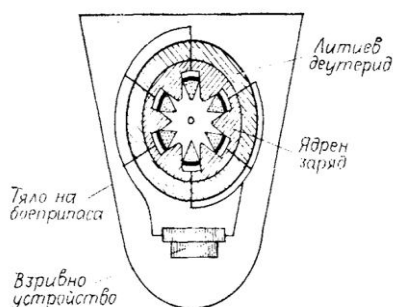


Fig. 5. Scheme of "fusion-synthesis" fusion devices

Artificial and non-tropical artefacts are used to excite the splitting chain reaction at the exact time to increase the number of concurrent starting divisions.

The fission-synthesis fusion charges (Figure 5) have in their composition a nuclear charge of fission and fusion fuel, lithium deuteride (a chemical compound of deuterium with the isotope of

lithium-lithium-6), and in the case of the detonation of such charges the third is obtained directly in the blast process (when neutrons affect lithium-6).

The power of fusion charges depends on the amount of deuterium and tritium and practically is unlimited.

For warfare, depending on their purpose, the nuclear charges are placed in one or the other bundle and supplied with the explosive device to provide a blast at a specific time or at a specific height.

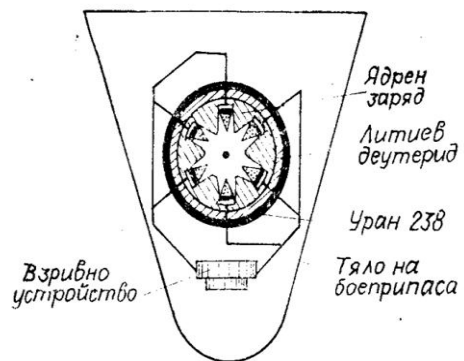


Fig. 6. (schematic diagram of a combo-fusion device of the "division-synthesis-division"

Nuclear munitions are called nuclear and fusion missile heads (missiles) of rockets of various types and purposes, aviation bombs, torpedoes, underwater bombs, artillery shells, and special nuclear mines.

The power of nuclear munitions is characterized by the trolley equivalent b, ie by the weight of the trotyl charge, the explosive energy of which is equal to the energy of the nuclear charge explosion.

Current nuclear charges may range from several tons to hundreds of millions of tons.

Depending on the power, nuclear munitions are widely divided into the following caliber:

- overweight - less than 1000 (1 kiloton) t,
- small - from 1000 to 10 000 t inclusive,
- an average of 10 000 to 100 000 tonnes inclusive,
- Large - from 100,000 to 1 mil. t including,
- at a rate of more than 1 ml. t.

The nuclear explosion is accompanied by the formation of a shining area, a source of intense light radiation. Gamma rays and neutrons emitted during the partition reaction process generate a penetrating radiation stream. From the center of the blast in all directions spreads a spherical zone of sudden compression to the air, called the shock wave. In addition, a large amount of radioactive material is created in the nuclear explosion, creating radioactive contamination of the locality and objects.

Shockwave, light radiation, penetrating radiation, and radioactive contamination are major emerging factors of the nuclear explosion.

The electromagnetic impulse that occurs at the moment of the explosion in the surrounding space is also related to the striking fac

3. Conclusions:

1. Nuclear Weapons would reach the destruction of hundreds of planets like our Earth;
2. The presence of a nuclear weapon has a more deterrent effect on opponents than it would be in real use;
3. The development of nuclear weapons must be under control and the military-industrial complexes must not be uncontrollable. The control bodies must also be public and accountable to society to reduce the amount of space for weapons;
4. The use of nuclear weapons would be detrimental to the inhabitants of the Earth and terrorist organizations should not have access to such weapons.

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, ISJ Security & future, №1/2017;
3. Статев Ст., Радиационна физика, изд. ПИК, В. Търново, 1997;
4. Постановления и решения на МС на Република България, София,

MAIN ASPECTS OF THE ECOLOGICAL POLICY OF THE EUROPEAN UNION AND ENERGY RESOURCES IN BULGARIA

Assoc.prof. Galina Todorova, PhD

Aviation Faculty, National Military University, Bulgaria

galibs@abv.bg

Abstract: *European environmental policy faces major challenges arising from the interaction between public production and nature. The challenge for us, today's people, is to create material goods without disturbing eco-equilibrium. The main reasons for the emergence of environmental policy is conditioned by objective factors, the most important of which are: climate change, resource depletion in the face of rising global energy needs, price level dynamics, problems and environmental damage from the development of the classical technologies. One of the possible solutions to this problem is the application of new sources of energy, such as renewable energy sources.*

Keywords: ECOLOGY, NATURAL RESOURCES, EUROPEAN POLICY, ECONOMY, DEVELOPMENT STRATEGY

European ecological policy faces major challenges arising from the interaction between people's modern lifestyles, public production and the continuous pollution of nature from various sources. The biggest cause of pollution is production in all its aspects. It takes place on a global scale, has a devastating impact on nature, and so the environmental problem is born. According to G. Mateev and Iv. Pavlov "modern ecology also intensively studies the problems of human interaction and the biosphere. Today ecology in biological terms is understood as a science of the environment and causal relationships. "[1] A wider interpretation in this direction is made by RA Novikov and AK Khiritsky [2], who conclude that the contradiction "Man - society - nature" acquires a global character. The result of this contradiction is also the environmental problems associated with the formation of the ozone hole, acid rain, greenhouse effect, radioactivity and others. Therefore, the challenge for us, today's people, is to create material goods without disturbing eco-equilibrium. The main reasons for the emergence of environmental policy are: climate change, depletion of resources against the backdrop of rising energy needs, the dynamics of price levels of energy resources, problems and environmental damage from the development of classical technologies.

In our opinion, one of the reasons of the ecological problem is the development of the economies of the individual countries, the constant pursuit of raising the living standards of the people, and this inevitably leads to an increase of the harmful environmental factors. By nature, this phenomenon is complicated and requires a deep and comprehensive scientific understanding, but not only at national and European scale. It was not a coincidence that European and environmental policy was created. Its main framework is formed by the following guidelines and documents [3]:

- ✓ **Environmental Action Programs** - in 2013 The Council and the Parliament of Europe adopted the Seventh EU Environment Action Program for 2020, entitled "Prosperity within our planet." Building on several recent strategic initiatives (the Resource Efficiency Roadmap, the Biodiversity Strategy for 2020 and the Roadmap for moving to a competitive low carbon economy by 2050), it sets nine priority objectives and the most important ones are: nature conservation, greater environmental sustainability, sustainable resource-efficient and low-carbon growth, and the fight against environmental risks to health. The program also highlights the need for better implementation of EU environmental law, the latest scientific achievements, investment and the integration of environmental aspects into other policies.
- ✓ **Horizontal strategy** - this is the EU's most recent strategy for smart, sustainable and inclusive growth "Europe 2020", which is a priority for the development of the RES sector. Its promotion is based on the cost-effectiveness principle of EU co-funded programs for specific projects to increase European added value. The Cohesion Fund for RES 2007 - 2013 is from two sources -

the European Regional Development Fund and the Cohesion Fund.

- ✓ **Environmental impact assessment and public participation** - the basis for such an assessment was the Aarhus Convention. It was signed in 1998 by the EU under the aegis of the United Nations Economic Commission for Europe (UNECE) and later ratified by it.

According to the Convention, "Public Participation in Decision-Making" [4] is one of the three environmental rights that are guaranteed to the public. Other two rights are : the right of access to environmental information available to public authorities (for example on the state of the environment or human health if affected by the state of the environment) and the right of access to justice when the other two rights were not respected.

- ✓ **International cooperation on the environment** - maintains partnership agreements in the EU and cooperation strategies with a number of countries and regions. Such is, for example, the European Neighborhood Policy (with the Eastern and Mediterranean countries). It is used as a means of solving problems occurring at the external borders of the EU, incl. related to the environment - water quality, waste management, air pollution.

Environmental policy and efforts to combat climate change are becoming increasingly important both in terms of energy to reduce greenhouse gas emissions and to place greater environmental responsibility on companies without compromises their competitiveness. The basic principles on which it is based, according to UNESCO's normative documents, are the following [5]:

- Environmental protection and reproduction is a continuous, timeless process. It is complemented and enriched at every stage of the development of society;
- environmental policy is a strategic direction in the general policy of the state;
- environmental protection and reproduction takes place in a variety of forms of ownership;
- Conservation measures are complex in nature, using the latest advances in science and technology;
- environmental policy uses for its purposes modern monitoring and information systems;
- Environmental policy is the result of international cooperation in the field of environmental protection.

Our conviction is that the implementation of the European energy policy in relation to the wider use of renewable energy sources (RES) or so-called "green energy" which according to the European legislation is:

- Geothermal energy.
- Wind energy.
- Solar energy.

- Biofuels.
- Co-generators.

By their very nature, RES is a resource for the production of material goods from natural sources such as sun, wind, water and natural waste, which carry the source directly into the energy system product. They are multifunctional and are used both for commercial production and for the individual household. The main purpose of the RES sector is the production of non-traditional energy, whose main feature is the resilience of resources, guaranteeing the country's security and reducing dependency and import.

In ZEWE [10], the same term is also defined as "production sites" for electricity, heat and cooling. The authors Bliznakov, Z. Gargarov and N. Marinova define as renewable "these resources, whose current scales can be sustained or even increased, despite the constant or even growing consumption. These are resources that are either virtually inexhaustible (sun, water, air) or biologically reproducible (forests, game, plants)" [11]. For other authors, "RES are existing environmental energy flows and have a continuous and recurring character." [12] That is to say the renewable energy sources are indigenous inexhaustible resources and are a priority of national energy policy. Our belief that more massive use will make it possible to tackle most of the existing environmental problems for the countries of the European Union, and that will certainly lead to better sustainability and stability for European economies as well.

In this regard, the main ecological problems in our country can be identified:

- Air pollution by increased emissions of sulfur dioxide, nitrogen dioxide and dust, the largest source of these harmful substances being energy production [6]. According to a Eurobarometer survey conducted in the member states of the European Union, "61% of Bulgarian citizens are of the opinion that the air quality in the country has deteriorated over the last 10 years" [7]. By air quality, our country ranks at an average level in the European Union.
- Poor waste management. In the structure of generation of industrial waste, the largest share belongs to the TPP and the chemical industry.
- Industrial pollution, due to the lack of compliance with environmental requirements years ago in the construction of a large part of the enterprises.
- Other environmental problems are soil pollution, erosion, weathering and the urban environment.
- They all have a negative impact on human health. These problems are difficult for us to solve, because at present, the EU economy, including Bulgaria, is still heavily dependent on fossil raw materials and fuel imports, but this tendency is expected to change in the coming years because: "The EU is a leader in renewable energy technologies. It holds 40% of the world's renewable energy patents and in 2012 almost half (44%) of the world's renewable energy production capacity (excluding hydroelectric power) is located in the EU. The EU's renewable energy sector currently employs around 1.2 million people." [8] Evidence of positive changes is the increase in the share of renewable energy in gross final energy consumption. According to Eurostat [9], renewable energy production in the EU is based primarily on biomass (46%) and water (16%), but also on renewable sources such as solar and wind power. In this regard, the most important conclusions are:
- The use of inexhaustible energy in the environment is necessary to provide mankind with energy while preserving the ecological equilibrium of the earth.
- Renewable energy mainly focuses on local stocks. Bulgaria has all the necessary natural resources and can develop this type of industry that enables local economic, social and infrastructure problems to be solved, increases energy regions, creates new

high-tech productions and jobs. In this regard, the most important conclusions are:

- The use of inexhaustible energy in the environment is necessary to provide mankind with energy while preserving the ecological equilibrium of the earth.
- Renewable energy mainly focuses on local stocks. Bulgaria has all the necessary natural resources and can develop this type of industry that enables local economic, social and infrastructure problems to be solved, increases energy regions, creates new high-tech productions and jobs.
- The European path of Bulgarian energy is closely related to renewable energy, which is defined as a complementary energy. Our country is implementing the EU 20/20/20 Program, which foresees a 20% reduction in carbon production by 2020, 20% of the electricity produced from renewable energy sources and eco-technologies.
- The legislative regulatory framework is a basic prerequisite for the development of RES. Its disadvantage is frequent changes, which are a prerequisite for destabilizing the sector. The recommendations on the improvement of the regulatory framework are mainly focused on SEWRC and ASWER and generally refer to: : reducing unnecessary bureaucratic procedures; improving independence; strengthening powers and responsibilities and cooperation with foreign regulators at European level.
- The aggressive policy of intensive sector development has led to the fulfillment of the national mandatory target of a 16% share of renewable energy (RES) in gross final energy consumption by 2020 by 2020. State protectionism linked to with compulsory purchase of energy from NEK at preferential prices, has created a number of problems such as the burgeoning construction of new capacities, a lack of a clear concept of transmission and distribution networks, a lack of vision of how and where construction should be restricted. Additional problems have arisen in the management of the electricity system, at the prices for the end user, in the substations' capacities, in the distribution of costs in the system, which negatively affects the competitiveness of the economy

We believe that European policy to support the deployment of renewable energy sources, despite rapid pace of development, will continue to be a necessary and still long process, will continue to be necessary and still a long process as there is no competitive internal energy market in the EU. EU governments need to work to phase out harmful and inefficient subsidies for fossil fuels that encourage excessive consumption and harm the environment.

The pace of economic development on a global and national scale and the dynamics of growing consumer awareness of clean technologies and energy will continually increase.

The reasons for this are: global trends for wider application of clean and renewable sources, the ever-decreasing global and national reserves of non-renewable resources as well as significant political support and increasing subsidies in this area, and the benefits to the public are indisputable!

Literature:

1. Mateev G., Pavlov, Iv. Ecology Sirius 4 V. Tarnovo 1993
2. Novikov, R., Zhiritsky, A., Marcushina, V., Global Ecological Problem. Москва «Мисль», 1988
3. Environmental policy: general principles and basic framework. <http://www.europarl.europa.eu/aboutparliament/en>
4. Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters <http://www3.moev.government.bg/files/file/KVESMS/>
5. UNESCO, Teaching global change through environmental education Connect, 1993, No1.

6. Deneva, A., Sirashki G. et al. Problems of Energy Development - Renewable Energy Sources, Svishtov, 2011.
7. Over 60% of Bulgarians feel a deterioration in air quality
<http://www.klassa.bg/news/Read/article>
8. Renewable energy
http://www.europarl.europa.eu/aboutparliament/en/displayFtu.html?ftuId=FTU_5.7.4.html
9. Changing the future of energy: civil society as a major player in renewable energy generation - FINAL REPORT, (January 2015).
10. LAW ON RENEWABLE ENERGY. - SG, No. 35 of 03.05.2011
11. Bliznakov, A., Gargarov, H., Marinova, N., "Ecology and Economics, Economics and Ecology (Unity or Incompatibility)", NBU, Sofia, 2012
12. Antonova, D., Mihaylov, N., Andonov K., et al. Renewable energy sources. Russia 2012

INNOVATIVE INVESTIGATIONS OF THE CRIME SCENE USING 3D SCANNERS

Prof. Wieczorek T., PhD., DSc

Department of Industrial Informatics – Silesian University of Technology, Poland
tadeusz.wieczorek@polsl.pl

Abstract: Innovative solutions that can be applied in contemporary forensic science, including the examination of the place of the incident or crime, are still being sought. One of them is the preservation of evidence by means of 3D scanners. In Europe, 3D scanners have got, among others, Police services of the following countries: Switzerland, Germany, France, Spain and Italy. In the paper, the results of research on the preservation of the crime scene using 3D scanning techniques have been presented. The research used Creaform hand scanners, both laser and structural light, Smarttech3D portable 1.3MPix, a scanner on the measuring arm - FARO Laser ScanArm AND TERRESTIAL scanners (Faro, Leica, Z + F). The accuracy and precision of scanners were carried out on a certified measurement pattern. The obtained accuracy results for the tested scanners are within the accuracy range given by the manufacturers in the technical specifications of the devices. To examine the scanners' resolution, an object with a complicated shape and many small elements was used. It was examined how the tested scanners behave when attempting to scan surfaces generally considered as hard to scan surfaces. Attempts have also been made to use a 3D structural light scanner to scan snow tracks. The possibilities of combining scans from a portable scanner (Go! SCAN50, Smarttech) and a scanner on a measuring arm (Faro), with scans obtained from long-range were examined. It has been found that it is possible to supplement clouds of points acquired in 3D scanning technology with photos from digital cameras, detailed scans of selected traces and precise geographical locations.

Keywords: 3D SCANNING, CRIME SCENE, LASER SCANNERS, STRUCTURED-LIGHT SCANNERS

1. Introduction

Preservation of the crime scene and the discovered forensic evidence is the first and very important stage in the investigation process. It is important to document the crime scene, possibly without any changes, so that it is a reliable material in further investigations, reconstructions or trial experiments. The results of the Research Project, implemented by the authors as part of the "Polish State Security and Defense Research Program", have allowed the development of innovative solutions supporting the preservation of the crime scene and the detection process based on evidence recorded using 3D scanning techniques. The developed methodology assumes that both the terrestrial and portable scanners will be used at the crime scene (terrestrial scanners to scan the entire scene of the event, usually often hundreds of meters in size). The presented article discusses only chosen test results.

The world is constantly looking for modern solutions that can be applied in contemporary forensic science, including the examination of the crime scene. 3D scanning technology is such a solution. The most common 3D scanning techniques are used by the US police services, primarily in the forensic examination of traffic incidents and on the spot of the most serious criminal events, most often with the use of weapons. In Europe, 3D scanners have, among others, Police services of the following countries: Switzerland, Germany, the Netherlands, Luxemburg, Italy, and Spain. Danish and British Polices assume that in the near future they will introduce 3D scanning into routine forensic work. Currently, the Police use the help of external companies in the field of 3D scanning, handling complex and extensive incident scenes. In Poland, so-far, 3D scanning technology applied to the investigation of the crime scene has been used only incidentally. The main goal of the research and development project carried out by the authors, was the implementation of 3D scanning for the Police practice.

2. Testing portable 3D scanners

The research used Creaform [Creaform 2017] portable scanners, both laser (HandyScan, MetraScan), KonicaMinolta Range 7 and structured-light (Go!Scan), Smarttech3D, and a scanner on the measuring arm - FARO Laser ScanArm.

2.1 Testing scanners' precision

The accuracy test was carried out on a certified measurement pattern (determined with an accuracy of one micrometer). Due to the fact that scanners use different methods of positioning, the measured pattern was placed on a specially prepared pad with markers (Fig.1). Thanks to this solution, each of the scanners will be able to position themselves appropriately and the obtained results

can be compared with each other. The diameter of the bullets is 38.107 mm (left ball) and 38.111 mm (right ball). In addition, the distance between the ball centers, which is 648.413 mm, was determined. Each scanner was tested with 6 pattern scans each time placing them in a different position on the pad. Measurements on scans were made using the manufacturer's software - VXelements.



Fig. 1 The pattern for testing scanners' precision.

The results of the measurements are presented in the table 1. For each measurement, precision was determined and the average value was calculated.

Table 1: Results of portable scanners' precision testing [CaspSystem 2016]

Scanner type	Handy SCAN	Metra SCAN210	Go!Scan50
Average value - left ball [mm]	38,117	38,159	38,159
Average error - left ball [μm]	19	52	52
Average value - right ball [mm]	38,110	38,156	38,147
Average error - right ball [μm]	23	45	36
Average value - between balls [mm]	648,371	648,512	648,621
Average error - between balls [μm]	49	107	322
Average scanner's precision [μm]	30	68	137

2.2 Testing scanners' resolution

To examine the scanners' resolution, an object with a complicated shape and many small elements was used. Thanks to the use of such model, it was possible to check the accuracy of grid mapping. During the examination, the object was scanned four

times each time with different resolution of: 0.5mm; 1.0mm; 1.5mm; 2.0mm.

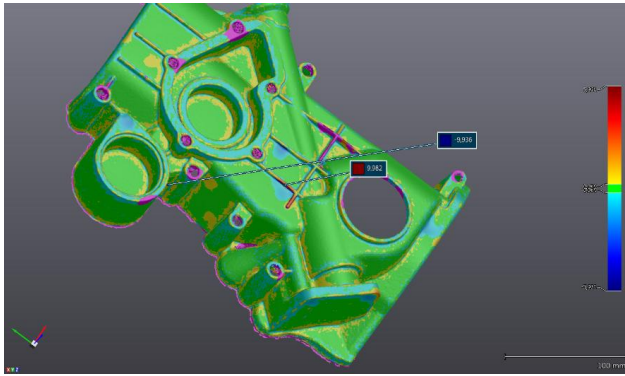


Fig. 2 The map of deviations compared models scanned with 0,5 and 2mm.

The change in scanning resolution for all examined scanners achieved similar effects. In the case of scans made with high resolution, the model had more clearly visible edges and better mapped smaller elements. In the case of smaller resolutions, however, the scans were smoother, and in some cases the reproduction of small elements was impossible. The figure 2 shows a colorful map of deviations resulting from a comparison of averaged models scanned with a resolution of 0.5mm and 2.0mm (green color, practically no errors). The maximum errors are marked in the figure (blue color negative deviation, red positive). The biggest deviations can be observed at the edges of the model. Certain fragments (purple) are off the scale. They represent fragments that could not be measured at all, while scanning at a resolution of 2mm.

Another aspect of resolution changing is the scan time and the size of the resulting scan files. Higher resolution scans have a larger number of triangles. Please note that the mesh of the tested element (about 240x320x80mm) when scanning with a resolution of 0.5mm has got more than 800,000 triangles. The highest resolution, this number can reach tens of millions, which of course also affects the scanning time, strongly enlarging it. That's why, it is so important to find the right compromise between the resolutions, the size of the files and the time of scanning.

2.3 Scanning of different surfaces

The tested portable scanners are based on optical systems, therefore the optical parameters of the object being scanned are very important to them. In order for the scanners to be able to correctly acquire the data, the light beam displayed by them (whether it be a laser beam or a structural pattern) must be properly visible on the scanned surface. Therefore, surfaces that are highly reflective, transparent, strongly absorbing light or causing its dissipation are difficult materials to scan.

The tests were carried out on six samples of materials. It was a black polyurethane foam, a piece of fabric with a weave, a nickel element with a high degree of reflexivity, an acrylic glass plate, a steel plate and a white sponge with a small bubble structure filled with air.

Surfaces with high reflectivity are very difficult for 3D scanners. They cause so-called mirror effect. To investigate this effect, a polished nickel-plated component and a steel plate were used. Both the laser scanner and the structural light scanner had very big problems with scanning the nickel element (fig.3). The correct surface could not be scanned. As a result, an uneven and jagged surface was obtained. The solution to the problem with scanning highly reflective surfaces may be the use of surface matting powders. But in the case of crime scene, the method cannot be used because of traces contamination. Similar materials with a high reflectivity (steel plate) were tested. For such elements, both laser scanners and structural light were able to create a very good surface model.

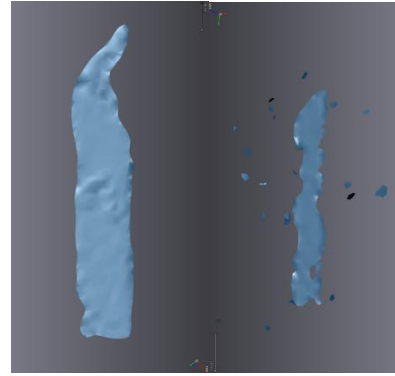


Fig. 3 Results of a nickel element scanning: laser and structured-light scanners.

Attempts have also been made to use a 3D structured-light scanner to scan snow tracks [Smarttech 2017]. The MICRON3Dgreen 10Mpix scanner, manufactured by Smarttech3D, with the accuracy of 0.041mm was used for the measurements. Six scans of the snow track were carried out, moving the scanner around the object being scanned. The resulted cloud of points has been transformed into a grid of triangles, becoming the model of the tested track. In order to confirm the high accuracy of the scan, a computer model of the shoe was made, and then both models were compared. The results are presented in a colorful deviation map (Fig.4). The green color means a practical lack of errors, which is fulfilled for almost the entire print.

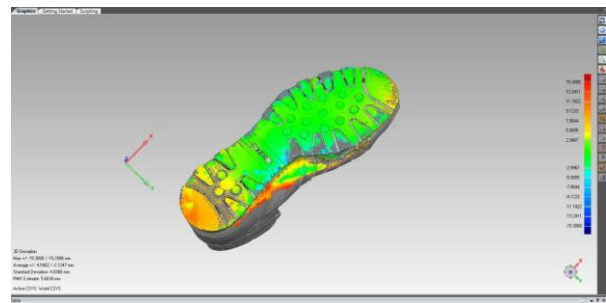


Fig. 4 Results of a shoe print in snow scanning - a map of deviations (source [Smarttech 2017]).

Transparent materials are virtually invisible for scanners. If the pattern emitted by the scanner is not reflected and the registered creation of the model is impossible. This is exactly what happens with all transparent materials, i.e. glass or plexiglass. The transparent surface was not registered for both the laser scanner and the structured-light scanner (fig.5). On the other hand, the effects of light passing through the transparent plate are visible. The edges of the scanned plate are clearly visible. The scanners captured all the elements of the environment, i.e. the base with markers, on which the plate was placed and the protective foil glued on the bottom of the half of the plate.

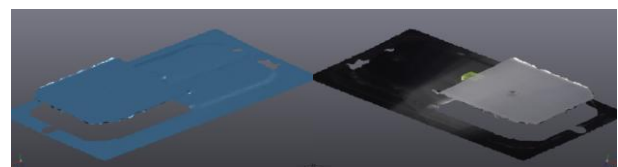


Fig. 5 Results of a plexiglass element scanning: structured-light and laser scanners.

A sample, which absorbed light very much, was a white sponge made of bubbles filled with air. The structure of this material causes very strong penetration of the light inside without the possibility of leaving it. In addition, the white color makes it difficult to recognize the pattern especially for structured-light scanners, due to the very low contrast between the pattern and the surface. In the case of laser

scanners, the result is correct, whereas the structured light scanner had problems with surface acquisition. The structure of the material caused a very large loss of pattern visibility on the scanned surface. The obtained surface had discontinuities (fig.6).

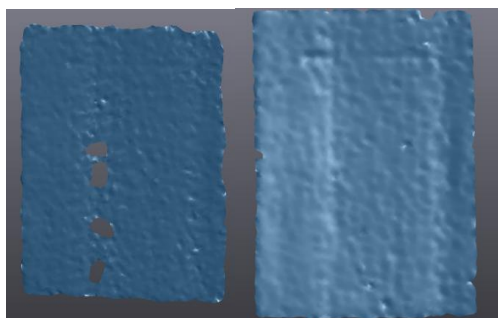


Fig. 6 Results of scanning of a white sponge made of bubbles filled with air: structured-light and laser scanners.

3. Testing terrestrial scanners accuracy

An important issue is to determine the distance between two selected points on the scan (e.g. the position of the object and the assumed reference point of measurements in the scene). The precision of determining the distance consists of two factors - the first is the precision of the scanner itself, the second is the precision of pointing of the measuring points on the scan. Accuracy tests of measurements making on the scan were carried out for scanners: Faro, Trimble, Z + F, Leica. Many testing measurements have been taken on different scans made either inside buildings, like at the simulated "scene of crime" - fig.7 or outside. In tab. 2 example results have been presented.



Fig. 7 Simulated "scene of crime" for scanners accuracy testing.

To test the accuracy of measurements on 3D scans a series of measurements was made on the real scene (for long distances with accuracy ± 1 cm, for small elements ± 1 mm), and then the same measurements were made on 3D scans. Considering accuracy of measurements taken on scans we should notice that the data acquired by the scanners are useless unless they are processed using specialized software (we tested Faro Scene, Leica Cyclone, Z+F Laser Control).

Table 2: Results of terrestrial scanners' precision testing

Description	RD [mm]	DMS [mm]
Left drawer handle – left leg of the chair	2270	2286
Washing machine-cabinet: corner-corner	195	198
Corner to corner of higher cupboards	2875	2860
Floor – top of the wall cabinet	1999	1961
Width of the beam	135	137
Table in the room	500x1500	498x1488
Heel - the corner of the table	960	911

Drawer handle – cupboard's top corner	7085	7098
Thickness of the table top	18	20
The width of the door	940	949
Lath-threshold	1955	1952
The width of the lamp	1265	1249

RD – real distance; DMS – distance measured on the scan

Some of obtained errors could be considered as too big (i.e. 16 – 38 mm). But the problem was to properly determine equivalent point in the scan e.g.: drawer handle – reflective, shining surface, corner of cabinets - overlapping edges in the scan, rounded edges of the washing machine, lamp housings made of transparent plastic etc. The most important causes of errors and difficulties occurring while dimensioning objects on the scan:

- surfaces difficult to scan (e.g. reflective),
- carefully choose the perspective to mark the measurement point because often the edges overlap,
- for small objects (e.g. table top thickness) problems occur due to the scanner's resolution (at a further distance from the scanner the resolution is a few mm),
- errors done by measurements in the real scene.

Accuracy of measurements taken on the scan strongly dependent on the software and an operator's skills. Z+F Laser Control software supports distance measurements by introducing the so-called "spatial grabs", i.e. characteristic elements - planes, edges and corners, so that the measurement is better suited to the characteristics of the object being measured. This solution is very useful, because it allows to reduce the error resulting from the imprecise indication of the measurement point.

4. Integration of 3D models

An important aspect for the documentation of the crime scene is the integration of data from various types of devices. It is possible to supplement the cloud of points obtained in the technology of scanning 3D by photos from digital cameras, detailed scans of selected traces and precise geographical locations. Therefore, the possibilities of combining scans from a portable scanner (Go! SCAN50, SmartTech) and a scanner on a measuring arm (Faro) with scans obtained from terrestrial scanners (Faro, Leica, Z + F) were tested. Attempts to integrate scans were carried out using the following programs: VXelements - Go! SCAN scanner software, SCENE - Focus 3D X130 scanner software, Leica Cyclone - P40 scanner software, 3D Systems Geomagic Design X, CloudCompare (Open Source Project). Each of the tested software has various possibilities of importing and exporting files in given formats. Terrestrial scanners operate on point clouds, while portable scanners (in particular the Go! SCAN scanner and measuring arm scanner), as a result of the scan, immediately generate a grid of triangles. In all cases, therefore, format conversions were carried out. All scans were made in one room in similar time intervals and the individual elements of the scene are in the same position in relation to each other on each of the scans performed. The study locations were simulated crime scenes with many key elements. Using terrestrial scanners, a general overview of the scene was made, and scans of key elements of the scene of traces discovered at the scene were made using portable scanners. In all attempts, the resulting files have a total size of GB and work with them is extremely time-consuming and cumbersome, requiring the highest-class computer equipment. For example, in the case of a simulated crime scene with 7 detailed evidences, the editing of the joint model was possible only on a computer with an i7, 2.6GHz processor and with 16GB RAM memory. That is why the Project was proposed as final solution to create a full documentation of the crime scene in the form of a set of files, linked together with hyperlinks. Since all native programs of the examined scanners allow to attach a label and assign a link to an external file or application, the resulting set can be protected as a whole (folder).

Preparation of documentation of the crime scene (in the form of a set of files) using 3D scanning requires adaptation of the methodology to secure the integrity of the registered space to current Police standards [Wieczorek T. at all. 2017]. Applicable standards include the need to calculate checksums (hash functions) of data recorded at the scene (results of the process of image or sound recording for process purposes) and attach them in the form of a certificate to a record prepared for each medium on which the image was registered. The certificate must be made obligatorily and the check sums should be calculated and attached to the record. The following applications were tested, mainly in terms of their functions and capabilities: SHA256 Checksum Calculator, #hashing, HashTab, HashMyFiles, Febooti fileTweak Hash & CRC, WinMD5Free, Microsoft File Checksum Integrity Verifier, HashCalc, Md5sum, ComputeHash 2.0, MD5 & SHA-1 Checksum Utility 1.1, File checksum integrity verifier, Md5 checker 0.9, Checksum control 2.0, MultiHasher. In the course of the research, it was found that only the application SHA256 checksum calculator v.1.2 meets the main criteria set (in particular the criterion of the ability to calculate checksums for many files at once). Therefore, the program was selected for further testing. Next, the software license of the program was analyzed, in terms of the possibility of its use to secure the integrity of the documentation of the crime scene inspection. It was stated that the license terms of the program allow its use in order to safeguard the integrity of the documentation of the crime scene. Finally, as the suggested application to secure the integrity of the inspection documentation of the crime scene, the application "SHA256 checksum calculator v.1.2" is indicated. This application has met all the requirements. The results of the research have allowed the development of a methodology in the application of methods of securing the documentation of the crime scene in investigative practice. This methodology is currently being tested under real conditions of crimes and road accidents.

5. Summary

Analysis of devices for spatial scanning in the form of commercially available systems was carried out. An analysis was also carried out in the field of forensic technology used in the world in investigating of crime scenes, stating that in many EU and other countries 3D scans are used by the Police of these countries, also to inspect the crime scenes and places of incidents.

It was stated that the precision of devices declared by manufacturers corresponds to the requirements set in the project (i.e. for long-range scanners: 3 mm for 50 m and 6 mm for 100 meters, and 35 µm for the scanning head mounted on the measuring arm) - [Wieczorek T. and Górawska A. 2017]. The use of the measuring arm is associated with numerous limitations regarding the scanning conditions, and the precision of the measuring arm itself used for positioning the scanning head. The work of the measuring arm can easily be disturbed (in experiments in the case of an unstable floor there are disturbances resulting from the trembling of the floor caused by cars passing the nearby street), which means that they can only be used in laboratory conditions.

Series of 3D measurements were made using various 3D scanners in terms of construction and technology. Terrestrial 3D scanners, portable scanners with dynamic positioning in relation to the scanned object and measuring arms with 3D scanning heads were tested. The tests carried out in laboratory conditions allowed to check devices using various 3D scanning techniques and various techniques of light projection and scanner positioning. Further tests were carried out at measurement stations that mapped real conditions. These tests were aimed at determining the limitations of the use of individual devices in real conditions. Both in laboratory measurements and measuring in conditions close to real, accuracy measurements and analysis of the influence of changing environmental conditions on measurement accuracy. For this were used measurement patterns and markers provided by equipment manufacturers. The conducted research allowed to select devices that meet certain technical parameters and to determine the functional properties of these devices, which will affect their

functionality during the inspection of the crime scene. As a result of the research, a technology for performing spatial scans, their processing, combining and matching was developed, taking into account the diversity of devices used.

In the investigative practice of the methods of securing the documentation of the inspection of the crime scene, it is necessary to calculate checksums for "each file included in the record" and attach them to the media record. During the research, the procedure of securing the documentation (using a 3D scanner) of the inspection of the crime scene was carried out. The procedure presents step by step how to calculate checksums (using program SHA256) for a 3D scanner result files and finally execute and attach the checksum printout to the media record.

6. References

1. Casp System: Badania dotyczące określenia parametrów i charakterystyk skaningu 3D w zastosowaniu do zinventoryzowania miejsca zdarzenia – skanery ręczne. Raport z badań, Casp System, 2016 mat. niepubl.
2. Creaform: <http://www.creaform3d.com/en> (31.08.2017)
3. SmartTech: Możliwości wykorzystania skenera 3d do skanowania śladów w śniegu, raport z badań. <http://skaner3d.pl/wp-content/uploads/2017/04/SMARTTECH> (31.08.2017)
4. Wieczorek T., Górawska A.: Portable 3d scanners for crime scene investigations. *Studia Informatica*, vol.8, no.3, 2017, 132-141.
5. Wieczorek T., Zubańska M., Wiciak K., Szymczak M.: Techniczne i prawne aspekty oględzin miejsca zdarzenia z wykorzystaniem skaningu 3D. [In] *Przestępczość teleinformatyczna*, pr. zb. pod. red. J. Kosińskiego. Wydawnictwo Wyższej Szkoły Policji w Szczytnie, 2015.

TYPES OF BULLETPROOF VEST. CLASSIFICATION

Assist. Prof. Eng. Yaneva S. PhD¹, Assist. Prof. Eng. Tumbarska A. PhD², Prof. Eng. Petkov S. PhD³
 Technical University of Sofia¹, IMSETHAC-BAS-Sofia^{2,3}
 svetlana_ianeva@tu-sofia.bg

Abstract: This report proposes a classification of the bulletproof vest according to various features, which is based on a study and analysis of modern threats and the use of vest by military, police and other units. This classification would allow for a quick, easy, adequate and reasoned choice of the appropriate vest kind and type depending on the tasks and the environment of operation.

Key words: BULLETPROOF VEST, CLASSIFICATION, CLASSIFICATION SIGNS, LEVEL OF PROTECTION, STANDARDS

1. Introduction

Modern multi-component bulletproof vests are an important and indispensable element of the equipment of the officers of various types of forces. Different types and purpose bulletproof vests exist. Recently, modular type vests are becoming more and more relevant, which can be transformed depending on the task being performed and the degree of risk. To the main part of the armor (back and chest securing section providing full torso protection at the front and rear), additional safety components in the form of separate modules can be attached to protect the side parts of the torso, shoulders, neck, and the loins. Bulletproof vests play an important role in preserving the health and life of anti-terrorists in fulfilling their duties and resolving crisis arising in various critical situations.

2. Classification of bulletproof vests

The study carried out on the state of the art of the bulletproof vests available at the market and the vests used by anti-terrorists found the existence of a wide variety of models produced by both Bulgarian and foreign companies [1, 2, 3, 4, 5, 6].

Based on the analysis of the results obtained from the study, a classification of the bulletproof vests can be suggested according to the following features:

- in terms of purpose;
- by the levels of protection;
- by the way of wearing;
- by gender of the individual carrying it;
- by the protective panels materials.

➤ CLASSIFICATION BY PURPOSE

Depending on their intended use, the bulletproof vests can be assigned to one of the following groups:

- Military;
- Police;
- Civil.

Military bulletproof vests can be divided into:

- Tactical;
- Special;
- Water inflatable.

Tactical vests provide ballistic protection to the front, rear and side parts of the torso. Lateral overlap of ballistic panels ensures complete torso coverage. These bulletproof vests are comfortable to carry, allow free movement of the hands and do not restrict the movement when squatting. They are designed for use in various tactical actions. Typically, the outer case is made of a masking cloth that matches the terrain in which it will be used. Most often the spots are in the so-called desert variant or in the shades of green colors. These bulletproof vests are mainly with protection classes IIIA, III under NIJ and levels 4 and 5 under GOST.

Specials vests provide ballistic protection for the front, rear and side parts of the torso, as well as protection for the neck, throat, shoulders, biceps and loins. They are mainly used for patrolling. The outer case is made of a masking cloth depending on the terrain in which it will be used [7]. Most often the spots are in the so-called desert variant or in the shades of green colors. These bulletproof vests are mainly with protection classes III and IV under NIJ and levels 6 and 6a under GOST.

Water inflatable vests provide ballistic protection to the front, rear and side parts of the torso as well as to the neck. The collar of the vest is inflatable and through it the body of the fighter is kept on the surface of the water. This type of bulletproof vests has extra belts that ensure safer grip on the body in buoyancy conditions. These vests are mainly used by special and anti-terrorist forces. The outer case of the vests is made in a signal color or in the color of the uniform. These bulletproof vests are mainly with protection levels IIIA, III under NIJ and levels 4 and 5 under GOST.

Police bulletproof vests can be divided into:

- Tactical;
- Special.

Tactical vests provide ballistic protection to the torso's front, back and sides to ensure full torso coverage. The protection of the torso side portions is ensured by the lateral overlapping of the ballistic panels. This type of bulletproof vests is comfortable to wear throughout the day, providing freedom of movement for the hands and feet while walking, running and squatting. They are intended for use in various operations. The outer case is made in black. These bulletproof vests are mainly with protection levels IIIA, III under NIJ and levels 4 and 5 under GOST.

Specials vests provide ballistic protection for the front, rear side of the torso, as well as protection for the neck, throat, shoulders, biceps and loins. They are mainly used in patrolling. The outer case is made in black. This type of bulletproof vests is mainly with protection levels III and IV under NIJ and levels 6 and 6a under GOST.

Civil bulletproof vests can be divided into:

- Ordinary;
- VIP.

Ordinary vests provide ballistic protection to the front and rear of the torso. They are used by security guards and civilians. They are light and comfortable for long wearing and can be placed above and below the clothes. These bulletproof vests are mainly with protection levels I, II under NIJ and levels 1, 2 and 3 under GOST.

VIP bulletproof vests provide ballistic protection for the front and rear of the torso. They are mainly used by businessmen and high-ranking persons. They are lightweight and comfortable to wear for a long time. They usually wear under clothes and are not noticeable. These bulletproof vests are mainly with protection levels I, II under NIJ and levels 1, 2 and 3 under GOST.

➤ CLASSIFICATION BY PROTECTION LEVEL

The protective qualities of the bulletproof vests are determined depending on the level of protection provided by them, in accordance with the requirements of existing standardization documents [8, 9, 10, 11, 12, 13, 14, 15, 16]. The latter are prepared in accordance with a number of regulatory requirements for individual ballistic protection means, environmental conditions, the degree of risk in specific structures, and weapons used in the region.

Some of the most widely used worldwide standardization documents on ballistic resistance of bulletproof vests are the standards of: US National Institute of Justice - NIJ 0101.04 and NIJ0101.06; National Standard of Russia - GOST 50744-95; German - German Schutzklassen and VPAM; as well as those of the UK Police - PSDB and HOSDB.

As regards the bulletproof vests resistance to puncture, these are: the US National Institute of Justice - NIJ 0115.00 and the United Kingdom Police Standard - HOSDB 2007. Part 3.

Table 1 shows equivalent ballistic protection levels, and Table 2 - equivalent puncture protection levels, specified in some of the most commonly used standards for bulletproof vests.

Table 1. Equivalent ballistic protection levels

Ballistic protection level according to some of the leading standards in this field		
GOST 50744-95 (Russia)	NIJ 0101.04 NIJ0101.06 (USA)	German Schutzklassen (Germany)
1	I	SK L
2	II — IIIA	SK 1
2a	—	SK 2
3	—	SK 3
4	III	SK 4
5	—	—
6	IV	SK 4
6a	—	—

Table 2. Equivalent puncture protection levels

Puncture protection level according to some of the leading standards in this field	
NIJ 0115.00 (USA)	HOSDB 2007. Part 3 (United Kingdom)
1	KR1+SP1
—	KR1
2	KR2+SP2
—	KR2
3	KR3+SP3
—	KR3

➤ CLASSIFICATION BY THE WAY OF WEARING

- for visible wearing;
- for hidden wearing.

Visible wearing - this type of armor is worn on the clothes. They are mainly used by military and police, as well as by some security guards. The outer case is made in black for police; in camouflage, with various patterns for military; in black, signal or the color of uniform for guards. These bulletproof vests are mainly with protection levels IIIA, III, IV under NIJ and levels 5, 6 and 6a under GOST - for police and military; and with protection levels I, II under NIJ and levels 1, 2 and 3 under GOST - for security guards.

Hidden wearing - this type of armored vests are worn under the clothes. They are mainly used by security guards, officials and businessmen. The outer case of these vests is usually made in white or black. These bulletproof vests are primarily of protection levels I, II under NIJ and levels 1, 2 and 3 under GOST.

➤ CLASSIFICATION BY THE GENDER OF THE INDIVIDUAL

- for men;
- for women.

For women - they are made according to the specific of the female body in all classes of ballistic protection, according to the standards and in the colors and patterns of the outer case depending on the purpose.

For men - they are made in all classes of ballistic protection, according to the standards and in the colors and patterns of the outer case depending on the purpose.

➤ CLASSIFICATION ACCORDING TO THE MATERIALS OF THE PROTECTIVE BALLISTIC PANELS

- Flexible ballistic panel;
- Hard ballistic panel / armor plate.

The flexible ballistic panels can be divided to:

- single-component;
- multi-component.

Single-component flexible ballistic panels are made of one type of ballistic material. Special materials are used, such as: UHMWPE - Dyneema®, Spectra®; p-aramids - Kevlar®, Twaron®, Artec®; PBO - Zylon®; Polyhydroquinone-diimidazopyridine-M5®.

Multi-component flexible ballistic panels are made of combined two or more ballistic materials. It is possible to combine any of the above materials with m-aramids, ceramic materials and more.

The hard ballistic panels can be divided to:

- single-component;
- multi-component.

Single-component hard ballistic panels are made of one kind of material, while different combinations of materials are used in the production of *multi-component hard ballistic panels*. [17]

Some materials used in hard ballistic panels are: steel and steel alloys; titanium and titanium alloys; composite materials; ceramic materials; UHMWPE materials; p-aramid materials, etc. [18]

3. Conclusion

Excellent knowledge of modern weapons and existing means of individual ballistic protection are crucial to the right choice of means to protect the health and life of the officers during law enforcement, anti- and counter-terrorist, peace supporting, military and other operations.

The classification of the various bulletproof vests by a given feature allows for a quick, adequate and reasonable choice of the kind and type of a bulletproof vest, according to the specific needs and requirements of the given organization, depending on performed tasks, degree of risk and environment of the operations.

4. References

- [1] <http://www.marsarmor.com>
- [2] <http://www.armyequipment.com>
- [3] <http://www.outlast.com>
- [4] <http://www.garantigiyim.com>
- [5] <https://temp3000.com>
- [6] National Institute of Justice, September 2000, Ballistic Resistance of Personal Body Armor, NIJ Standard-0101.04, National Institute of Justice, Office of Science and Technology, Washington, DC 20531
- [7] Nikolova, V. Special means of individual protection (Personal protective equipment for critical infrastructure, counterterrorism and crisis response operations). Scientific monograph. IMSETHAC-BAS, 2014, ISBN: 978-619-90310-2-5, 184
- [8] Nikolova V. New development of fabrics with digital camouflage for the Bulgarian army. Fifth International Scientific Conference "Partnership, Research and Defense Technologies HEMUS 2010", Plovdiv, 2010, ISSN 1312-2916
- [9] National Institute of Justice, July 2008, Ballistic Resistance of Body Armor, NIJ Standard-0101.06, National Institute of Justice, Office of Science and Technology, Washington, DC 20531
- [10] State Standard of the Russian Federation, 2016, Armored clothing. Classification and general technical requirements, GOST R 50744-95, IPK Publishing House of Standards, Updated: 2016
- [11] Deutsches Institut für Normung, 2003, Bullet-Resistant Vests with Stab Protection, German Schutzklassen Deutsches Institut für Normung, 2003
- [12] Croft, J., PSDB Body Armour Standards for UK Police (2003) Part 2 - Ballistic Resistance, Publication No 7/03/B, Home Office Police Scientific Development Branch Sandridge, St Albans Hertfordshire AL4 9HQ, United Kingdom
- [13] Croft, J., Longhurst, D., HOSDB Body Armour Standards for UK Police (2007), Part 1: General Requirements, Publication No. 39/07/A, ISBN: 978-1-84726-424-4, Crown Copyright, 2007
- [14] Croft, J., Longhurst, D., HOSDB Body Armour Standards for UK Police (2007), Part 2: Ballistic Resistance, Publication No. 39/07/B, ISBN: 978-1-84726-425-1, Crown Copyright 2007
- [15] National Institute of Justice, September 2000, Stab Resistance of Personal Body Armor, NIJ 0115.00, National Institute of Justice, Office of Science and Technology, Washington, DC 20531
- [16] Croft, J., Longhurst, D., HOSDB Body Armour Standards for UK Police (2007), Part 3: Knife and Spike Resistance, Publication No. 39/07/C, ISBN: 978-1-84726-426-8, Crown Copyright 2007
- [17] Nikolova, V. Materials used in the production of the soft panel of the bulletproof vest. Advantages and disadvantages. Collection of papers "Fourth National Conference with International Participation, Metal Science, Hydro- and Aerodynamics, National Security 2014", Sofia, 2014, ISSN 1313-8308
- [18] Nikolova, V. Ceramic materials used in the manufacture of armor plates for bulletproof vests. Collection of papers "Fourth National Conference with International Participation, Metal Science, Hydro- and Aerodynamics, National Security 2014", Sofia, 2014, ISSN 1313-8308

SPATIAL TECHNOLOGIES FOR CRISIS MANAGEMENT

ПРОСТРАНСТВЕНИ ТЕХНОЛОГИИ ЗА УПРАВЛЕНИЕ ПРИ КРИЗИ

Assos. Prof. Milen Ivanov PhD, Ivailo Neshev PhD
 NMU „Vassil Levski” Veliko Tarnovo, Bulgaria
 e-mail milen_i1970@abv.bg
 e-mail neshev_in@abv.bg

Abstract: Over the last decades the impact of natural disasters to the global environment is becoming more and more severe. In this context, satellite remote sensing, along with Geographic Information Systems (GIS), has become a key tool in flood risk management analysis. Remote sensing for supporting various aspects of flood risk management was investigated in the present thesis. In particular, the research focused on the use of satellite images for flood mapping and monitoring, damage assessment and risk assessment.

Key words: SPATIAL TECHNOLOGY, RISK MANAGEMENT, DISASTER, NATURAL HAZARDS, GEOINFORMATION TECHNOLOGY, REMOTE SENSING SYSTEM, GEOGRAPHIC INFORMATION SYSTEMS.

1. Introduction.

The last two decades have witnessed the increasing use of satellite remote sensing for understanding the geophysical phenomena underlying natural hazards [3]. Being able to observe large portions of the Earth surface, to perform frequent and regular in time measures and with the capability to investigate in the different bands of the electromagnetic spectrum, satellite remote sensing allows to study phenomena not directly accessible with the traditional surveying techniques and ongoing situations difficult to identify in another way [4].

In the broadest sense, the measurement or acquisition of information of some property of an object or phenomenon, by a recording device that is not in physical or intimate contact with the object or phenomenon under study; e.g., the utilization at a distance (as from aircraft, spacecraft, or ship) of any device and its attendant display for gathering information pertinent to the environment, such as measurements of force fields, electromagnetic radiation, or acoustic energy. The technique employs such devices as the camera, lasers, and radio frequency receivers, radar systems, sonar, seismographs, gravimeters, magnetometers, and scintillation counters.

Today, we define satellite remote sensing as the use of satellite-borne sensors to observe, measure, and record the electromagnetic radiation reflected or emitted by the Earth and its environment for subsequent analysis and extraction of information.

Satellite remote sensing, along with Geographic Information Systems (GIS) – fig.1, has become a key tool in disaster risk and damage assessment analysis [5]. Satellite images, acquired during, before and after a flood event, can provide valuable information about flood occurrence, intensity and progress of flood inundation, river course and its spill channels, spurs and embankments affected/threatened etc. so that appropriate mitigation measures can be planned and executed in time.

Throughout the World in the recent past, whether it is a natural hazard or by the intervention of human activities, disasters have become an issue of rising alarm [11]. Natural disasters arise in many parts of the earth, and each type of disasters is confined to particular regions. It have been estimated that more than 95 percent of all deaths in developing countries were due to natural disasters. These places are particularly vulnerable to disasters because of densely packed population and poor infrastructures which gets coupled with unbalanced landforms and continuous exposure to severe weather changes.

Risk arises out of uncertainty. It is an inherent part of existence and is the chance of something happening as a result of a hazard or a disaster which will impact on community and environment. It is measured in terms of the likelihood of it happening and the consequences if it does happen that be tried to reduce the likelihood of risk effecting on community. The risk is the probability or chance that the hazard posed. Thus, it can be minimised by initially preparing a suitable risk management.

Risk Management is a process consisting of well defined steps which, when taken in sequence, support better decision making by contributing to a greater insight into risks and their impacts. It is as much about identifying opportunities as it is about used to avoid, reduce or control risks. The first step in the risk management process is focused on the environment to establish the boundaries in which risks must be managed and guide decisions on managing risks, and develop risk evaluation criteria. The second step involves identifying the risks which arise from aspects of the environment that will be established from previous step to develop a complete inventory of the risks and what each involves, by selecting suitable techniques to identify potential risks, examining sources of possible risks, pose a major threat to community. Assess and analyse the impact of the risks represent the third step, which involves deciding on the relationship between the likelihood (frequency or probability) and the consequences (the impacts) of the risks that be identified. The level of risk should be analysed in relation to what are currently doing to control that risk. Control measures decrease the level of risk, but there may be sufficient risk remaining for the risk to be considered with others. Risk evaluation will be clarified the following as the activity of risk managing and its outcomes, the degree of control over the risk, the potential and actual losses which may arise from the risk, and the benefits and opportunities presented by the risk. The next step is to treat the risks that be decided as unacceptable by identifying the options which could use to treat the risks, selecting the best option in terms of its feasibility and cost effectiveness, preparing a risk treatment plan, and implementing the risk treatment plan.

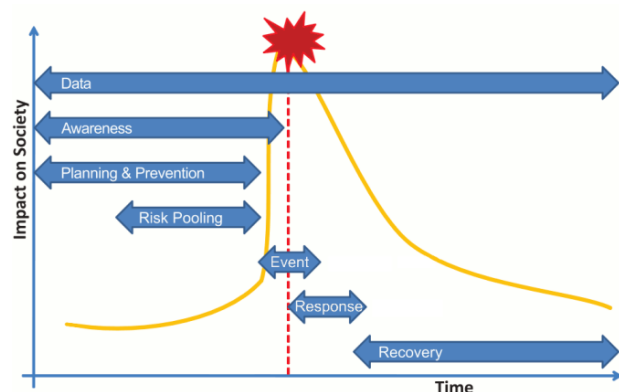


Figure 1. Information support to Crisis management.



Figure 2: Risk management

The main concern of this thesis is the delineation of flood prone areas, the identification of damaged areas and the development of hazard maps indicating flood susceptible areas by means of geospatial approaches. In particular, the contribute of satellite remote sensing and GIS for flood mapping and monitoring, damage assessment and risk assessment was explored referring to selected cases of study.

2. Spatial technologies and risk management

Earth Observation System (EOS) otherwise known as Remote Sensing (RS) and GIS assist professionals of disaster management in a very effective manner and provides more precise data. With this technology it is ease to obtain homogeneous data covering the entire world over a short period of time. Remote Sensing involves in assessing the extent of damage incurred during the time of disaster, identification of possible escape routes and location of areas for storage of temporary housing.

Each sensor provides distinctive information about different properties of surface objects or the shallow layers of the earth. For instant to measure surface temperature thermal sensors are employed, microwave sensors used to detect dielectric properties. This in turn reveals the moisture content of surface soil or of snow. For details, see Appendix 1.

Being able to observe large portions of the surface of the Earth, to perform frequent and regular measures and with the capability to investigate in the different bands of the electromagnetic spectrum, satellite remote sensing allows to study and analyse phenomena not directly accessible with the traditional surveying techniques and ongoing situations difficult to identify in another way.

The last two decades have witnessed the increasing use of remote sensing for understanding the geophysical phenomena underlying natural hazards [4][10][3]. In particular, the development of new acquisition systems in the field of optical remote sensing, with the possibility to direct the sensor to specific areas, has enabled to increase the spatial and the temporal resolution of the satellite images, allowing theoretically to collect scenes of any part of the Earth surface with a time interval ranging between 1 and 7 days. Capable to collect data in all weather and lighting condition, active microwave sensors have proven to be useful to identify various spatial phenomena; especially in the context of natural disaster management, Synthetic Aperture Radar (SAR) images are used for detecting damaged areas and for the real-time monitoring of harmful events.

In this context, remote sensing provides valuable information helping to understand spatial phenomena and supporting the decision making with objective data. In particular, it can contribute to the disaster management activities through the identification of hazardous areas, the assessment of the damaged zones in a timely manner and assisting the recovery plans after the occurrence of a disaster.

3. Satellite remote sensing in the disaster risk management cycle

An increasing number of studies have been elaborated on the importance and applications of remote sensing, with particular reference to satellite remote sensing data, in the disaster risk management [3][10]. A major reason of using remote sensing in this field is that it is the fastest means of collection data for pre and post-event disaster studies [14].

Satellite remote sensing refers to the technology used for observing various earth phenomena with instruments that are typically on board a spacecraft. These observations consist of measuring the electromagnetic energy of phenomena that occur without physical contact with the object of interest. Therefore, to investigate the Earth's surface without being in contact with it is an important feature considering the limited accessibility of the areas affected by a disaster and, in many cases, their extension and imperviousness. In addition, bandwidths are a crucial component of remote sensing operations. In fact, the different bandwidths of the electromagnetic spectrum are related to certain phenomena and Earth parameters that can be monitored and analysed using various sensors.

Satellite remote sensing can provide valuable information in each phase of the disaster risk management cycle, helping to understand spatial phenomena and supporting the decision making with objective data [4][8]. It can contribute to the risk management activities through the identification of hazard areas, the assessment of damaged zones in a timely manner and assisting the recovery plans.

Each phase of the risk management cycle requires satellite images data with appropriate characteristics of spatial, spectral and temporal resolution depending on the kind of information to be obtained, such as physical indicators and measureable features, and the spatial scale of the analysed hazard [7].

In the mitigation stage, the remote sensing data are usually employed for mapping landscape features (i.e. land use/land cover) and for detecting potentially hazardous areas; therefore, the update representations of a territory is an important requirement to select useful satellite images. Furthermore, high spatial resolution images can allow for the identification of infrastructure and buildings in risk areas, for the hazards consequence assessment (vulnerability) and the potential losses evaluation.

In the preparedness phase remote sensing data can support the developing of risk maps and models, using the information obtained in the previous stage, which are generally used by authorities to communicate information about location and range of hazard to the community.

During the pre-event phases and recovery stage there is sufficient time for selecting appropriate remote sensing data; instead, the timeliness is a crucial factor in the response phase during which the rapid damage assessment is fundamental for efficient emergency services and to assist evacuation plans. Moreover, the availability of high spatial resolution images allows a detailed representation of the ongoing situation.

In the recovery stage, remote sensing data are used for post-disaster census information, for identifying the rebuilding sites and for the long term monitoring of the territory; in particular, remote sensing can support this stage providing time series images over large areas with both high and medium spatial resolution from which changes can be detected and quantified.

Satellite data support to disaster management and risk assessment is also defined by a set of interrelated activities or business processes, which may be grouped into the following stages:

1. Initiation, including research to determine an observation strategy and predictive capabilities;
2. Operational / steady-state event detection and response;
3. Disaster recovery, risk assessment, and mitigation.

Initiation

Operational activities are often preceded by *disaster management initiation*, with the following activities:

- Evaluate candidate satellite observations for use in disaster related applications (e.g., for predicting volcan-ic eruptions)
- Identify inputs for event detection; event triggers
- Identify indicators for situational awareness (e.g., flood extent)
- Define modeling elements (e.g., regional flood model)
- Define workflows and data flows for processing and delivery
- Identify automation opportunities (e.g., subscriptions, custom products)
- Develop methods for validating products
- These initiation activities may be repeated any number of times, e.g., to review and refine the observation strategy, incorporate new inputs, or revalidate predictive methods.

Event detection and response

Once initiation is complete, steady-state *event detection and response* may begin, with the following activities (depicted in Figure 3):

1. *Detect (and possibly predict) events* based on global or regional monitoring, models or reports from users;
2. *Monitor operations*—this operations shared awareness of a dynamic situation, enabling timely decisions about data assimilation, analysis, and dissemination;
3. *Task Sensors and acquire other data* for high-resolution observations of areas threatened or impacted by a disaster event;
4. *Model and Predict* to pinpoint priority times and locations for response and recovery efforts; and to better understand the natural phenomena.
5. *Analyze and Interpret* data obtained via satellite or in situ sensors or other sources (this includes validating the resulting information products);
6. *Disseminate* visual products to end users, including reports or updates. (In fact, user access is potentially a part of any of the activities depicted here, allowing users to draw upon, or even to shape, the gathering, processing, or production of information.)

Figure 3 shows how these steady-state processes relate to each other: for example, when flood forecasting models detect a flood risk, decisionmakers may task a satellite to observe the affected area, and apply a variety of processing algorithms to interpret it. The resulting data, along with data from *in situ* rain and stream gauges, feeds another model to determine detailed flood areas.

Recovery and mitigation

Following the detection and response phases, recovery and mitigation activities include the following processes:

- Overlay earth observations with data on settlements and infrastructure from many local sources (for damage assessment and recovery planning and prioritization);
- Periodic surveys to assess the progress of reconstruction and recovery efforts;
- Review historical data (and where appropriate, conduct disaster simulations) to identify risk patterns and trends over time, and to quantify future risk (for budgeting and risk pooling / insurance). These studies also aim to understand the spatial variability of risk (for setting land-use policies or property values) and to characterize key risk factors (for improved environmental or development policies; and for infrastructure improvements where appropriate).
- Research towards improving disaster prediction, preparedness, or response, from recent experience. This may lead into, or combine with, the initiation activities outlined earlier.

Not every instance of disaster management or risk assessment will include all of these processes; however most will fit into some subset of Figure 3, and can thus trace their relationship with other processes.

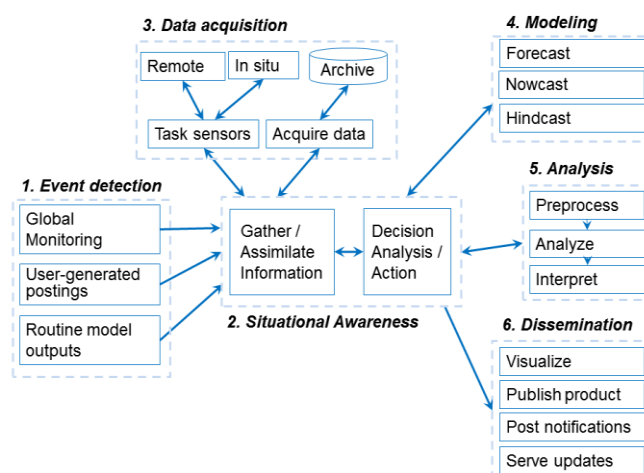


Figure 3. Activities involved in the use of remote sensing in disaster management and risk assessment.

4. Remote sensing and GIS tools.

Mitigation of natural disasters can be successful only when detailed knowledge is obtained about the expected frequency, character, and magnitude of hazardous events in an area. Many types of information that are needed in natural disaster management have an important spatial component. Spatial data are data with a geographic component, such as maps, aerial photography, satellite imagery, GPS data, rainfall data, borehole data etc. Many of these data will have a different projection and co-ordinate system, and need to be brought to a common map-basis, in order to superimpose them.

We now have access to information gathering and organising technologies like remote sensing and geographic information systems (GIS), which have proven their usefulness in disaster management.

First of all, remote sensing and GIS provides a data base from which the evidence left behind by disasters that have occurred before can be interpreted, and combined with other information to arrive at hazard maps, indicating which areas are potentially dangerous [8]. The zonation of hazard must be the basis for any disaster management project and should supply planners and decision-makers with adequate and understandable information. Remote sensing data, such as satellite images and aerial photos allow us to map the variabilities of terrain properties, such as vegetation, water, and geology, both in space and time. Satellite images give a synoptic overview and provide very useful environmental information, for a wide range of scales, from entire continents to details of a few metres. Secondly, many types of disasters, such as floods, drought, cyclones, volcanic eruptions, etc. will have certain precursors. The satellites can detect the early stages of these events as anomalies in a time series. Images are available at regular short time intervals, and can be used for the prediction of both rapid and slow disasters.

Then, when a disaster occurs, the speed of information collection from air and space borne platforms and the possibility of information dissemination with a matching swiftness make it possible to monitor the occurrence of the disaster. Many disasters may affect large areas and no other tool than remote sensing would provide a matching spatial coverage. Remote sensing also allows monitoring the event during the time of occurrence while the forces are in full swing. The vantage position of satellites makes it ideal for us to think of, plan for and operationally monitor the event [11]. GIS is used as a tool for the planning of evacuation routes, for the design of centres for emergency

operations, and for integration of satellite data with other relevant data in the design of disaster warning systems.

In the disaster relief phase, GIS is extremely useful in combination with Global Positioning Systems (GPS) in search and rescue operations in areas that have been devastated and where it is difficult to orientate [5]. The impact and departure of the disaster event leaves behind an area of immense devastation. Remote sensing can assist in damage assessment and aftermath monitoring, providing a quantitative base for relief operations.

The volume of data needed for disaster management, particularly in the context of integrated development planning, clearly is too much to be handled by manual methods in a timely and effective way. For example, the post disaster damage reports on buildings in an earthquake stricken city, may be thousands. Each one will need to be evaluated separately in order to decide if the building has suffered irreparable damage or not. After that all reports should be combined to derive at a reconstruction zoning within a relatively small period of time.

One of the main advantages of the use of the powerful combination techniques of a GIS, is the evaluation of several hazard and risk scenarios that can be used in the decision - making about the future development of an area, and the optimum way to protect it from natural disasters.

Remote sensing data derived from satellites are excellent tools in the mapping of the spatial distribution of disaster related data within a relatively short period of time [14]. Many different satellite based systems exist nowadays, with different characteristics related to their spatial-, temporal- and spectral resolution.

Remote sensing data should generally be linked or calibrated with other types of data, derived from mapping, measurement networks or sampling points, to derive at parameters, which are useful in the study of disasters. The linkage is done in two ways, either via visual interpretation of the image or via classification.

The amount and type of data that has to be stored in a GIS for disaster management depends very much on the level of application or the scale of the management project. Natural hazards information should be included routinely in development planning and investment project preparation [4]. Development and investment projects should include a cost/benefit analysis of investing in hazard mitigation measures, and weigh them against the losses that are likely to occur if these measures are not taken.

Although the selection of the scale of analysis is usually determined by the intended application of the mapping results, the choice of a analysis technique remains open. This choice depends on the type of problem, the availability of data, the availability of financial resources, the time available for the investigation, as well as the professional experience of the experts involved in the survey. See also Cova (2002) for an overview of the use of GIS in emergency management.

4.1. Remote Sensing Vs GIS

GIS (Geographic Information System) is a kind of software that enables:

- The collection of spatial data from different sources (Remote Sensing being one of them).
- Relating spatial and tabular data.
- Performing tabular and spatial analysis.
- Symbolize and design the layout of a map.

A GIS software can handle both vector and raster data (some handle only one of them). Remote Sensing data belongs to the raster type, and usually requires special data manipulation procedures that regular GIS does not offer. However, after a Remote Sensing analysis has been done, its results are usually combined within a GIS or into database of an area, for further analysis (overlaying with other layers, etc) [1]. In the last years, more and more vector capabilities are being added to Remote Sensing softwares, and some Remote Sensing functions are inserted into GIS modules.

4.2. Remote Sensing Vs Aerial Photography / Photogrammetry

Both systems gather data about the upper surface of the Earth, by measuring the Electromagnetic radiation, from airborne systems. The following major differences can be given:

- Aerial photos are taken by an analog instrument: a film of a (photogrammetric) camera, then scanned to be transformed to digital media. Remote Sensing data is usually gathered by a digital CCD camera.
- The advantage of a film is its high resolution (granularity), while the advantage of the CCD is that we measure quantitatively the radiation reaching the sensor (radiance values, instead of a gray-value scale bar). Thus, Remote Sensing data can be integrated into physical equations of energy-balance for example.
- An Aerial photograph is a central projection, with the whole picture taken at one instance. A Remote Sensing image is created line after line; therefore, the geometrical correction is much more complex, with each line (or even pixel) needing to be treated as a central projection.
- Aerial photos usually gather data only in the visible spectrum (there are also special films sensitive to near infrared radiation), while Remote Sensing sensors can be designed to measure radiation all along the Electromagnetic spectrum.
- Aerial photos are usually taken from planes, Remote Sensing images also from satellites.
- Both systems are affected by atmospheric disturbances. Aerial photos mainly from haze (that is, the scattering of light – the process which makes the sky blue),
- Remote Sensing images also from processes of absorption. Atmospheric corrections to Aerial photos can be made while taking the picture (using a filter), or in post-processing, as in done Remote Sensing. Thermal Remote Sensing sensors can operate also at nighttime, and Radar data is almost weather independent.
- In Photogrammetry the main efforts are dedicated for the accurate creation of a 3D model, in order to plot with high accuracy the location and boundaries of objects, and to create a Digital Elevation Model, by applying sophisticated geometric corrections. In Remote Sensing the main efforts are dedicated for the analysis of the incoming Electromagnetic spectrum, using atmospheric corrections, sophisticated statistical methods for classification of the pixels to different categories, and analysing the data according to known physical processes that affect the light as it moves in space and interacts with objects.
- Remote Sensing images are more difficult to process, and require trained personnel, while aerial photographs can be interpreted more easily.

5. Conclusions

This paper presents a general review on utilization of remote sensing and GIS for natural disaster management cycle. Remote sensing can be potentially employed to address various aspects of disaster management cycle. Rather focusing only on emergency response, it is essential to consider all facets of disaster management. Remotely sensed data extend their support to disaster management organizations via providing relevant and accurate information in a temporally, spectrally and spatially significant context. In addition to it, one should tailor the technologies owing to remote sensing to fulfill the desired requirements of the disaster organization. It is necessary to examine and evaluate the so far

6. Literature

1. Belward A. S., Valenzuela C. R., Remote sensing and geographical information systems for resource management in developing countries, Kluwer academic publishers, London, 2001

2. Cova T.J. Extending geographic representation o include fields of spatial objects, Int. J. geographical inforation science, vol.16, № 6, 509-532 p., 2002

3. Janssen L.F., Huurneman G.C., Principles of remote sending, ITC, Enschede, Netherlands, 2001

4. Ivanov M., Yankov Y., Determination of potential floodings through geoinformation technology, Bulletin Stiintific XXI, Sibiu, 2016

5. Ivanov M., Yankov Y., Application of geographic information systems in crisis management, Revista XXI, Sibiu, 2016

6. Ivanov M., Yankov Y., Improvement of early warning systems, International scientific conference, 11 to 14 December, 2017, Borovets, Bulgaria.

7. Ivanov M., Yankov Y., Application of mobile giservices in disaster management, International scientific conference, 11 to 14 December, 2017, Borovets, Bulgaria.

8. Levin N., Fundamentals of Remote Sensing, Remote Sensing Laboratory, Geography Department, Tel Aviv University, Israel, 1999

9. MC 296/1 NATO Geospatial Policy, 2006.

10. Satyanarayana P., Yogendran S., MILITARY APPLICATIONS OF GIS ENC QC Department, IIC Technologies Private Limited, Hyderabad

11. Schott J. R., Remote sensing the image chain approach, 2nd edition, Oxford university press, 2007

12. STANAG 7016 IGEO – Maintenance of geographic materials, edition 4, 2002

13. STANAG 7163 Vector Map (Vmap) Level 1, edition 1, 2003

14. <http://www.ccrs.nrcan.gc.ca>, Remote Sensing, Accessed 29.08.2017.

Appendix 1. EMR Wavelengths and Sensors

Wavelength	Waveband	Applicable for	Sensors example
Visible (VIS)	0.4-0.7mm	Vegetation mapping	SPOT; Landsat TM
Building stock assessment		AVHRR; MODIS; IKONOS	
Population density		IKONOS; MODIS	
Digital elevation model		ASTER; PRISM	
Near infrared (NIR)	0.7-1.0mm	Vegetation mapping	SPOT; Landsat TM; AVHRR; MODIS
Flood mapping		MODIS	
Shortwave infrared (SWIR)	0.7-3.0mm	Water vapour	AIRS
Thermal infrared (TIR)	3.0-14mm	Active fire detection	MODIS
Burn scar mapping		MODIS	
Hotspots		MODIS; AVHRR	
Volcanic activity		Hyperion	
Microwave (Radar)	0.1-100cm	Earth deformation and ground movement	Radarsat SAR; PALSAR
Rainfall		Meteosat; Microwave Imager (aboard TRMM)	
River discharge and volume		AMSR-E	
Flood mapping and forecasting		AMSR-E	
Surface winds		QuikScat radar	
3D storm structure		Precipitation radar (aboard TRMM)	

MAINTENANCE OF TECHNICAL SYSTEMS IN THE FUNCTION OF SAFETY AT WORK

Veljanovski D. MSc. , Jovanovska V. PhD.
Faculty of biotechnical sciences – Bitola
University of "St.Kliment Ohridski" - Bitola, Republic of Macedonia
darkoveljanovski@yahoo.com

Abstract: *Safety engineering is consistently promoted and there is an evident need for improvement and development. The maintenance process is dependent on the method of editing and organizing the setup and execution of such kind commitments.*

Working with the maintenance system itself determines the manner of maintenance.

The contractor's responsibility for providing a high level efficiency of system maintenance because the process involves detecting and reducing degradation and restoring the functions of the system in working order.

The purpose of this paper is to overcome the shortage of updating data for occupational safety for maintenance, knowledge and to introduce new methods to protect workers and the working environment, as well as monitoring the current trends and standards.

Keywords: ORGANIZATION, MAINTENANCE, SYSTEM, SAFETY ENGINEERING.

1. Introduction

Safety at work and safety throughout the maintenance of the technical system is of utmost importance in order to preserve the health of both the operator and the health of those who care about the system's correctness, so that they can continuously meet the expected norms. For that purpose, analyzes, constant surveillance and regular checking of the correctness of the system are performed. There are also several ways to check, monitor the situation and maintain the technical system, because as such it is an assemblage of multiple smaller systems, multiple parts, and elements. Any irregularity, inadequate functioning, deviation, and alteration must be noted.

The role of safety and the protection of health at work is determined by its purpose, rights and obligations of the employer and the employee. It is difficult to comply with the law and other regulations in these areas, to achieve the highest level of health and psychophysical protection. In that sense, the working conditions, the means and the organization of work must be tailored to the needs of the worker, and at the same time workers must be motivated to actively engage in all activities. The significance of safety and health at work is perceived as a human, social and economic point of view.

Working in humane conditions is a pleasure for every individual, but also success and pride for the employer and the society as a whole. The social significance is mostly the case with a large number of employees who get injured or lose a life at work, get sick from occupational diseases and other work-related illnesses, but often in relation to their family, for which the company takes care. The economic dimension of occupational safety and health is dealt with through the consequences of injury at work, occupational and other diseases and ends with certain financial indicators that depend on the number and severity of such cases.

Occupational injuries and occupational diseases are often given absenteeism, which makes expenses because the worker is not working, because of the stagnation that occurs in production and because of the knowledge that is being issued for the treatment of the employee, his earnings and other expenses fall at the expense of the employer and the social security fund. This means that safety and health at work affect the productivity and economy of the work, as well as the quality and competitiveness of the product on the market, the employer has an immediate interest in the product to be as efficient as possible.

Safety engineering affects on the maintenance which is a process that is carried out in order to extend the life cycle of the technical system, as well as to increase the time-consuming exploitation of that system, which can last longer.

2. Maintenance goals of technical systems

Technical production systems are becoming more complex and parallel, they must work with greater reliability. The permissible level of reliability can be ensured by an adequate application of maintenance, which is a process that allows managing the technical condition and reliability throughout the "life cycle" of the system.

Maintenance, as a function of the production system, aims to provide opportunities for functioning of the means of operation according to the requirements of other functions of the production system, at given time and conditions at certain costs. This objective prior to maintenance sets complex and diverse tasks.

It is certain that every maintenance worker, regardless of his position and role in the given process, has the desire to provide reliable and safe operation of the system with minimal costs. Thus, the maintenance objectives include, inter alia, the sphere of economic activity. Therefore, modern science of maintenance is increasingly studying and increasing the level of importance in the economy and society.

The maintenance objective can be fully realized only through the efficiency of the basic production process, so that the maintenance costs and the cost of production downtime can be as small as possible and the productivity in the production as large as possible.

All costs incurred in the exploitation process should weigh to a certain minimum. Maintaining the technical systems greatly influences the increase in the efficiency of the efficient operation of the manufacturing enterprises.

The basic objectives to be achieved through the maintenance process are:

- providing the necessary level of reliability;
- minimizing maintenance costs;
- limitation of the aging of the technical system;
- increasing productivity at work;
- increasing the level of motivation;
- timely performance of the function, etc.

It can be said that the maintenance of the technical systems encompasses all the procedures that should be undertaken for the technical system to work longer in a working state, i.e. in a lifetime, with the permissible level of reliability, productivity and economy.

3. The maintenance function and its structure

The maintenance function affects the overall flows and outputs of the work in the production system, and its influence increases with the mechanization and automation of the means of production. Maintenance is a function of the production system which contains all the activities and elements necessary for ensuring

the functioning of the means of operation, from determining the requirements for their construction to exclusion from exploitation.

Maintaining is essentially related to the underlying production process, since it contributes to the production being rational with the optimal level of reliability of all systems in the enterprise. Maintaining as a function of the production system has all the elements of a single system: goal, input, output, structure, condition and process, (Figure 1).

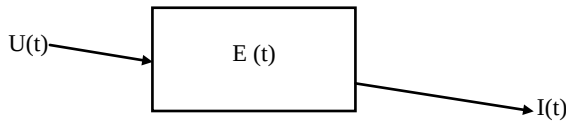


Fig. 1 Maintaining as a function of the production system

- $U(t)$ - vector for entry in function of maintenance;
- $I(t)$ - the output from the maintenance function;
- $E(t)$ - transform vector.

The components of the output vector of the maintenance function have different appearance patterns.

Basic forms are:

- the functioning of the maintained funds, i.e. the state "in operation" and the condition "in the rejection";
- activities carried out with the maintenance function and
- total income realized with the contribution of the maintenance.

As a natural form of a product from the maintenance function are the forms of "working" condition and a condition "in the cancellation" of the funds being maintained.

The input components coming from the production system and its environment are:

- spare parts and maintenance materials;
- maintenance persons;
- energy;
- the influence of the production function;
- objectives of the maintenance function and others.

The structure of the maintenance function is complex because it is composed of natural-technical and organizational systems. It consists of:

- executors of maintenance;
- maintenance means;
- maintenance strategy;
- funds that are being maintained;
- concept of maintenance approach and
- connection of all elements.

Maintenance is a constituent part of the reproduction process and therefore is studied as an integral activity in ensuring the planned "life cycle" of each technical system. Modern predictions give it a major role to play in production, in order to achieve optimum production results by introducing new maintenance technologies, in fact, creates modern technical maintenance that provides all the maintenance activities, plans, coordinates, controls the technical and economic efficiency of the production plants.

4. Confidentiality and safety of the technical system

Technical systems represent a set of components, their relationships and their characteristics structured in a way that ensures operation in the work and performance of the function in day time and given conditions. The problem of achieving confidentiality in technical systems is most closely related to the behavior of the system at a given time and given environmental conditions. The development of technical systems and their increasing complexity require a greater degree of confidentiality. Therefore, research on increasing the degree of confidentiality

should be one of the tasks that should be given special attention in order to achieve safer and more economical production.

The reliability of the entire system is a new approach to this problem and it covers the confidentiality of the entire system of the production system or of several common production systems. Modern concepts require the confidentiality of the entire system to be managed with appropriate measures, while using the same parameters and measured characteristics throughout the system's lifespan.

It should be emphasized that the confidentiality of the whole system is understood as the characteristics of the components of the system, as well as the needs of the planned and preventive maintenance activities. The production systems need to accomplish the function of the target, but this function can not always be maintained, because there must be interruptions or cancellations, interventions or repairs occasionally i.e. maintenance procedure. On this basis, the basic characteristics of the system (achieved and expected production) are obtained, which is in fact the reliability of the system.

The reliability of the technical system is measured by the relative time for which the system is capable of production in terms of time required to work without any omissions and no standby maintenance. Due the exploitation of the technical systems, special attention must be paid to the proper maintenance of these systems. In addition to achieving "good" production, it is also necessary to achieve cost-effective operation, by mutually harmonizing production and costs, by optimizing confidentiality. But in some cases, the higher the level of reliability of the technical system is of much greater importance.

Researching about confidentiality in production-technological systems is carried out in order to define and plan the maintenance process and make the right choice of a maintenance strategy. The motives that appear for the study of the reliability of the technical systems are the following:

- the technical systems are becoming increasingly complex, which increases the likelihood of failure and the inability to maintain them with maximum effectiveness;
- striving to increase production;
- maintenance difficulties can occur in difficult access parts of the system;
- the need for safe and safe operation;
- economic damages arising from the bad functioning of the technical system and
- increased confidentiality ensures a quality system as a whole.

The reliability of the system is an integral part of the effectiveness of the system. The effectiveness of the system is a probability for the system to successfully enter into operation and perform the function of the criterion at projected time and given conditions.

The effectiveness of a system in mechanical engineering is a product of the components:

- system reliability (R),
- the system's availability (G),
- functional eligibility (FP)

expressed by the formula: $Es(t) = R(t) \cdot G(t) \cdot FP$ $0 < Es < 1$

The availability of the system is a probability that the system can successfully enter into operation and realize the projected output sizes in the necessary minimal time for the given conditions in the environment. The conditions of the environment are a particularly important factor that makes the availability function complex. The availability of the system is a direct indicator of the readiness of the system to perform its function, which reflects the value of the function of confidentiality and the function of system eligibility.

Functional eligibility is the ability of the system to successfully adapt to the environment at a given time. If the functional suitability is greater, even its adaptability to environmental conditions is greater - more flexible. However, this does not give the right to design systems with maximum possible changes, as this leads to a minimal utilization rate. The functional eligibility of the system

moves within the limits $0 \leq FP \leq 1$ and shows to what extent the system is able to adapt to the changing conditions and disruptions in the process of operation.

The working ability of the system is in fact the ability to perform the criterion function at a given time. Each technical system is exposed to different influences, by size, direction and dimensions that cause deviation from the ground of the set function of the criterion and decrease of the working ability of the system. Each technical system when introducing into production should satisfy the function of the target with given criteria.

However, it is not known how long the system will be able to fulfill the function of the target with the given criteria. The fulfillment of the desired parameters of the system according to some criteria is conditioned by the exploitation of the system and the mode of operation of their elements. The ability of the system to maintain the working ability at the time of exploitation is called *confidentiality*.

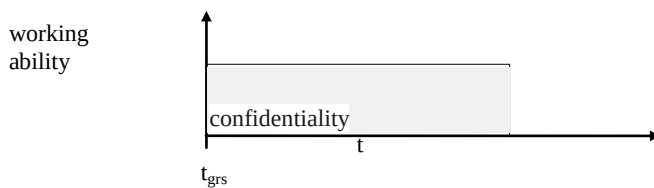


Fig. 2 Working ability of the system

Determination of the function is done by the following formula:

$$F(t) = \int_0^t (\text{working ability}) dt$$

The sketch shows that the working ability has a constant value, that is, the system is or is not capable of working. This particular confidentiality is the size that can be determined after a failure occurs in the system.

5. Basic conditions and system failures

The technical system is exposed to different by size and direction influences. Changing the criterion function under the influence of many influences within the permitted deviations determines the baseline situation as follows:

- condition in operation (the system is capable of working);
- failure state (the system is incapable of working).

The system is capable of working if it provides the required designs and permitted output sizes, that is, it meets the performance criterion. An incompetent system is one in which the mutually established dependencies of the parts and the relations between them and their characteristics are disturbed, i.e. it does not perform the criterion function, and it is therefore necessary to undertake measures for returning to a state of work that we call maintenance intervention.

In the case of technical systems, the following failures can occur: complete failures where the working capability is zero, partial failures where the system performs work under the given limit of the allowed deviations. Failure conditions and reduce the degree of utilization of working time - to the next sketch.

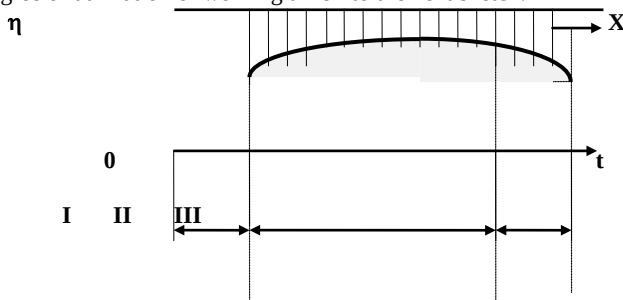


Fig. 3 Basic conditions and system failures

X – loss from a standstill

t – time unit

The basic state of the technical system is conditioned by the operating, operating and managed mechanisms of the system, whereby the situation in the work results in the performance of the criterion function within the limits of the allowed deviations, and the state of failure to lose the working ability of the system, that is, the inability of the system performs the function of the criterion.

The failures conditioned by changing the parameters of the systems can be:

- sudden abnormalities, caused by the cause of random, nonmonotonic, which are difficult to predict and
- gradual failures, caused by systemic, monotone of known sizes.

Failures caused by the inadequacy of parts of the system are:

- independent refusals, retain the internal state of the parts of the system, that is, the inability of the system to perform the criterion function in the boundary of deviation and
- dependent failures, which arise as a consequence of interdependent parts in the system.

The appearance of failures studied through causes and consequences is of particular importance through perceiving the relative frequency of phenomena of failure. There are three basic periods in the „life cycle“:

- I – period of early dismissal, occurs during the introduction of the system in operation;
- II – period in regular work, where there are random failures and
- III – period of increased number of failures, which arise from fatigue, corrosion, etc.

6. Maintaining complex technical systems

The maintenance of complex technical systems has its own special purpose. The purpose covers the procedures that are being undertaken in order for the systems to be as long as possible in the so-called. The state of operation, it is necessary during the life cycle to work on the necessary them, allowing them to complete their lifespan safely. Maintaining is a very complex problem and for its resolution it is necessary:

- detailed analysis;
- possible source of cancellation at all stages of development and
- exploitation of the system.

It is clear that maintenance is not a goal for itself. It is also deterring from harmful consequences which in fact are a failure of the technical system, partly in some part of it, establishing a specific technical system.

To achieve this goal technical system, during the exploitation period, must fulfill the foreseen functions with a satisfactory responsibility, suitable for fulfillment. Responsibility and convenience are also different, but also complementary features of complex technical systems.

The need for improving the maintenance of the existing system, in terms of safety and health protection during work, is the result of:

- scientific achievements in the field of preventive engineering and engineering maintenance;
- technological development of the facility of maintenance;
- the development of the technological elements applied in the maintenance and
- the desire to increase the end result and to reduce the total maintenance costs, all supported by the creation of safe working conditions and the working environment.

The lifetime of a machine, device or any other technical system has a complex structure. It goes through separate but

interconnected and time-synchronized group activities. The relationship of these segments is determined by the action of a number of facts. Life span covers five time phases:

- conceptual and ideal solution;
- development and design;
- production and commissioning;
- use, maintenance and expenses.

7. Safety engineering – safety and health at work

Safety and health at work means realization of working conditions, in which certain measures and activities are undertaken in order to protect the life and health of the employees and other persons entitled to it. The dangers of the workplace and the consequences of the working conditions (injuries and disease) should be studied and determined at the very beginning, ie in the phase of preparation of the construction of the product, and the production technology itself. The organization of work protection in production processes has two types of approaches, one of which is conventional and the second is contemporary.

The maintenance of the technical equipment is largely carried out with appropriate tools, because appropriate tools make the maintenance easier, more precisely and safer, for about what show the results of the survey presented in the next graph in percent of respondents (Fig. 4)

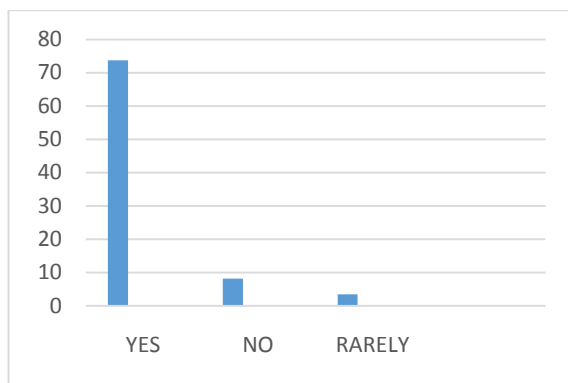


Fig 4 Using appropriate maintenance tools

Results about that question from the survey presented in percent in figure 4, clearly show that more than 70% of the respondents agree that the using appropriate maintenance tools is important for them and for the entire maintenance process.

Do workers need to know how safety engineering works? A significant question, whose answers (showed on the next graph in percent of respondents - the Fig.5) indicate the need for training, in terms of safety and health at work for each employee.

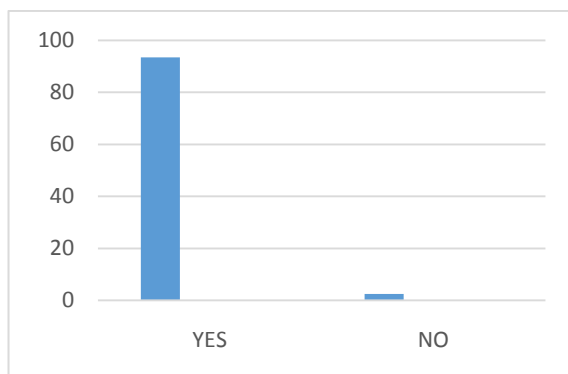


Fig.5 Workers need to know how safety engineering works

Most of 90% of respondents agree with that the workers need to know how safety works.

Safety engineering at work is one of the most important issue, because his ignorance will harm the life and health of the workes,

and that is more important than the correctness of the technical system itself.

8. Conclusion

Maintenance, as part of the organization, should follow modern trends and standards, especially with regard to workers' safety and environmental protection.

The purpose of the maintenance is to provide a high level of utilization and availability of the technical system during its lifetime.

Safety at work and safety throughout the maintenance of the technical system include analyzes, constant supervision and regular checking of the correctness of the system. There are also several ways to check, monitor the condition and maintain the technical system.

Appropriate tools for safety maintenance should be used due the maintenance of the technical systems.

All workers, especially workers who are directly included in the maintenance of the technical systems use to know how safety engineering works, what safety and health at work mean, what kind of safety should apply to achieve their life and health till they are at work.

9. References

1. Todorovic P., Jeremic B., Osnovi na odrzuvanje, Krguevac, Masinski fakultet, 2008
2. Radonjić B., Jelić M., Radojević S., Rajaković R., Kovačević Lj. *Priručnik bezbednost i zdravlje na radu – za pripremu stručnog ispita*. Beograd, 2008
3. grupa, autora. *Bezbednost i zdravlje na radu – priručnik za pripremu stručnog ispita*,. Beograd, 2008
4. Niebel, B. *Engineering maintence menagement*. 1994
5. Popović P., Ivanović G.. „*Projektovanje pouzdanosti mašinskih sistema*“. Beograd : Institut za nuklearne nauke Vinča, 2005
6. prim. dr. sci Paunović-Pfaf Jelena, *Poslodavac i bezbednost i zdravlje na radu*. Beograd, 2010
7. Ivanovic G., Stankovic D., Baker I.,Odgovornost na tehnickite sistemi, Novi sad,2010