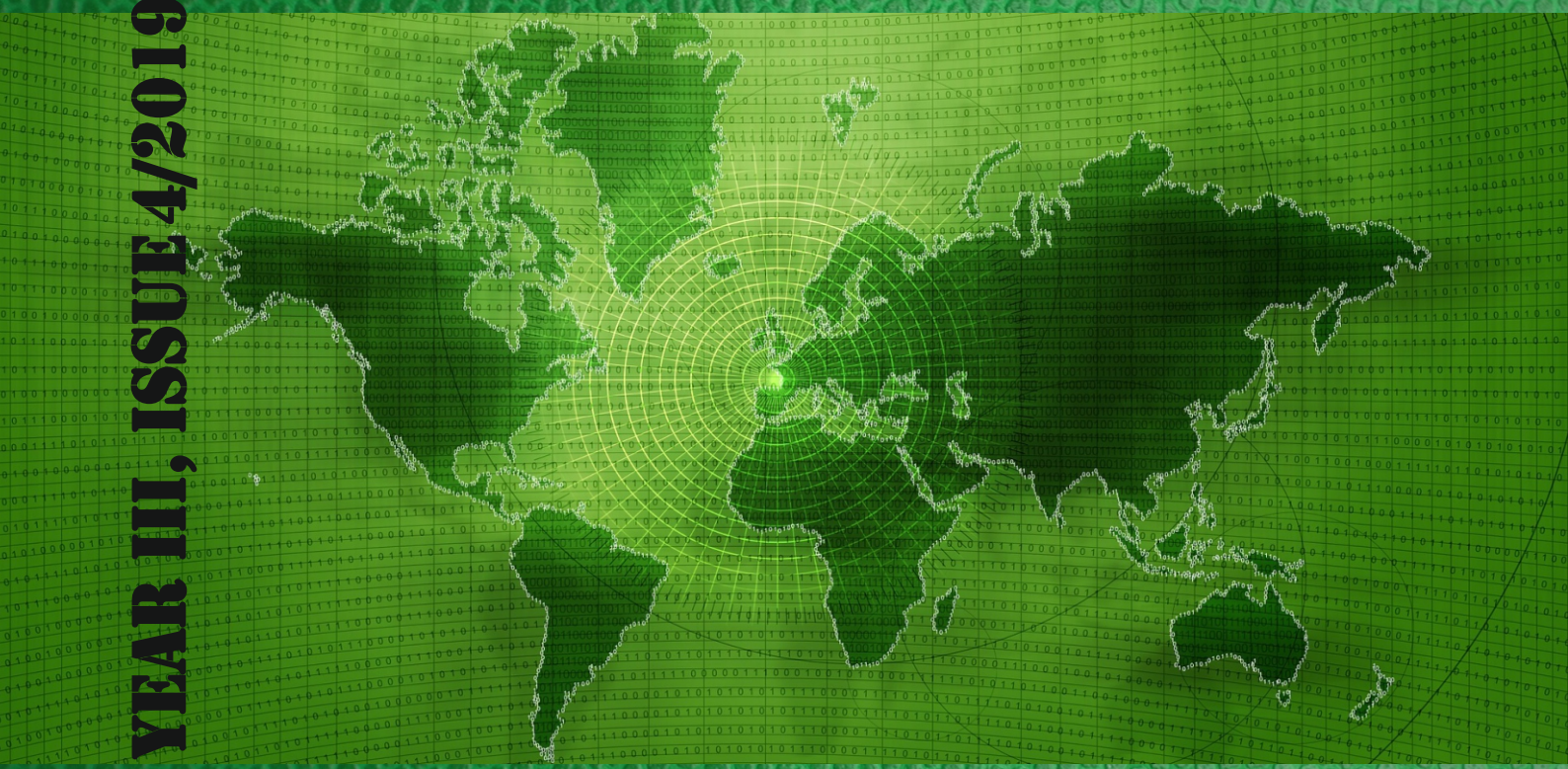
INTERNATIONAL SCIENTIFIC JOURNAL

# SECURITY & FUTURE

ISSN: (PRINT) 2535-0668
ISSN: (ONLINE) 2535-082X



YEAR III, ISSUE 4/2019

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 III, ISSUE 4 / 2019**

# 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 Biffl, 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 Univercity 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 |

# C O N T E N T S

## THEORETICAL FOUNDATIONS OF SECURITY

**MECHANISMS FOR ENSURING THE REGION'S TECHNOLOGICAL SECURITY STRATEGY**
Doctor of Economic Sciences, Professor, Zhavoronkova G., PhD (Economics), Associate Professor, Zhavoronkov V. ..... 123

**COMPERATVE EVALUATION OF MODELING AND SIMULATION TECHNIQUES FOR INTERDEPENDENT CRITICAL INFRASTRUCTURE**
Associate professor Dimitrov D.L., Ph.D. ..... 128

**ASSESSMENT OF NEUROTECHNOLOGIES: THE QUEST FOR SOCIAL AND PERSONAL SECURITY**
Eng. Ivana Lacková Miroslava Kováčová ..... 132

**RISK PERCEPTION BY STUDENTS: CASE OF FACULTY OF SECURITY ENGINEERING, UNIVERSTIY OF ZILINA**
Ing. Titko Michal, PhD., doc. Ing. Mária Hudáková, PhD. ..... 136

## NATIONAL AND INTERNATIONAL SECURITY

**ORGANIZED CRIME ACTIVITIES ON THE ILLEGAL MARKET AND SECURITY IMPLICATION*i***
Full Prof. Bošković G. PhD., M.Sc. Dmitrašinović S. ..... 140

**SYSTEMIC APPROACH TO THE DEVELOPMENT OF SECURITY SYSTEMS FOR CRITICAL INFRASTRUCTURE PROTECTION AS A RESEARCH METHODOLOGY APPLIED AT THE CENTER OF COMPETENCE *QUASAR***
Chief Assistant Dr. Eng. Panevski V.S. ..... 144

**HUMAN SECURITY AND CROSS-BORDER COOPERATION**
Assistant Prof. Dafinka Sidova, Ph.D. ..... 148

**ELECTRONIC ADMINISTRATION OF UNMANNED AVIATION WITH PUBLIC KEY INFRASTRUCTURE (PKI)**
M.Sc. Vránics D. F., Dr. Palik M. PhD, Dr. habil. Bottyán Zs. PhD ..... 152

**COUNTERACTION TO SMOLDERING CRISES IN THE NATIONAL SECURITY SYSTEM**
Markov N. ..... 156

**AN ATTEMPT TO SUMMARIZE THE PSYCHOLOGICAL PORTRAIT OF PERPETRATORS OF ORGANIZED CRIME**
Assoc. Prof., Madzharov, E. A.,PhD ..... 158

**DEFINING THE STRATEGIC CENTER OF GRAVITY OF HEZBOLLAH**
Ph.D. student: Faisal Warikat ..... 161

## INFORMATION SECURITY

**CROSS-SITE SCRIPTING ATTACKS AND THE SECURITY OF WEB APPLICATIONS**
Ass. Prof. Dr. Petar Halachev ..... 163

**CODE CONTRACTS VS INPUT VALIDATION**
L.Petkova. PhD ..... 167

**ON THE POWER TO DETECT ERRORS OF ONE ERROR-DETECTING CODE**
Prof. Ilievska N. PhD. ..... 170

## TECHNICAL FACILITIES FOR ENSURING SECURITY

**SECURITY OF THE B-MSS – THE NEW CHALLENGE FOR THE SATELLITE SYSTEM DESIGNERS**
Assos. Prof. M. Sc. Demirev V.B. Ph.D ..... 174

**OPTIMIZATION OF THE DESIGN OF FRAGMENTATION WARHEADS FORMING AN AXIAL FLOW OF PREFORMED FRAGMENTS**
MSc Petkov, P.S. and Assist.-Prof. Dr. Eng. Tumbarska, A. ..... 178

**MODIFIED PETRURGICAL MATERIALS BASED ON SEDIMENTARY ROCKS USED FOR BALLISTIC PURPOSES**
Prof. L. Lakov PhD, Senior Assist. Prof. Kr. Toncheva PhD, Assist. Prof. Marieta Gacheva ..... 182

# MECHANISMS FOR ENSURING THE REGION'S TECHNOLOGICAL SECURITY STRATEGY

Doctor of Economic Sciences, Professor, Zhavoronkova G., PhD (Economics), Associate Professor, Zhavoronkov V.,
PhD (Economics), Associate Professor, Klymenko V.,
National Aviation University, Kyiv, Ukraine
zhavor@ukr.net

***Annotation.*** *One of the key concepts that expresses essential processes in techno-economic development is the technological way of production. The concept has been forming for a long time. The economic opportunities of the regions are differentiated due to the presence of different geographical, historical, demographic and other factors. The article identifies the author's concept of "technological security of the region" and the main reason for the state's technological security. The main provisions for the development of the concept of technological security strategy of the region are proposed. It is determined that the region's technological security strategy is a long-term plan of action aimed at ensuring the technological interests of the region, finding and creating appropriate reserves to prevent, avoid and eliminate the risks, threats and threats to the development of the region. The mechanism of implementation of the technological security strategy of the region includes state regulators and market institutions, as well as their influence on the processes taking place in the innovation and technological sphere. It is proved that the main purpose of the mechanism of implementation of the technological security strategy of the region is to create conditions with ensuring a high level of technological security and with observance of social, labor and environmental standards for the population of the region. The priority tasks of scientific and technological support for the solution of technological security problems in the region is the innovative policy of both the state and the regions, on the development and application of high technologies, protection of intellectual property rights, creation of human resources of science and knowledge bases subject to state protection. The strategic directions of state regulation of the development of economic and technological potential of the region for ensuring its technological security have been determined.*

***KEYWORDS****: TECHNOLOGICAL SECURITY OF THE REGION, TECHNOLOGICAL SECURITY OF THE STATE, REGIONAL DEVELOPMENT, TECHNOLOGICAL SECURITY STRATEGY.*

## *1. Introduction*

One of the key concepts that expresses essential processes in techno-economic development is the technological way of production. It is such a complex that forms the basis of economic development during a certain and long historical period of socio-economic progress. The concept has been forming for a long time [1].

It is well known that the economic opportunities of regions are differentiated due to the presence of different geographical, historical, demographic and other factors. Therefore, ensuring the technological security of the region is often associated with the realization by the region of absolute and relative advantages in the possession of various resources (labor, financial, natural, scientific and technological).

Here is the author's definition of the concept of "technological security of the region" - this is the state of its research, innovation, technological and production-technical potential, which allows to ensure the proper functioning of the regional economy, sufficient to achieve and maintain the competitiveness of products and economic entities, and also guaranteeing financial autonomy and economic sustainability at the expense of their own intellectual and technological resources with simultaneous controlling their exports and facilitating the latest technologies to the region [2].

Significant differentiation in the levels of economic and technological potential of regional development poses a direct threat to the technological security of the state [3]. The main reason for this threat is the lack of an effective regional development policy in Ukraine, which has led not only to widening imbalances and aggravation of socio-economic problems in the regions, but also to a decrease in the level of technological security.

Lack of work on the correlation of national security and national regional policy, mechanism to promote the protection of national interests in economic and technological spheres, in the formulation and implementation of national regional policy, require the development of appropriate proposals and recommendations.

## *2. Concept of Region's Technological Security Strategy*

The necessity to fulfill the constitutional requirements for the implementation of the functions of government bodies the regional level aimed at ensuring technological security requires the development of the concept of a technological security strategy of the region, which should include the following main provisions:

- methodology of forming the strategy for ensuring the state technological security at the regional level;
- priority of the goals of ensuring state technological security and its regions in the long-run period;
- methodology of diagnostics of technological security of the region and organizational principles of its application;
- classification of risks, threats and dangers that will facilitate the process of their diagnosis, prevention and neutralization;
- criteria and indicators of the state technological security of the region, mechanisms of correspondence of status indicators for the analysis and evaluation of the integrated index of technological security of regions;
- mechanisms for implementing strategic plans, programs, etc. ensuring the technological security of the regions;
- monitoring and control of technological security of the region.

The region's technological security strategy aims to protect research, production, technological and innovation activities from external and internal hazards and to ensure the economic stability of the region, which can be defined as an opportunity for effective control by regional authorities of the use of their own intellectual resources and inflowing resources from the outside for the economic growth of the region, as well as ensuring the competitiveness of business entities.

The region's technological security strategy is a long-term plan of action aimed at securing the technological interests of the region, finding and creating appropriate reserves to prevent, avoid and eliminate the risks, threats and dangers of the region's development. The concept of the technological security strategy of the region is a sequence of actions of the authorities, which includes a set of functions, principles, methods and tools, as well as targeted comprehensive programs for ensuring technological security at the regional level (Figure 1).

The objects of the region's technological security strategy are:

- scientific and technical activities and education;
- information, and information and communication technologies;
- environmental technologies;
- industrial production based on the latest technologies and techniques;
- energy using promising and unconventional technologies and resources;

- combined transport infrastructure for diagnostics and monitoring of technological infrastructure objects;

- Systems for protection of high-tech objects from accidents and catastrophes.

In order to increase the efficiency of innovative development [4], it is necessary that the main directions of formation of the technological security strategy of the region ensure the utilization and reproduction of economic and technological potential. It should be noted that for the development and successful implementation of this strategy it is necessary to achieve a high level of information and analytical support, which is a prerequisite for the technological development of the region.

The main goals of the technological security strategy of the region should include:

- cardinal improvement of technological infrastructure as a basis for sustainable development of the region, its integration into national and international markets;

- ensuring the technological independence of the region and the competitiveness of regional products;

- positive balance of payments related to technology transfer;

- providing safeguards for protection of vulnerable technological systems and intellectual property;

- institutional and structural changes in the field of material production of high-tech objects;

- reducing technological risks of environmental pollution;

- integration of basic technologies into a single, highly efficient system.

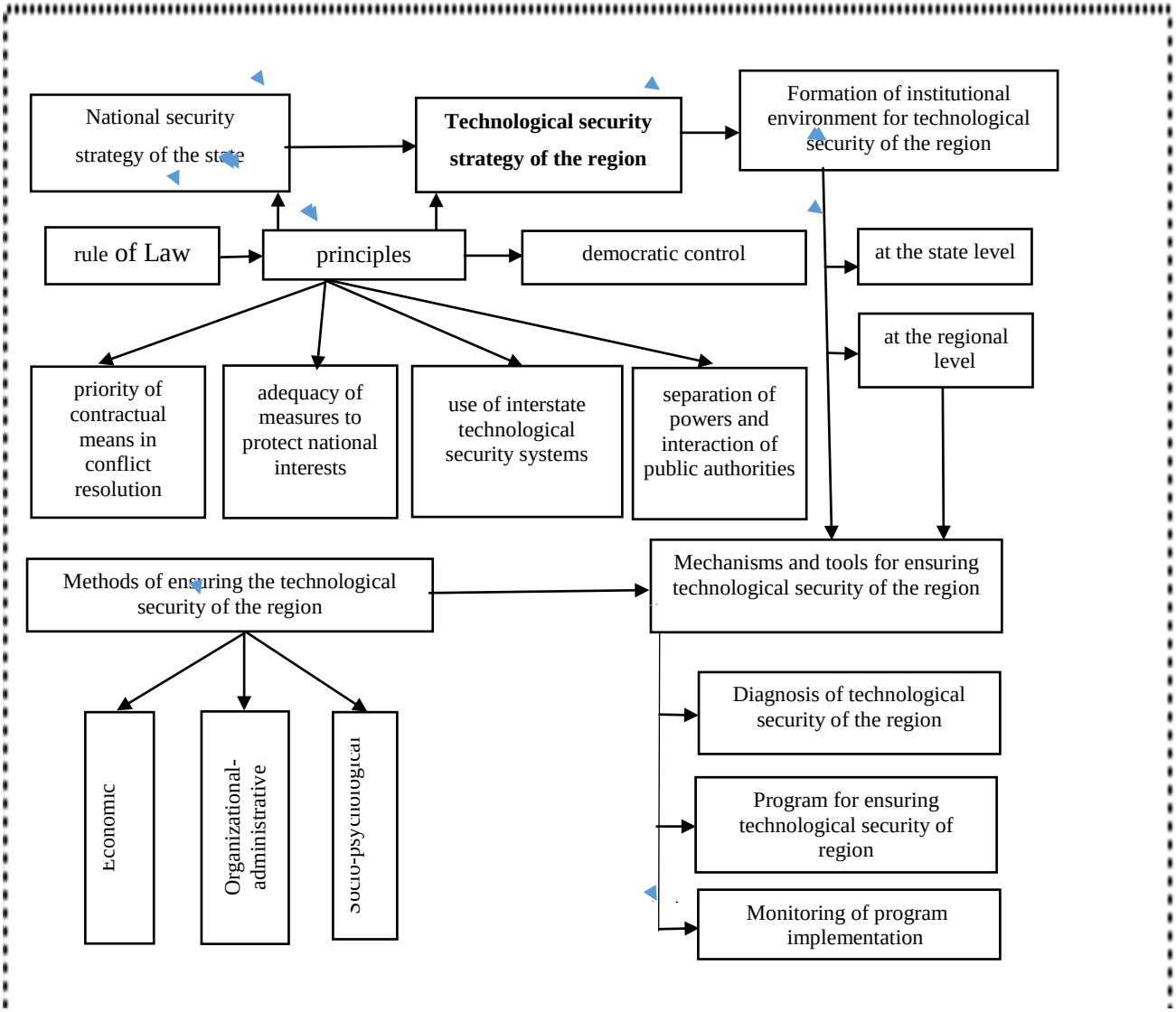



***Figure 1*** *The concept of the technological security strategy of the region*

The objectives of ensuring the economic security of a region are specific, desirable indicators of the individual determinants of technological security of the region, which must be achieved within a certain period of time.

Thus, in order to increase the level of technological security of the region (industry), the state policy of forming an innovative model of economic development should include the implementation of the following measures:

-promoting the promotion of the widespread use of the world's intellectual, scientific output in all spheres of the national economy through the development and implementation of economic incentives to create an effective institutional environment [5];

-expansion of the domestic market of unrealized technologies and increase of effective demand for domestic R&D results;

-stimulation of comprehensive development of the intellectual potential of the individual, which implies the active influence of the state at all stages of human capital formation in the region;

-improvement of the system of indirect methods of state influence on the development of high-tech industries sector [6];

-creation of a stable functioning legal framework for generating a highly productive knowledge resource, which needs to be addressed in the education and science system, and complete the formation of an effective system of protection of intellectual property rights.

## *3. Mechanisms for Implementation of the Region's Technological Security Strategy*

The lack of a mechanism for implementing a regional technological security strategy that takes into account the protection of national interests in the economic and technological spheres in the formulation and implementation of national regional policy requires the development of appropriate proposals and recommendations. Ensuring balanced and innovative development of the regions in the context of the technological security strategy of the region determines the following principles in developing the implementation mechanism and measures [6]:

-innovation, that is, structural restructuring of the economy of the regions, taking into account the peculiarities of their economic and technological potential;

-equality of regions at the expense of improvement of the state strategic, budgetary and financial planning;

-economy and integration of research activity of regions with the use of territorial division and cooperation of labor;

-development of cross-border and inter-regional economic relations on the basis of industrial cooperation and integration, creation of industrial-financial groups, scientific and technological clusters;

-balance of interests between the scientific center and the regions, clear delineation of liabilities, rights, powers and responsibilities and their legal formulation, introduction of contractual relations between them;

-improving the development of targeted state support programs for regions with regional research programs, ensuring their balance and coordination at all stages;

-prioritizing the development of regions of strategic technological importance for Ukraine;

-development of criteria and mechanisms for providing state support for innovative development of regions;

-responsibility of regions for failure to comply with measures in national research programs;

-efficiency of inter-regional distribution of scientific work, improvement of the mechanism of use of intellectual labor resources, promotion of formation of their regional labor markets;

-the reliability of the regional system for preventing and counteracting the emergence and spread of threats to the technological security of the region.

For the implementation of the strategy of technological security of the region, it is important to direct the process of strategic decision-making to ensure the optimal balance of profits and costs of economic entities, so that the content of economic risk management would be viewed from the standpoint of providing a system of measures not only to neutralize the negative consequences of problem situations, but also to prevent them occurrence.

The mechanism of implementation of the technological security strategy of the region is a functional and institutional way of organizing the interaction of elements of the economic system in order to coordinate and manage economic and technological processes to ensure the realization of national and regional economic interests, prevent threats to technological security, eliminate their consequences and achieve given level of technological security.

The main starting points of the formation of the mechanism of technological security strategy implementation were determined:

-system incorporates different models of regulation – from traditional to full liberalization model;

-production and commercial activities of knowledge-intensive enterprises are adapted to regulatory regimes and market conditions;

-mechanism is based on a systematic approach that integrates the requirements of international legal documents, market mechanisms, national regulatory processes and the elements of interrelated production activities;

-transition from the traditional to other regimes of regulation takes place in stages, taking into account changes in the parameters of supply and demand, market pricing, competitive environment based on the assessment of the economic efficiency of commercial activities of knowledge-intensive enterprises in market conditions;

-interests of the state, developers and consumers of high-tech products (as a priority) are agreed.

The mechanism of implementation of the technological security strategy of the region includes state regulators and market institutions, as well as their influence on the processes taking place in the innovation and technological sphere (Figure 2) [7].

The main purpose of the mechanism for implementing the strategy of technological security of the region is to create conditions in which the scientific and technological sphere of the region can develop in a stable, cost-effective manner, while ensuring a high level of technological security and respecting social, labor and environmental standards for the population of the region.

There is no doubt that without the proper logistical support and maintenance it is impossible to create the conditions for the development of efficient high-tech production. Now, taking into account domestic and foreign experience, it is necessary to set the task of creating their own high-tech means of high-tech production.

The outcomes of Ukrainian producers of high-tech products, competitive in foreign markets, depends on the cost of labor; total costs of the enterprise for high-tech raw materials, materials, components, as well as upgrading production facilities, putting into operation machines and equipment for technological processes [8].

Thus, the main directions of further technical re-equipment of science and production should be:

- effective state support for the development of the market of material and technical resources of high-tech production through pricing policy, introduction of preferential loans, improvement of the system of financial leasing, creation of favorable conditions for wide attraction of domestic and foreign investments;
- modernization of production capacity taking into account modern economic and technological potential, with improved technical and operational indicators and reduction of operating costs for production of high-tech products;
- computerization and production automation, etc.

The fulfillment of these requirements will not only ensure the implementation of the state innovation policy, especially in terms of bringing the country to the stage of sustainable economic development and the revival of domestic knowledge-intensive production, but will also increase its profitability and competitiveness of innovative products, increase employment and improve the standard of living, which will guarantee high level of technological security of both countries and regions.

## *4. Management of Region's Technological Security*

The technological security of the region is managed through an appropriate system. In the future, the system of technological security management in the region will be understood as an organized set of entities: state bodies, public organizations, officials and individuals, united by the goals and objectives of protecting national and regional interests that carry out concerted activities within the legislation. The main functions of this system are: creation and support in the readiness of forces and means of ensuring technological security; management of the security system; implementation of planned and operational activities; participation in national and international security systems.

Since the formation of the technological security management system in the region requires institutional support, it is necessary to create a certain organizational structure that will be responsible for its formation. At the region level, we propose to create a special unit at the regional state administration, which will include its own system of management, monitoring and control over the implementation of the technological security strategy of the region.

Thus, the formation of a mechanism for ensuring technological security in the region should take into account two main factors: 1) creating the conditions for the transition to an innovative path of development; 2) the emergence of motivation in economic entities to activate innovation and technological processes. The first factor can be attributed to the process of formation of technological infrastructure as an independent element of the economic system. In the second case, it is about stimulating innovation and technological activity.

The development of a mechanism for the implementation of the technological security strategy of the region will allow: to create the organizational and legal basis for the construction, operation and development of the technological security system; to identify and evaluate potential threats; to participate in international, national technological security systems. The monitoring of the the region should be carried out by an institutional and organizational monitoring system.

The main activities that will enhance the technological security of the region include: the development of fundamental, university and corporate science; creation of technological infrastructure; commercialization of innovations and retraining system, formation of economic and technological potential of the region, etc. In view of this, the main task of the regional authorities in enhancing technological security is to promote the influx of new technologies into the region with simultaneous control of their exports for the economic growth of the region, as well as to ensure the competitiveness of economic entities.

## 5. Conclusions

Significant differentiation in the levels of economic and technological potential of regional development poses a direct threat to the technological security of the state. The main reason for this threat is the lack of an effective regional development policy in Ukraine, which has led not only to widening imbalances and aggravation of socio-economic problems in the regions, but also to a decrease in the level of technological security.

The priority tasks of scientific and technological support for the solution of technological security problems in the region is the state and regional innovative policy on the development and application of high technologies, protection of intellectual property rights both in the domestic and foreign markets, creation of human resources of science and knowledge bases, including special ones, which are subject to state protection.

Strategic directions of state regulation of development of economic and region technological potential for ensuring technological security should be: providing conditions for production activity of subjects of innovative entrepreneurship in order to increase production volumes in accordance with the needs of Ukrainian society and the world market; regulation of the price affordability of products for the consumer.

## *6. References*

1. Zhavoronkova G., Zhavoronkov V. The technological imperative and technological safety in the systems of national security of the state // International scientific journal «Security and future». 2/2018. P.63-66.

2. Жаворонкова Г.В. Стратегія технологічної безпеки регіону / Г.В. Жаворонкова // Вісник Національного технічного університету «ХПІ»: зб. наук. праць. Тематичний випуск: Технічний прогрес і ефективність виробництва. – Харків: НТУ «ХПІ», 2012. – №15. – С.89-95.

3. Регіональні інноваційні системи України: стан формування та розвитку в умовах інтеграційних процесів : монографія / за ред. д-ра екон. наук професора Л.І. Федулової; НАН України, ДУ «Ін-т екон. та прогнозув. НАН України». – К., 2013. – С. 554-602.

4. Urmas V. How to improve the National Innovation Systems of catching-up economies? / Urmas Varblane, David Dyker, Dorel Tamm //Trames. – 2007. – Vol. 11, No 2. – Pp. 106–123.

5. National Security Throuh Technology: Technology, Equipment and Support for UK Defence and Security [Electronic resource]: Presented to Parliament by the Secretary of State for Defence by Command of Her Majesty February 2012 / Ministry of Defence. – 63 p. – Electronic text data. – Access mode: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27390/cm8278.pdf (date of the application: 08.09.2019). – Title screen.

6. Саліхова О.Б. Високотехнологічні виробництва: від методології оцінки до піднесення в Україні / О.Б. Саліхова; НАН України, Ін-т екон. та прогнозув.. – К., 2012. – 624 с.

7. Жаворонкова Г.В. Напрями забезпечення реалізації технологічної безпеки регіону / Г.В. Жаворонкова // Економіка і прогнозування. – 2012. – № 3. – С. 135-144.

8. Zhavoronkova G. Institutionalization of innovative and social strategy of regional development /G. Zhavoronkova**,** V. Zhavoronkov, V. Klymenko // Economika i orhanizatsiia upravlinnia: Collection of scientific articles. Vol. № 3 (23). – Vinnitsa: DonNU 2016. – P. 49-59.

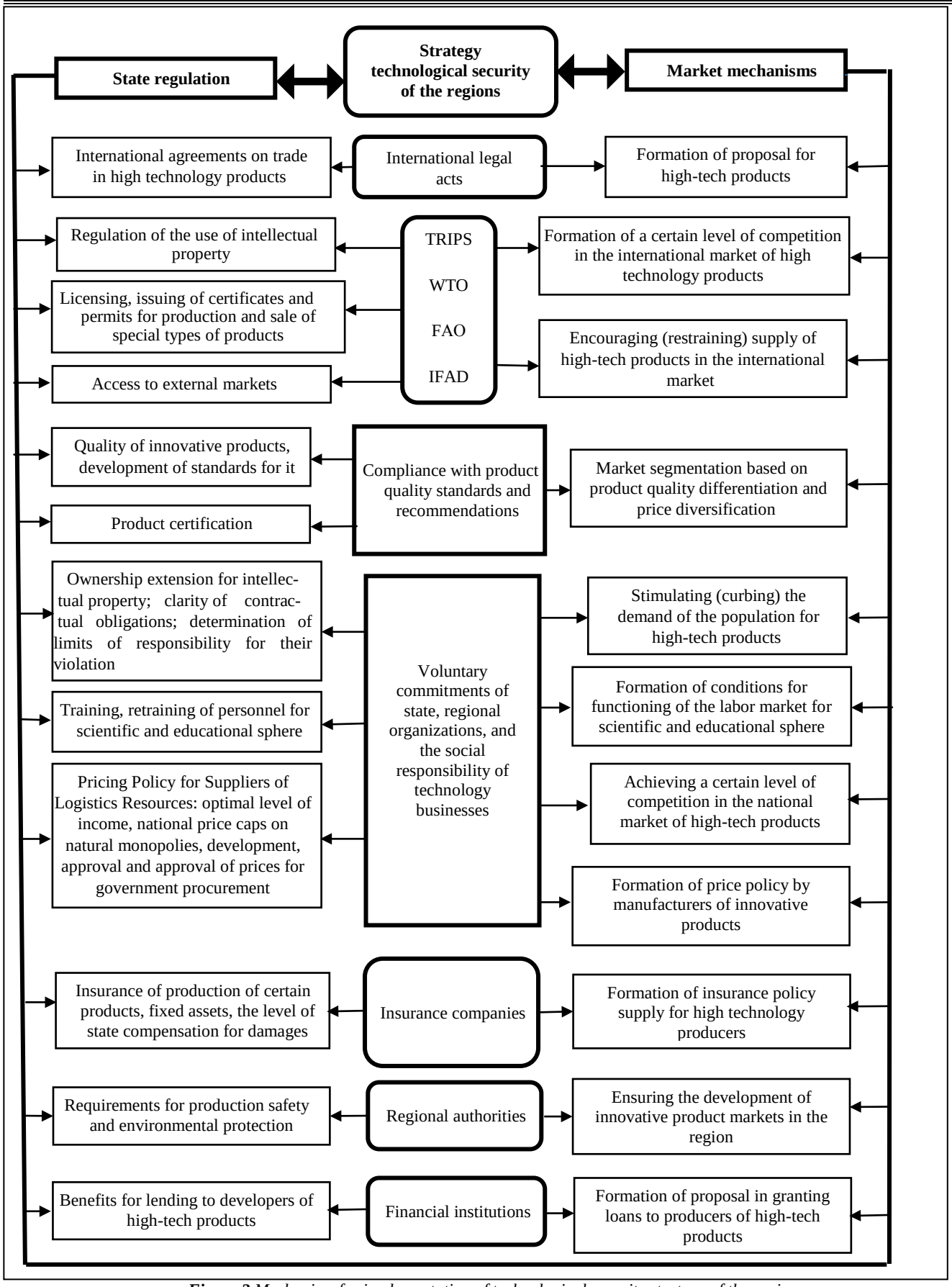



***Figure 2*** *Mechanism for implementation of technological security strategy of the region*

# COMPERATVE EVALUATION OF MODELING AND SIMULATION TECHNIQUES FOR INTERDEPENDENT CRITICAL INFRASTRUCTURE

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:*** *There are numerous methodical approaches to model, numerically analyses or/and simulate single systems' behavior. However, modeling interdependencies between different systems (so called system-of-systems) and to describe their complex behavior, necessarily by simulation, is still an unresolved issue.*
***KEYWORDS:*** *CRITICAL INFRASTRUCTURE, VULNERABILITY, RISK ASSESSMENT, RISK MANAGEMENT, MODELING AND SIMULATION*

## *1. Introduction.*

As is well known, a number of studies and attempts have been made to characterize the various infrastructures and their degree of criticality. Critical infrastructure analysis can focus on different goals (reliability, risk, vulnerability, etc.), may vary in scope (sectoral, system-wide or system-of-systems) and may follow different methodological approaches and / or competing approaches.

These facts usually create confusion and require comparative analysis with respect to different models and analytical techniques. The content of this report aims to establish clear criteria for such a comparison, with a focus on vulnerability of critical infrastructures and evaluation of modeling and simulation techniques.

These methodologies have been described and evaluated relatively successfully with respect to their overall suitability for critical infrastructure vulnerability assessment, with an emphasis on the role and impact of interdependencies, and for the purposes of the report will address some of the key benchmarks (e.g., " Types of interdependencies ";" Types of simulation events ";" Consequences of events ";" Need for data ", etc.)

On the one hand, critical infrastructures are defined as "a network of independent, large-scale, human-created systems that work together and in sync to produce a steady flow of essential goods and services" [1] and are also essential on economic development and social well-being. They are subject to a number of potential asymmetric threats (technical, intentional or unintentional - human-caused, physical, natural, cybernetic) that pose a risk to them.

Critical infrastructures are highly interdependent, both physically and in widespread use of information and communication technologies. In other words, critical infrastructures are characteristic of highly dynamic and complex systems, dependent on each other to varying degrees and with different intensities [2]. At the systemic level, critical infrastructure is viewed from a technical point of view as a problem for the security of logistical systems and their software.

Ensuring the continuous functioning of critical infrastructure sites, ie reducing the vulnerability to acceptable levels is one of the ideas behind the creation of the Competence Center "Quantum Communication, Intelligent Security and Risk Management" (Quasar) in the Republic of Bulgaria under Project BG05M2OP001-1.001-0006, funded by the European Union. Smart Growth Operational Program" [3].

On the other hand, we often define the vulnerability of critical infrastructure systems as gaps or weaknesses in their design, implementation, operation and / or management that make them susceptible to disruption / destruction, regardless of their ability to recover.

What does the term "vulnerability" mean in the context of critical infrastructure protection? Some researchers define the concept of vulnerability as follows: vulnerability is a manifestation of the inherent states of a system that make it susceptible to failure or loss. It is well described by a set of state variables that describe the weaknesses of the system and how they interact to cause loss due to a devastating event.

## *2. Requirements for methods and approaches for making comparative analysis.*

### *2.1 Need for a systematic study.*

There are a number of studies that call for and confirm the importance of understanding, modeling and simulating interdependent critical infrastructures.

Although there are studies on available techniques, it is clear that they lack comprehensive, clear criteria for assessing applicability. Therefore, the question of how to model the complex behavior of "system-of-systems" or which methods are best suited to accomplish this task is still open and provides a basis for finding additional approaches.

### *2.2 Objectives for comparative evaluation of techniques.*

The main objective is to select, describe and evaluate techniques with a view to their adequacy in the preparation of vulnerability analysis of infrastructure interdependencies.

To this end, it is logical to distinguish between obvious and hidden vulnerabilities - reviewing the results of a statistical data analysis helps to identify obvious weaknesses if the statistics show some clear problem areas / scenarios - e.g. conclusions based on "power outages". Other indications of apparent vulnerability are operating errors, emergency procedures, etc.

A more accurate analysis must be adopted if the evaluation of the readings is not "clearly outlined" and the underlying hidden vulnerabilities are still expected. Particular attention should be paid to interdependencies within or between systems, and simplified procedures prepared at an earlier stage (including "system separation") should be evaluated.

For these and other reasons, as we know, on January 24, 2003, US President George W. Bush created the Department of Homeland Security (DHS), one of the main tasks of which is to conduct a comprehensive analysis of critical infrastructures as well as an organized national planning and protection process - CIP [4].

The $ 35 billion project was launched as a result of the terrorist attack on the two World Trade Centers on September 11, 2001 and accelerated the process of exploration for modeling and simulation of critical infrastructures. This fact has led to a significant increase in the intensity of research and, at the same time, the international interest in this field and the number of publications on these infrastructures.

Secondly, there are a number of inconsistencies in definitions and classifications that depend heavily on the scientific field. In the current scientific literature, recent methodological approaches are often incorrectly defined.

Therefore, the purpose of comparative evaluations of different techniques is to analyze the strengths and weaknesses of different methodologies, as well as to analyze, characterize and propose appropriate techniques for modeling and simulating interdependent critical infrastructures[5].

## *3. Basic benchmarks*

### *3.1. Basic modeling approaches.*

Two main approaches to modeling and simulation have been described in the contemporary literature: Interdependence analysis, which includes qualitative approaches, and Systematic analysis, which rather covers quantitative approaches.

*Interdependence analysis [6]* - includes qualitative techniques for identifying critical infrastructures and for analyzing the characteristics and dimensions of their interdependence. These techniques include extensive use of expert interviews, roundtables or seminars, appropriate questionnaires, and more. Models are relatively easy to build, but are limited to items explicitly examined by experts and are not able to systematically detect hidden critical elements and their respective vulnerabilities.

*Systems Analysis [7]* - uses approaches that are more quantitative techniques, can identify hidden dependencies, and are strongly associated with computer simulations. These techniques require sophisticated computer architectures as the approaches are very detailed and time consuming.

### *3.2. Modeling and simulation strategies.*

The most important aspect of evaluation, not only in the development of optimal modeling and simulation strategies, is the decision to choose between two basic strategies: bottom-up and top-down, and a combination of both can be applied:

*Bottom-up approach*: the whole system is described starting with the individual parts [8]. This type of approach usually refers to complex adaptive systems that can be built on the results of interacting elements, such as basic entities with specific locations, capabilities, and memory that reflect their identification.

The bottom-up approach is generally considered to be more intuitive and less error-prone than the top-down approach and can usually be implemented with relative ease in software code. While the components are well defined, it can produce very accurate output. However, the exceptional use of the bottom-up approach can neglect significant system-level constraints, especially when used in the absence of sufficient input;

*Top-down approach:* The distinctive feature of the top-down approach is its focus on the overall properties of the system, combined with its relatively easy applicability. However, this approach is less appropriate than the bottom-up approach of capturing lower-level factors, such as problems with system-specific issues, as well as details of the implementation of specific details that tend to accumulate quickly and can significantly influence the evaluation [9].

### *3.3. Types of interdependencies.*

This criterion describes the different types of infrastructure dependencies. Each type has its own characteristics and effects on infrastructures, but usually modeling and simulation approaches do not take into account all types of dependencies. There are four main types of interdependencies between critical infrastructures [10]:

*Cyber interdependencies* - connect infrastructures to each other through electronic, information links; outputs of information infrastructures are inputs to other ones;

*Geographic interdependencies* - observed when elements of an infrastructure are in close spatial proximity. For example, a damaged underground water main may cause interference to power lines and optical communication cables in a collector - the so-called "causal failures";

*Physical interdependencies* - describe the material flow between different infrastructures. Such interdependence arises from a physical connection consisting of input and output streams. For example, electrical systems and information and communication technologies (ICTs) are physically interdependent. Electricity supplies ICTs while they can control and manage the operational data for the proper functioning of that energy production, transmission and distribution;

*Logical interdependencies* - dependencies that exist between infrastructures but do not belong to the above types. Often logical dependencies are caused by human decisions and actions taken in both political and public fields, e.g. the volume of oil and gas supplied is highly dependent on the political decisions of OPEC members.

### *3.4. Types of simulation events.*

A significant challenge related to modeling and simulation techniques may be to create a "what-if" scenario for critical infrastructure interdependence analysis. The following information for a subsequent event is possible [11]:

*Incident:* The incident describes a wide range of accidental and potentially damaging events, such as natural disasters, whose origin is usually outside and independent of the system;

*Attack:* A series of potentially damaging actions taken by an intelligent opponent to achieve certain results. Cyber-attacks include penetration, probing and denial of service. In addition, the idea itself can have as much impact on a system as if it actually materialized. A system that takes an overly defensive position because of the threat of attack can significantly reduce its functionality and reallocate excessive resources to monitor the environment and protect the assets of the system;

*Failure*: A potentially damaging event due to defects in one system or in an external element on which the system depends. Damage can result from incorrect design, production and operational (human) errors, corrupted data, etc.

### *3.5. Consequences of events.*

Interdependencies affect the effects of single or multiple failures or interruptions within interconnected systems. Different types of dependencies can trigger feedback circuits that have accelerating or delaying effects on systems response, as observed in dynamics.

The following types of events are distinguished:

*Cascading events:* A situation where an adverse event occurs in one part of the infrastructure and the effect of them in the other parts. An example of a cascading event in electrical systems is the congestion and interruption of a transmission line from the electricity grid [12]. In that case, its load will be shifted to a nearby electricity transmission line, which - even without additional load - can also be switched off and without electricity leaving much of a region;

*Increasing events:* can be seen as a consequence of cascading events, ie. the resulting "problem" in one infrastructure can affect other infrastructures, causing them to malfunction or interrupt into other infrastructure by increasing the burden or recovery time. This in turn may affect the recovery of the service provided by the infrastructure initially affected;

*Common cause events*: Dependent failures in which two or more malfunctions occur simultaneously or within an interval of time as a direct result of the common cause. For example, fiber optic cables and power lines often share a common funnel in tunnels or over bridges. If this tunnel or bridge is damaged by a fire caused by a road accident, it may also disrupt telecommunications and energy supply as a result of disruption of spatial traffic [13];

*Closed events*: damages that do not have a cascading, escalating or general impact on the infrastructures under consideration.

### *3.6. Need for data (information).*

This criterion requires the availability of general information on the quantity and quality of input required to apply the appropriate methodological approach[14]. Input data includes information about the topology and layout of the system, the flow of the product, its operation, as well as numerical values of the modeling parameters.

The availability of inputs and their quality are essential for the practical use of modeling and simulation approaches; lack of sufficient data is a widespread problem in scientific analysis and may reduce the use of sophisticated approaches. Two dimensions are known:

*High:* The methodological approach is highly dependent on the high quality and quantity of input data to provide applicable modeling approaches. These factors must be ensured before such an approach is implemented.

*Low:* The methodology can be applied with discrepancies in the quality or quantity of input submitted to ensure reliable results. In these cases, a minimum quality or quantity of information is required.

### *3.7. Observation scenarios.*

Depending on the criteria described above, the observation scenarios relate to modeling and simulation techniques, baseline data and available information. Interdependent models can be grouped into the following main categories, depending on the scenarios required:

*Vulnerability assessment*: the purpose is to identify and quantify vulnerabilities in the system. Vulnerability is defined as the likelihood of an accident, successful attack or failure. Vulnerability assessments can be seen as an extended analysis of element damage;

*Malfunction Analysis*: Human errors can cause disruption to infrastructure systems. Modeling and simulation techniques can provide systematic analysis and reliability theory by identifying and analyzing the most common failures. The failure analysis provides the identification of the critical components, helps to improve the system, as well as to understand the connections between the critical nodes of the network as a whole.

### *3.8 Modeling and Simulation Paradigms.*

Modeling and simulation of dynamic processes lead to changes in the state of the system / its components. Simulation is an "execution" process that takes over the model through discrete or continuous changes in its state over time "[15]. A combination of the two paradigms is also possible.

*Discrete Events:* The state is changed by "jumps". The models consist of entities (units of motion), resources (elements that provide the service), and control elements (elements that determine the states of entities and resources);

*Continuous events:* These describe changes in the state of continuous functions. If the material or information being simulated can be described as continuously moving rather than in separate steps or packages, it is most appropriate to use the continuous event paradigm. The simulation is based on solving differential equations that describe the development of the system.

### *4. Conclusion.*

Although there are many techniques currently available for analyzing the individual critical infrastructures, no universal method or common interdependent modeling and simulation tool is widely accepted, and therefore discussions continue on the suitability of different approaches.

In terms of the dynamics of a person's systems, a serious argument is offered that offers ways of possibly improving the analysis, security, functional understanding, and strategic management of critical infrastructure systems that will assist in the perception of the operation of the system and its changes over time.

Because efficiency reflects the state of resources or the provision of services, strategies can be developed and tested when modeling systems before policies are developed, physically implemented, and security decisions addressed to deviations from normal functioning, the presence of unexpected challenges.

With all of this in mind, it is quite possible to develop adverse scenarios that can be applied to critical infrastructure models to demonstrate such threats and vulnerabilities that would impact business continuity, accident management, and their consequences, attacks on information systems, cybercrime, protection of key sites against attacks, chemical, biological and radiological hazards, provision of water and food, identification and protection of adjacent droughts It is logical to apply maritime infrastructure to models of critical infrastructure.

Modeling system dynamics allows not only to monitor normal activity, but also functionality in adverse change and its effect on critical infrastructure systems as a whole, since without this knowledge critical infrastructure owners / operators will be very difficult and unprepared for all that is likely to happen.

Effective modeling of critical infrastructure would enable both public administration and critical infrastructure owners to analyze, identify and effectively manage and maintain stability, security and access to that infrastructure by developing solutions to unexpected or other sustainability challenges.

### *Literature*

[1]. Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection, Washing-ton D.C., 1997;

[2]. Eusgeld, I., Kröger, W., Sansaviini, G., Schläpfer, M., Zio, E." Investigations on the role of network analysis and agent-based modeling within a framework for the vulnerability analysis of critical infrastructures" (working paper). 5. Juni 2008 48/50;

[3]. Panevski V., Competence centres and intelligent security systems in Bulgaria, International Scientific Journal "Security & Future", YEAR III, ISSUE 1, НТС по машиностроене, 2019, ISBN:WEB ISSN 2535-082X, 14-16 2019;

[4]. Department of Homeland Security. "National Infrastructure Protection Plan", DHS, (2006);

[5]. Georgiev Nikolai, "Quality indicators for protection systems", International Journal of Economics, Commerce and Management, vol VI, issue 4, ISSN 2348-0386, 2018,p.836-842;

[6].S. Rinaldi, "Modeling and Simulating Critical Infrastructures and Their Interdependencies", Proceedings of the 37th Hawaii International Cconference on System Science. Hawaii, (2004);

[7]. S. Panzieri, R. Setola, and G. Ulivi. "An approach to model complex in-terdependent infrastructures", Universita "Roma Tre", Roma. (2005);

[8]. S. Lee "A frame work for supporting bottom up ontology evolution for discovery and description of Grid services". Expert systems with Applications, 32(2):pp.376-385, (2007);

[9]. V. Temnenco. "Software Estimation", Enterprise-Wide. (2007);

[10]. S. Rinaldi, J. Peerenboom and S. Kelly "Critical Infrastructure Interdependencies", IEE Control Systems Magazine, (2001);

[11]. R.J. Ellison, N.R. Mead, T. A. Longstaff and R. C. Linger. ,, The Survivability Imperative: Protecting Critical Systems", The Journal of Defense Software Engineering, (2000);

[12]. I. Dobson, B. Carreras, V. Lynch and D.E. Newman. ,, Complex systems analysis of series of blackouts: cascading failure, criticality, and self-organization", Bulk Power System and Control, Cortina d' Ampezzo, Italy, (2004);

[13]. F.M. Marshall, D. M. Rasmuson and A. Mosleh. "Common Cause Failure Data Collection and Analysis System", 1, U.S. Nuclear Regulatory Commission, NUREG/CR-6268, (1998);

[14]. Georgiev Nikolai, "Quality criteria for critical infrastructure protection systems", International Journal of Economics, Commerce and Management, vol VI, issue VI, ISSN 2348-0386, 2018, p. 265-271;

[15]. Borshchev, A., Y. Karpov, and V. Kharitonov, Distributed simulation of hybrid systems with AnyLogic and HLA. Future Generation Computer Systems, 2002. 18(6): p. 829-839 (2002).

# ASSESSMENT OF NEUROTECHNOLOGIES: THE QUEST FOR SOCIAL AND PERSONAL SECURITY

Eng. Ivana Lacková Miroslava Kováčová[1]
[1]Faculty of Economics and Management – Slovak University of Agriculture in Nitra, Slovak Republic.
mirkakovka@gmail.com

***Abstract:*** *Neurotechnologies are devices that by integrated technical (neurostimulation, neuromodulation, and neuroimaging) means change activity of the human brain. There are many different types of neurotechnologies, such as neural-control interfaces, brain-machine interfaces, direct neural interfaces, auditory brainstem implants, retinal implants, predictive brain implants, deep brain stimulators, transcranial stimulators. These devices can in various degrease monitor, coordinate and alternate brain activity and therefore neurotechnologies could fundamentally change the future of relationship between humans and technology. The article proposes new conceptual ramifications of neurotechnological devices, examines history of neurotechnological devices and points to possible threats and dangers of neurotechnologies for social and personal security.*

**Keywords**: NEUROTECHNOLOGIES, NEUROMODULATION, NEUROSTIMULATION, SOCIAL SECURITY, PERSONAL SECURITY

## *1. Introduction*

Neurotechnological devices (for short NTDes) are brain computer interface technologies that can monitor, coordinate and change brain activity. There are many different types of NTDes, for example neural-control interfaces, direct neural interfaces, brain-machine interfaces. There are also many different devices, such as auditory brainstem implants, retinal implants, predictive brain implants, deep brain stimulators, transcranial stimulators, which all can be categorized as NTDes. There are also various administrative aspects of NTDes. The devices can administrate stimulation of electrochemical brain activity according to some external quantitative requirements (direct synchronization or desynchronization of brain activity). The NTDe can also administrate mediation of external qualitative transformations in coordination with the subject's brain activity (direct mediation of brain activity). Via advanced brain computer technologies NTDes could be also used for administrative enhancement of direct brain-to-environment and direct environment-to-brain purposes (direct coordination and enhancement of brain activity). It is therefore not surprising that NTDes are not only technologically sophisticated tools, but also represent new set of possible challenges to social[1] and personal security. In what follows I will therefore briefly sketch the history of NTDes, the modal operational classification of NTDes and the security implications of operational use of neurotechnolgies.

## *2. Conceptual classification and history of neurotechnologies*

The working mechanism of NTDes is crucially depended on various techniques that directly or indirectly monitor structures and reactions of the brain (neuroimaging), operationally classify and evaluate neuronal data (processing unit), and effectively modulate the nervous system's activity (neurostimulation). The success and operational use of NTDes is therefore the result of decades of technical and scientific advances in neuroscience, information science, electro engineering, biotechnology and medical sciences. For this reason there are many possible types and technologies of NTDes. The modern usage of NTDes is however mainly tied to the successful experimental and clinical use in neurological research.

### *2. 1 First generation NTDes*

The real world functional history of NTDes begins in the 1980s with the experimental and therapeutic use in the field of neural medicine. First generation NTDes were neurostimulators used mainly for deep brain stimulation in Parkinson's disease patients. In these kind of settings NTDes have been successfully used to treat some of the symptoms of Parkinson's disease [2]. First generation NTDes were using neuromodulation techniques to directly alter brain activity in accordance with the respective quantitative therapeutic requirements (synchronization of brain activity). The goal was to effectively stimulate neuronal activity which could lead to a decrease or increase in brain, motoric or other functions (deep brain stimulation). This type of stimulation is regulated within the delivery of low-voltage electrical signals to a certain part of the brain. The exact mechanism of action of neurostimulation is not known, however it is believed that it can lead to desynchronization of abnormal oscillatory activity of neurons [3]. The neurostimulation is therefore mediated by an electrical signal, which is delivered by an electrode surgically placed in the respective part of the brain. The electrode is connected via a cable to the NTDes neurostimulator (internal pulse generator) as the source of stimulation. The neurostimulator is then usually implanted in the area under the skin near the collarbone, chest, or under the skin over the abdomen. The required range of electrical signals of the stimulation can be adjusted using another external computational instrument of the respective NTDe (access control device). Such adjustment is made by a researcher, physician. The variation is being determined according to the condition of the particular subject. In some cases, the subject maintains the ability to perform fine tuning of the actual adjustment on the access control device within the researcher, physician specified range of parameters. The targeted interference with a particular part of the brain therefore depends on the goals of the device. For example, in the case of Parkinson's disease, the most common target is the subtalamic nucleus, but interventions are also undertaken in other parts of the brain [4].

The fundamental advantages of first generation NTDes are their functional simplicity and operational reversibility. The electro stimulation is operationally reversible, because the frequency and intensity of the neuromodulation are manually preprogrammed and controlled. Take away the preprogramed signal and the stimulation stops. Functional simplicity means that the activity of this device is exclusively unidirectional and open, since the preprogramed signal is directed only from the device to the respective brain region. First generations of NTDes are thus based on the classical open loop system scheme. The output stimulation has no direct influence or direct effect on the control action of the input signal of the respective NTDes. The stimulation automatically and constantly follows the input command preprogramed by the definitions of the relevant goal. This approach can be successful in many administrative settings. First generation NTDes are nowadays medically used for treatment of Parkinson's disease, essential tremor, intractable pain, dystonia, obsessive–compulsive disorder and depression [4]. Current research is focused on possible clinical usage in treatment of anorexia, addiction and wide range of other psychological disorders [5]. However every technology has its price. In the case of first generation NTDes functional simplicity

[1] For definitions of social security see for example article by Wojnarowska-Szpucha S., Social security determinants [1].

limits not only the relevant modes of neurostimulation, but also control. A major disadvantage of any open loop system is its inability to respond to any relevant feedback. First generation NTDes cannot self-correct any errors of the electro stimulation output. The device is poorly equipped to handle dynamic disturbances or changes in the bioelectrical and biochemical conditions of the brain. This in many cases may reduce the ability to complete the desired goal. The brain is a dynamic system and therefore the appropriate technology should also be dynamic. This problematic aspect of first generation NTDes has led to research for new and innovative operational schemes.

### *2.2 Second generation NTDes*

The second generation of NTDes reflects the dynamic approach to brain computer interface relations by incorporating aspects of the closed loop system. The neurostimulator sends different neurostimulation signals to the appropriate part of the brain. These signals are monitored by neuroimaging technologies (monitor). The information obtained from the neuroimaging tools is then analyzed by the predictive processing unit. The results of this analysis affects the transmission of the form and range of other signals (calibration). The activity of second generation NTDes is thus multidirectional (mediation of brain activity). Different forms of electro stimulation signals are directed not only from the NTDe to the respective part of the brain (first generation NTDes), but also from the brain to the device via neuroimaging (information) and the processing unit (calibration, second generation NTDes). This operational scheme based on the idea of a closed loop system therefore increases the information, calibration, and hence the administrative function of the respective NTDe.

Second generation NTDes are currently experimentally used mainly for the treatment of pharmacologically resistant epilepsy [6]. The reason is that epilepsy is a neurological disease characterized by recurrent seizures. Transient cerebral dysfunction (seizure) is caused by abnormal brain activity. Various internal causes (e.g., metabolic disorder), external causes (e.g., situational stress), or combinations thereof (e.g., injury) may cause abnormal brain activity. A specific feature of epilepsy is that these causes cause seizures only in some cases. Stimulation of certain brain activities may therefore decrease, but also increase the likelihood of transient brain dysfunction. For this reason the use of open loop NTDes (first generation) is not safe and therefore not suitable for this kind of stimulation. Second generation NTDes which are operating on the closed loop system scheme however can operationally calibrate the required neurostimulation and mediate various and different brain activity patterns. The monitor (neuroimaging) records normal and abnormal brain activity of the subject. For example, an integrated electroencephalograph (EEG) is used to record brain activity. The EEG sends information to an external processing unit. The processing unit predicts the likelihood of a seizure by means of specially programed algorithm. This information is then transmitted to the implanted neurostimulation device. Neurostimulation on the basis of mediated or direct (processing unit) assignment performs appropriate (electrical) stimulation or inhibition (neurostimulator). The whole process is recorded by the monitor (neuroimaging) and the data is sent back to the predictive processing unit, thus closing the loop of the whole system (closed loop NTDe).

The main advantages of second generation NTDes are their stability and operational flexibility. This means, that this type of NTDe doesn't require continuous control and manual calibration of the system. If the system works, than the external interference is limited. The second generation NTDes are however also potentially very flexible. These types of NTDes can be used not only for the treatment of epilepsy, but also for many other means and purposes. In theory any attribute caused by recognizable (neuroimaging) and changeable (neurostimulation) brain activity can be administered (predictive processing unit) by this device. In this sense it is therefore not surprising that for example in the United States, Italy, Spain and Poland second generation NTDes are already being experimentally used to limit impulsive aggressive behavior of subjects with severe psychiatric disorders [6].There are also descriptions of NTDes schemes that could be used in the administration of various other social and personality characteristics and disorders [7].

Stability and operational flexibility comes with a tax. Second generation NTDes are prone to disadvantages which are derived from the functional specialization of these types of NTDes. Effective administration is linked to the specific problem for which the respective NTDe is used. This means that second generation NTDes are theoretically multi-operational, but more or less unifunctional systems. The system can learn (predictive processing unit) to adapt to only one specific task at a time. This means that the learning process is internally closed only to the use of the respective closed loop functionality (e.g. treatment of epilepsy). There are many beneficial uses for this kind of neurotechnology, however there are also many uses that are out of reach for this kind of NTDes. The brain is a multifunctional system and therefore some of the appropriate technologies should be also multifunctional.

### *2.3 Third generation NTDes*

Research into the third generation of NTDes is focused on the problem of multifunctional use of NTDes. The problems of second generation NTDes are dependent on the limitations of the learning input and output [8]. The solution is therefore theoretically pretty straightforward. Artificial intelligence has synergic effects [9]. Artificial intelligence could be used to adapt the NTDe not only to the specific brain (electrochemical brain patterns) but also to the environment as a whole. This could greatly enhance not only the learning ability of the respective NTDe, but also the potential multifunctional ability of NTDes and the brain (coordination and enhancement of brain activity). Third generation NTDes would utilize neurostimulation characteristics of the classical or advanced neurostimulator devices. Neuroimaging technologies would monitor different types of (environmental) inputs which could be than processed through the processing unit connected to the (real or virtual) environment. Adaptive deep learning algorithms (artificial intelligence) of the processing unit would link the environmental factors in the right interpretational language, which could be than used to transfer instructions to the neurostimulation device. This scheme would therefore mediated a direct brain-to-environment and direct environment-to-brain connection. Third generation NTDes could therefore enhance usability by mirroring functionalities (mirror system) of the brain and environment (brain signals, environmental signals), thus bridging the gap between (in philosophical terms) mind and matter and potentially leading to the so called age of transhumanism [10, 11, 12].

At present time third generation NTDes are partially only theoretical devices. There isn't currently any prototype that could be classified as a safe and functional full third generation mirror system NTDe. The successful use of first generation NTDes, promising results from the experimental use of second generation NTDes and some predictions about advances in biotechnological research are giving hopes for the possible technical functionality of third generation NTDes. Some expected breakthroughs in material sciences, informational science, computational science and neuroscience therefore could lead to technologies, which are required for the necessarily multifunctional ability of third generation NTDes. This isn't just an academic and futuristic speculation. The talks about robust brain computer interfaces (third generation NTDe) are nowadays step by step going mainstream. The most vocal popular proponent for this generation of technologies is for example E. Musk with his Neuralink project [13]. There are also many other companies, institutions and countries that bet on the possibility of a real world, real time brain computer connection. Projects for third generations of NTDes are on the way for example in Facebook [14], Emotive [15], DARPA [16] and EU [17]. This economical and research investment is proportional not only to the so called new tech hype, but also to the many possible uses of NTDes. Third generation NTDes will be multifunctional devices and therefore could (in principle) be used

for medical, therapeutic, industrial, informational, defense and other purposes. The possibilities of a direct fusion between brain and environment via computer are almost endless. The brain could directly manipulate with almost any kind of environment and the environment could directly mingle with almost any kind of brain (direct brain-to-environment and direct environment-to-brain connection, coordination and enhancement of brain activity). Some authors therefore even speculate that third generation NTDes could effectively merge biological and artificial intelligence and lead to super-intelligence, or the so called singularity [18, 19]. At the moment this scenario seems to be farfetched, but this doesn't change that fact, that there could be many different exciting and interesting possible uses for NTDes.

## *3. Personal and social security of neurotechnologies*

Every application of new technologies comes not only with different sets of opportunities, but also with new and different sets of problems. As in every technology the successful use of NTDes is dependent on the security of the relevant technology. The operational use of NTDes is however closely linked with the idea of a direct and intimate integration of this technology with human subjects. In this sense NTDes are not only interesting because of the technological security, but also on the ground of social and personal security.

In their simplest analytical form NTDes are devices that can (or could) monitor, coordinate and change brain activity. Based on this, we can then define three functions relevant to the problem of social and personal security: The information function, the predictive function and the automation function of NTDes. The information function of NTDes is used to record unchanged and altered (after impulse) brain activity (information). It is characterized by different ways of obtaining, recording and disseminating the necessary information (neuroimaging). The predictive function is used to process and evaluate information. It is characterized by a classification of activities that can alter brain activity (predictive processing). The automation function is used to process information and implement results that were obtained and based on the prediction (neurostimulation). The automation function is therefore characterized by an operation that changes brain activity. This change can occur autonomously and automatically (closed loop, mirror system).

It's not surprising, that the automation function of NTDes is of particular concern here, because it could have direct implications for personal security, social security and the problem of human autonomy [6]. For example, it is conceivable that the automation function of NTDes could limit, completely prevent, or override subject's free decisions. It is therefore understandably that such real, or just hypothetical usages would not only drastically decrease the operational employment of NTDes, but also increase public distrust in the safe and secure use of NTDes. If NTDes had just such uses and purposes, than it is certain and right that their public evaluation would be negative, or rather straightforwardly dismissive. The so called slave to the machine problem, however, has its limits. Every sincere technology assessment should focus not only on failures, but also opportunities. Focusing only on catastrophic consequences can lead to two problematic aspects, which could make it impossible to adequately assess the case of NTDes. The first problem comes with the potentially dangerous ignorance about the many beneficial uses of NTDes. The second problems consist in the potentially perilous unawareness to other possible negative aspects of NTDes.

### *3.1 The problem of force*

It should be assumed that, if NTDes are (or will be) used to directly manipulate the brain activity of a subject who doesn't agree with the procedure (or may reasonably be expected to do so), than such use of NTDes is an unacceptable case of a threat to personal and social security. However this doesn't mean that the automation which comes with NTDes is always unacceptable and unsafe.

The classical line of reasoning against the automation function of NTDes is the argument, that all automated interventions of NTDes are potentially dangerous, because they may in some direct sense conflict with the subject's decisions. The main problem with the automation function of NTDes is that it reduces the subject to a passive recipient. This passivity prevents the subject from realizing his own will even in potentially beneficial cases. Thus, NTDes would ultimately undermine personal and social security.

The main problem with this popular argument against NTDes is the misunderstanding that automation necessarily implies coercion. In some cases automation doesn't necessarily imply a disagreement of the subject with the intervention. Criticism of NTDes sometimes operates by confusing meanings between automation, force, coercion and disagreement. These terms are neither linguistically synonymous nor necessarily linked. Automation itself is neutral in nature. Neutrality subsists in the fact, that automation does not necessarily imply subject's disagreement with the correct procedure. There are conceivable situations where, for good reasons, the subject agrees with the automated intervention of technologically secure NTDes. Such situation may be, for example, the automatic administration of pulses and brain activity that ensure a continuous good and beneficial medical condition of the subject (e.g. treatment of epilepsy). However, there are also conceivable situations where the subject disagrees with some kind of automation, for some other reasons. Nevertheless, this doesn't change the fact that the automation automatically doesn't lead to coercion. The problem of the security of the closed loop NTDes is therefore not in the problems of the device (and function) itself, but only in the real and objective assessment of the concrete situation.

### *3.2 The problem of prophecy*

Argumentation for some of the aforementioned negative and positive aspects of the actual automation use of NTDes doesn't mean, that the other functions of this device may be automatically socially and personally secure and without a problem. The predictive aspect of NTDes doesn't lead to the problem of the automated control. The predictive part of NTDes simply gives a choice to the subject. However, in some cases, the prediction may fail. A broken or corrupted NTDe could provide the subject, or the implementation part of the NTDe, with information that are false. Acting (or not acting) according to false information is manipulation of the subject and therefore dangerous to the subject and his environment. This situation could also represent a serious threat to social security and public trust for NTDes. This type of problem is mainly technological in its nature. The solution consists in adequate design practice and appropriate technical regulations.

The problems of predictive function of NTDes may also occur if the device is functioning properly. The predictive function of NTDes would seem to increase the subject's information capabilities. In some cases, however, the quality of the information does not necessarily lead to more correct decisions. People simply don't make only rational decisions. The reason for this is not only incorrect information, but also the human nature of information processing [20, 21]. Sometimes information processing can be random or arbitrary. The randomness of this process is increased by the number of steps (operations) that lead to a certain decision. Increasing the number of decision-making steps increases the likelihood of a decision being random. Randomness can subsequently lead to the possibility of an incorrect decision. The information paradox is also confirmed by some studies on decision theory [6]. Some subjects that cooperate with artificial information assistants achieve in some cases statistically worse decision-making results, than subjects that do not cooperate with the assistant at all. But it's not the technology's fault. The results of some subjects cooperating with the assistant are even statistically worse than some of the proposed solutions of the artificial information assistant itself. The randomness of human behavior leads to the fact, that people can make bad choices even with the right incentives and information. The more this right information is conveyed the greater is the risk, that it will not be properly evaluated and implemented by

the subject. This in turn means that a better effect would be achieved if NTDes were not used at all, or if these devices were fully automated. Thus, in some cases, predictive function of NTDes may not increase personal security. In some cases open and transparent predictive information may lead to decisions that are incorrect for the subject, his environment and society.

### *3.3 The problem of secrecy*

The last function of NTDes is the information function. On its own this function prescribes nothing, but only informs. The information just ensures that the subject and the NTDe are "aware" of their condition and functions. Information increases knowledge of the subject and the operational functionality of the NTDe. The relevant information therefore increases the possibilities for the right kind of procedure. If the relevant procedure is the main goal, then the information function of NTDes doesn't seem to be problematic. Other problems arise when we concern other aspects of the whole situation. The main problem could be privacy and new privacy standards. The efficient information function of NTDes will fundamentally change some of our assumptions about relevant privacy settings. For some technological and other research reasons NTDes not only use, but also record information. This recording is used for the right kind of calibration of the entire loop of the respective NTDe and for the classification of other future uses of different kinds of NTDes. The successful use of NTDes therefore requires that some of the information about the subject's brain activity are not, in the strict sense, private anymore. Thus in some cases the NTDes may significantly undermine the subject's own privacy.

The problem isn't only the possibility of invasion of the subject's privacy, but mainly the possibility of exploiting personal data which are of a completely new and different kind. This data and information are integral parts of every subject and therefore essential characteristic of everyone's personal and societal security. Recognizing this fundamental qualitative difference of NTDes can helps us to understand the new qualitative aspect of protection that this exciting technology requires.

## *4. Conclusion*

NTDes compromise promises for technologies that could fundamentally challenge and change the relationship between the human brain and the human world [22]. NTDes therefore represent novel cognitive tools, which could revolutionize not only many aspects of scientific inquiries, but also some new aspects of anthropological self-understanding. First and second generation NTDes are now successfully used in the treatment of many serious and chronic diseases, psychological disorders and personal disabilities. We should therefore not assume that the current scientific research is focused only on some theoretical, hypothetical and controversial applications. Too much focus on some negative visions makes it impossible to see that NTDes are (and could be) used to help many people, which are in great need. However, this doesn't mean that NTDes are entirely unproblematic. NTDes belong to technologies with high security ramifications. Concerns about the security of machine-driven behavior are understandable, but automation and prediction doesn't automatically mean negative and false personal coercion. The automation and predictive function of NTDes is crucially determined by the information function of NTDes. Without a critical amount of the necessary information, neither prediction nor automation is possible. The sensitive nature of this information implies that the solution should consist in the critical analysis of the information security of NTDes. Neurotechnology of brain activity isn't only a quest for knowledge, but also a quest for social and personal security of knowledge.

## *5. References*

[1] Wojnarowska-Szpucha S., Social security determinants, Security & Future, 2 (4), 2018, pp.158-162.
[2] Miocinovic, S., Somayajula, S., Chitinis, S., Viterk, J. L., History, applications, and mechanisms of deep brain stimulation, Journal of the American Medical Association neurology, 70 (2), 2013, pp. 163-173.
[3] Popovych, O. V., Tass, P. A., Control of Abnormal Synchronization in Neurological Disorders, Frontiers in neurology, 5 (268), 2014.
[4] Odorčák, J., HÍbková mozgová stimulácia, identita a perdurantizmus, Filozofia, 69 (6), 2014, pp. 472-481.
[5] Gardner, J., A history of deep brain stimulation: Technological innovation and the role of clinical assessment tools, Social Studies of Science, 43 (5), 2013, pp. 707–728.
[6] Odorčák, J., Neuroadministratívné zariadenia a autonómia subjektu, Filozofia, 73 (6), 2018, pp. 449-457
[7] De Ridder, D., Langguth, B., Plazier, M., Menovsky, T., Moral Dysfunction: Theoretical Model and Potential Neurosurgical Treatments. In: Verplaetse, J., De Schrijver, J., Vanneste, S., Braeckman J., (eds.) The Moral Brain. Essays on the Evolutionary and Neuroscientific Aspects of Morality, New York: Springer, 2009, pp. 155-183.
[8] Valuch, J. M., Neurotechnologie, mozek a souvislosti, Praha: Galaxy, 2006.
[9] Radulov, N., Artificial intelligence and security. Security 4.0, Security & Future, 3 (1), 2019, pp. 3-5.
[10] Bobryk, J., Transhumanizm, coginitive science I wyzwania, Studia Socjologiczne, 3 (214), 2014, pp. 9-27.
[11] Klinec I., Transhumanizmus. Budúcnosť človeka v 21. Storočí. (Available online) http://www.akademickyrepozitar.sk/sk/repozitar/transhumanizmus-study-text.pdf
[12] Odorčák, J., Kritika transhumanistickej kritiky Friedricha Nietzscheho, Filozofia, 65 (6), 2010, pp. 552-556.
[13] Musk, E., An integrated brain-machine interface platform with thousands of channels, BioRxiv, 2019. (Available online) https://www.biorxiv.org/content/10.1101/703801v1
[14] Facebook, Imagining a new interface: Hands-free communication without saying a word. (Available online) https://tech.fb.com/imagining-a-new-interface-hands-free-communication-without-saying-a-word/
[15] Emotive, The Introductory Guide to BCI, (Brain-Computer Interface). (Available online) https://www.emotiv.com/bci-guide/
[16] Miranda, R. A., Casebeer W. D, Hein A. M., Judy J. W., Krotkov E. P., Laabs T. L, Manzo J. E., Pankratz, K. G, Pratt, G. A, Sanchez, J. C, Weber, D. J., Wheeler T. L., Ling G. S., DARPA-funded efforts in the development of novel brain-computer interface technologies, Neurosci. Methods, 244, 2015, pp. 52-67.
[17] Bauernfeind, G., Brunner, C., Müller-Putz, G., Steensel, M., Otal, B., Pichiorri, F., Schettini, F., Real, R., Blefari, M., Höhne, J., Poel, M., D1.4 - BNCI Horizon 2020 – Roadmap, 2015.
[18] Vinge, V., The Coming Technological Singularity: How to Survive in the Post-Human Era, In: Landis, G. A. (ed.) Vision-21: Interdisciplinary Science and Engineering in the Era of Cyberspace, NASA Publication CP-10129, 1993, pp. 11-22.
[19] Odorčák, J., Kopírovanie zabíja identitu osoby, Filozofia, 70, (5), 2015, pp. 367-377.
[20] Mráz, M., Urbanovičová, O., Findura, P., Prístavka, M., Use of information systems to support decision making according to analysis machines, Mechanization in agriculture & Conserving of the resources, 65 (2), (2019), pp. 59-62.
[21] Szyłkowska, M., Human factor in the proliferation of threats, Security & Future, 2 (2), 2018, Issue, pp. 55-57.

# RISK PERCEPTION BY STUDENTS: CASE OF FACULTY OF SECURITY ENGINEERING, UNIVERSTIY OF ZILINA

Ing. Titko Michal, PhD.[1], doc. Ing. Mária Hudáková, PhD.[1]
Faculty of Security Engineering – University of Žilina, the Slovak Republic[1]

michal.titko@fbi.uniza.sk

***Abstract:*** *The perception, awareness and understanding of risk by the population are important factors for the society safety, which contribute to increasing the preparedness of the population for the effects of crisis events, whether natural, industrial, economic, social, or in enterprise. The article focuses on the analysis of the need for education of students in the area of risk management and crisis management. The research groups were only students, not the population in general. The results were achieved by analysing the current state of education at the Faculty of Security Engineering - University of Žilina and a partial statistical evaluation of the questionnaire survey among students of this faculty. The results indicate that the risk perception of students is relatively low and the need for education in this field is justified.*

**Keywords**: RISK, RISK MANAGEMNT, CRISIS MANAGEMENT, EDUCATION, QUESTIONNAIRE SURVEY

## *1. Introduction*

Perception, awareness and understanding of risk by the population are important factors in building the security of society [1]. The significance and relevance of these attributes is highlighted in situations where security is threatened or even compromised [2]. In such situations, it is usually too late for adequate response and preventive measures. Risk perception, awareness and understanding allow us to better prepare for the crisis of any nature and to take preventive measures against the perceived risk [3].

The perception and importance of understanding risk is primarily encouraged by education in this field as well as personal experience of exposure to risk, either directly to the citizen or indirectly to the close surroundings. As far as education is concerned, this issue is generally covered by the areas of education related to risk management and crisis management. In the Slovak Republic, this issue is covered by the system of civil protection within nationwide and systematic education in this field, for various age groups [4]. However, the issue of risk perception, risk assessment and, ultimately, management is far more extensive, as it should also address other areas of application, such as: economic, social or enterprise area.

The article focuses on the analysis of the need for education of students in the area of risk management and crisis management, which the authors perceive as a prerequisite of a prepared and resilient society [5, 6]. Faculty of Security Engineering - University of Žilina educates students in the field of security, which also includes the mentioned areas. Development trends and practice requirements currently increased the requirements for graduate preparedness and interconnection with practice, and therefore it is very important for universities to reflect the current trend, which is based directly on the demand of practice. Recent EU research confirms that graduates lack practical skills to help them adapt better in practice [7]. It is a difficult task for universities to ensure an adequate range of practice during their studies. In the field of security, the task is even more complicated, because practicing real situations where life, health, property or the environment is endangered is practically impossible and direct involvement of students in solution of such situations is also dangerous. Education at the Faculty of Security Engineering - University of Žilina therefore focuses primarily on mastering the basic principles of working with risks, from understanding risk through risk analysis and evaluation, to working with risk management and reduction of risks. The faculty also deals with situations where it is necessary to apply the principles of crisis management and solution of the situations. The scope of education covers areas from natural hazards, through industrial, social, to economic and entrepreneurship risks. There are considerable differences in approaches to such risks. Therefore, the idea is to create a separate field of study that would focus on risk assessment only in the entrepreneurship area. However, the article attempts to link students' overall perception of risk with their current possibilities at the faculty and to reflect needs of practical training in the field of risk management and crisis management.

## *2. Education at the Faculty of Security Engineering, Department of Crisis Management*

Faculty of Security Engineering educates security professionals in various areas. These include education in the areas of protection of persons and property, emergency services, critical infrastructure protection and crisis management. The Department of Crisis Management includes both crisis management in public administration and risk management as well. The department ensures education on three levels - undergraduate (Bc.), graduate (MSc.) and post-graduate (PhD.) [8].

The graduates of the study programme Crisis Management are experts with university education able to carry out the position of the crisis manager. The study programme also deals with the risk management area in the conditions of the public administration and entrepreneurial subjects. The graduates are able to assess (identify, analyse, evaluate) the risks and threats of the natural, social, economic and technological processes as well as to design procedures for their reduction.

## *3. Methodology*

The authors utilized the following methods for fulfilling the stated goal:

- analysis of the current state of education at Faculty of Security Engineering – University of Žilina with a focus on linking with practice
- questionnaire survey conducted on a sample of students of Faculty of Security Engineering – University of Žilina focusing on attitudes to risk and risk perception. The questionnaire was distributed to randomly selected respondents and students of faculty of security engineering (also small number of students of other universities) primarily in electronic form (several were also written). For the purpose of this paper only students' responses are investigated.

## *4. Results and Discussion*

### *4.1 Assessing the current risk-aimed education at Department of Crisis Management with relation to practical activities*

Currently, the Department of Crisis Management ensures implementing of risk-aimed practical activities for the university education in the following areas:

**1 The professional practice of the students**

The professional practice belongs to the activities organised by department every year. The students carry out professional practice in selected organisations (public administration institutions or companies) where they can gain new practice experiences from the security and safety field. After that students take part in professional practice under the auspices of the Ministry of Interior and its educational center. During this practice exercises, students have a possibility to confront their knowledge with experienced employees of Civil Protection and crisis management departments, and also with experts from the integrated rescue services.

**2 Experts from practice included in educational process**

The department is cooperating with different institutions (public administration or private) at different level. Experts from these institutions can within specialised subjects (courses) enrich the educational process with practical inputs (examples from practice), eventually increase the attractiveness of the studies. Another form of symbiosis is realised through consulting with experienced professionals from the private sector, as well as organising seminars and workshops for students [9].

**3 Linked thesis with practical problems**

Final thesis (Bc., MSc., PhD.) are realised in cooperation with the risk and crisis management authorities, as well as with business entities which are open to solving the issue of crisis and risk management in their enterprises. Currently, we can observe an increasing demand for cooperation and we still looking for new possibilities of cooperation.

**4 Excursions**

The department teachers' organise interesting excursions in the framework of their subjects, e.g.: (1) to manufacturing enterprises: The aim of these trips is to get students acquainted with the manufacturing process in a particular company, with quality control procedures from the point of view of risk management, as well as with systemic risk assessment in Occupational Health and Safety; (2) to expert institutions specific for the crisis management: e.g. the coordination centre of integrated rescue services, resistance shelters and warning networks of the civil defence or the warehouses of the Administration of State Material Reserves; (3) other excursions: Nuclear Power Plant Mochovce and Nuclear Waste Repository RAO Mochovce, etc.

**5 Projects with companies**

The department has been cooperating in the long term with Slovak Rails - ŽSR, ŽSSK a ZSSK Cargo, with companies QUADRIQ, s. r. o., L. Mikuláš, GOSSIS, s. r. o., Nitra, LYNX Košice. Other organisations include Nemak Slovakia, s. r. o. Žiar nad Hronom, Geodézia, s. r. o. Žilina, Distribúcia SSE, a. s. Žilina, Žilina Region, KROS, a. s. Žilina. There is an effort to include students into solving of these project, unfortunately, this represents the weakest spot in the department-company cooperation [9].

**6 Research centers**

The Department of Crisis Management has two specialised centers at its disposal. The first one is the Crisis Management Simulation Centre, which creates conditions for independent scientific and research activities. The center focuses on providing students with practical experience and skills in the form of simulation of crisis scenarios in a given situation. The other one includes research laboratories at the University Scientific Park designated to provide efficient and complex training of crisis management specialists with the help of software simulation technologies [10].

**7 Reversed cooperation**

A good example is a cooperation with the Ministry of Economy (and in connection with this with the company VUJE, a.s.) which provided us with software products for the lectures of the Subject Crisis Planning. After updating the information system in practice we succeeded in continuing this collaboration and we ensured the access to the new application of this system for our students. Another example is our cooperation with the company Bel Power Solution, s.r.o. in 2016 – 2017 by involving the students in the project of manufacturing a new product in the company. The student´s role was to implement the risk management to the project.

The department as well as the whole faculty of security engineering offers various opportunities for students where they can acquire practical experience in the field of crisis management and risk management. However, the extent and numbers of students involved, which are unfortunately limited, remain problematic and therefore we think that it is still necessary to deepen the link between theoretical teaching and practice.

## *4.2 Questionnaire survey*

A questionnaire survey was conducted between January 2019 and July 2019. A structured questionnaire was used, based on various sources [e.g. 6, 11, 12] and supplemented with questions and formulations that the authors considered appropriate with regard to the subject of the research. The questionnaire was distributed students of our university in electronic form. Number of participants was 360 (n). For the purpose of this paper are used results related to the flood risk only.

***Table 1:*** *General information about survey participants*

| General information | | Share [%] |
|---|---|---|
| Gender | Male | 52.39 |
| | Female | 47.61 |
| Living type | In flats | 36.67 |
| | In houses | 63.33 |
| Living place | Rural | 57.50 |
| | Urban | 42.50 |

First of all, the experience that students have with crisis events, such as floods, can have some effect on the subsequent perception of the risk of such events in the future. 39.72% (Fig. 1) of the respondents have not yet experienced any crisis phenomenon and it can therefore be assumed that their attitude to risk may to some extent be different from those who have already experienced the crisis event. The type of crisis event, as well as its severity, can also have a different impact on a person's attitude to risk in the future. We have also examined the severity of the impact of such events once they have experienced a crisis event. The results suggest that they have experienced mostly crisis events with low impacts and minor complications of everyday life. It was seldom a threat to life. Only 2.77% of students experienced a flood during which their lives or lives of their family members were at risk.

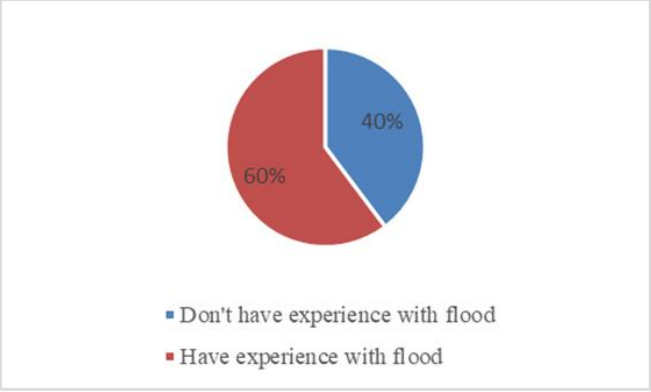



***Fig. 1*** *Percentage share of experience with crisis event (flood)*

In the section of experience exploration, we have also explored "How many students have ever been evacuated?" This tells a lot about the severity of the situation they have experienced, since

evacuation is only ordered in severe situations where it is impossible to save people otherwise from the area affected by a crisis event. The survey showed that only 8.05% of the students were ever evacuated (see Fig. 2), which is considerably lower rate compared to the experience with the occurrence.

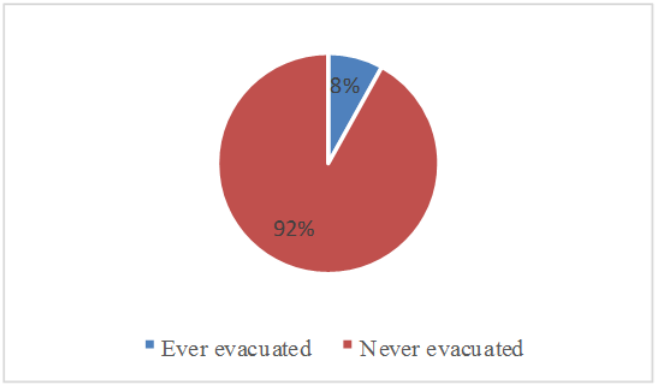



***Fig. 2*** *Percentage share of evacuated students*

Although they do not have much experience with serious impacts of crisis events, there is a presumption (statistics of the Ministry of Interior of the Slovak Republic - Fig. 3), which indicates that crisis events occurrence will increase and at the same time there will be more crisis event with more serious impacts. These figures are not only valid for the Slovak republic, but when we look at this issue broadly, this increasing trend is also seen in the neighbouring countries in Europe and worldwide [13, 14, 15, 16, 17]. There are, of course, considerable differences between countries, but the overall increasing trend is obvious, according to scientists [13, 14, 15, 16, 17].

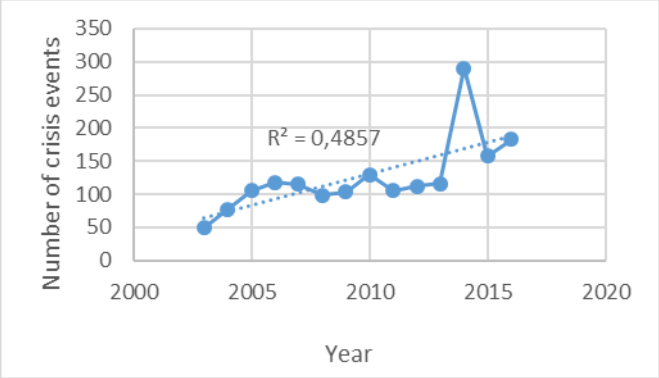



***Fig. 3*** *Development of the occurrence of crisis events in the Slovak Republic (adapted from [18])*

Therefore, we were interested in the view of students regarding the occurrence of crisis events in dependence to the development of the global environment and climate change. How do students perceive this development? The results are shown in Fig. 4, where it can be seen that approximately one third of them (34.17%) report either "slightly higher frequency" or "higher frequency" of crisis events occurrence compared to the past.

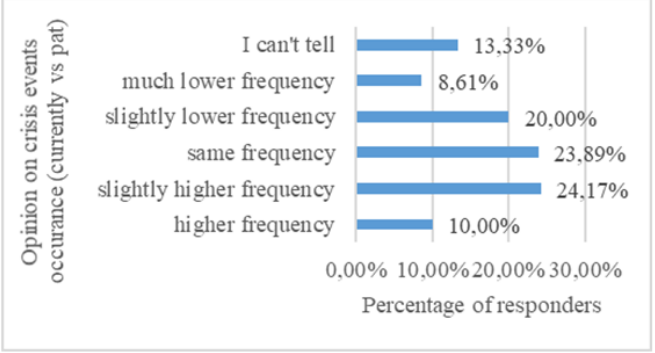



***Fig. 4*** *Opinions of students on crisis events occurrence*

Not only these facts, which indicated the current situation of risk awareness and preparedness among students, but also subjective evaluation of the level preparedness is important as well. This factor suggests that students think that they are prepared only moderately (almost half of the responses - 48.06%) and approximately a third (24.44% + 8.33%) think that they are prepared poorly or not at all (Fig. 5). The high share of responses within the middle level (3) may also be due to the fact that students do not know what is threatening them, what preparation would contain and therefore they decided to mark the middle level. It is possible that if we evaluate them individually and objectively, the results could be more inclined to lower preparedness.

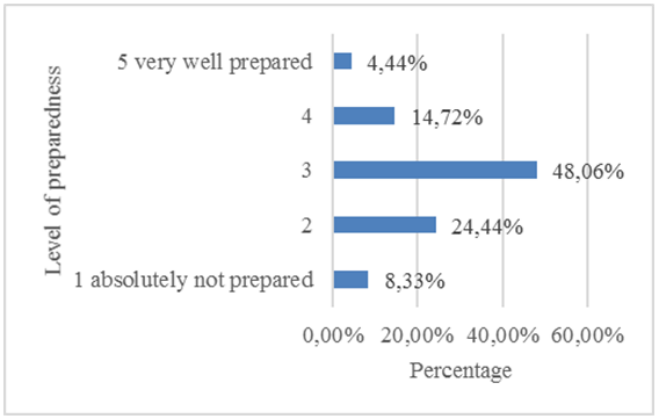



***Fig. 5*** *Preparedness level of students*

It is very positive that 81.67% of students showed interest in risk management or risk reduction, risk management and risk protection (Fig. 6). Nowadays, students preferred the more modern ways of obtaining this information (mainly electronic form) such as mobile applications, websites, information to mail, but there is still interest in a more common way of providing information by lectures and practical demonstrations.

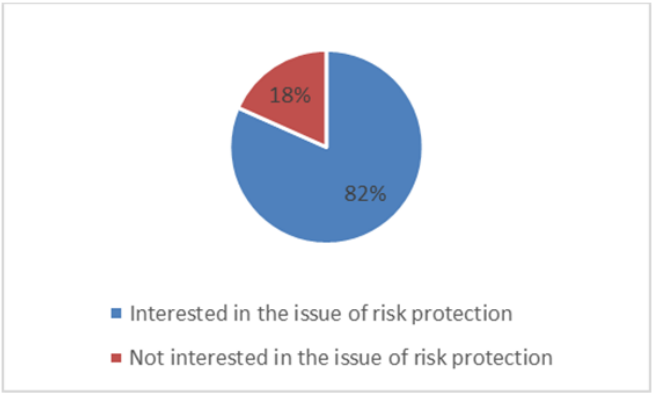



***Fig. 6*** *Interest in the issue of risk protection*

Initial results of the analysis of the current state of practical education at the Department of Crisis Management and the results of the survey show that although students have direct experience as well as practical teaching activities, self-assessment of their readiness is sceptical as well as opinions on security environment development. In principle, we see 2 explanations: (1) poor effectiveness or extent of practical education or (2) direct experience with crisis events was modest and did not change their attitudes and preparation for risks of different nature.

## *4. Conclusion*

In summary, it can be stated that students have some experience of risk effects, but they are unsure about their overall readiness for their manifestations. On the positive side, however, they are aware of their shortcomings in this filed and they would like to improve it

and learn more about the issue of risk management as practical as possible.

Demonstrated interest and current evolution of the environment suggest that the issue of risk management and crisis management is very attention-requiring. At the same time, it is a challenge for teachers and educational institutions to be able to train professionals in this field, as security is a rapidly changing area and requires a high degree of flexibility to address it comprehensively. Therefore, teachers should also be flexible and try to use modern teaching techniques and connect theoretical knowledge with practice more frequently.

Not only for teachers but also for public administration and enterprise entities alike, education, training and risk awareness-raising of various nature should be a priority in the field of raising the level of security. Practical education of students appears to be the desired phenomenon, and this highlights the importance of the study fields dealing with crisis and risk management. In this context, the idea of the Faculty of Security Engineering in Žilina is to continue in the established trend of applying practical elements to the teaching process and to try to find other ways to do these activities better in order to (1) improve perception, awareness and understanding of risk among students and (2) to ensure the prerequisites for employment in security and safety sector.

## *Acknowledgements*

Publication of this paper was supported by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic – VEGA No. 1/0805/18 „Establishing the principles and sequence of steps to measure the awareness and preparedness of the population to the risks of natural disasters and institutional grant project. “

Publication of this paper was supported by the Scientific Grant Agency: The project KEGA No. 030ŽU-4/2018 - Research of Risk Management in Enterprises in Slovakia to create a new study program Risk Management for the FBI University of Zilina.

## *References*

[1] Šimák, L. „Krízový manažment vo verejnej správe“, [Crisis Management in Public Administration]. Žilina, EDIS, 2016.

[2] Luskova, M. Buganova, K., 2011. The Importance of Effective Risk Management System in the Slovak Enterprises. In: WMSCI 2011: 15TH WORLD MULTI-CONFERENCE ON SYSTEMICS, CYBERNETICS AND INFORMATICS, VOL II. Int Inst Informat & Syst. 2011. p. 284–289. ISBN 978-1-936338-30-6.

[3] Holla, K., Mitasova, V., Pavlenko, T. Risk assessment model verification in hazardous industrial processes. 12th International scientific conference of young scientists on sustainable, modern and safe transport. Vol. 192, p. 324-329, 2017.

[4] Act of the National Council of the Slovak Republic No. 42/1994 Coll. on Civil Protection.

[5] UNISDR, Sendai Framework, Geneva: UN, 2015.

[6] Shapira, S. Aharonson-Daniel, L., Bar-Dayan, Y. Anticipated behavioral response patterns to an earthquake: The role of personal and household characteristics, risk perception, previous experience and preparedness In: International Journal of Disaster Risk Reduction. Vol. 31, pp. 1–8, 2018.

[7] Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions on a renewed EU agenda for higher education. Accessed on 27/10/2019, http://eur-lex.europa.eu/legalontent/EN/ TXT/?qid=1500025237385&uri=CELEX:52017DC0247

[8] Faculty of Security Engineering University of Zilina, Accessed on 10/10/2019, Available at:http://fbi.uniza.sk/

[9] Hudáková, M., Buganová, K., Dvorský, J. Increasing integration of practical activities to the higher education in the risk management in Slovakia”. in 10th International Conference of Education, Research and Innovation (ICERI 2017), Seville/ Spain: IATED Academy, pp. 996- 1003, 2017.

[10] Lovecek, T., Ristvej, J., Sventekova, E. Siser, A., Veľas, A. Currently Required Competencies of Crisis and Security Managers and New Tool for Their Acquirement, Proceedings of 3nd International Conference on Management Innovation and Business Innovation, Manila/Philippines, vol. 58, pp. 3-8, 2016.

[11] Appleby-Arnold, S., Brockdorff, N., Jakovljev, I., Zdravković, S. Applying cultural values to encourage disaster preparedness: Lessons from a low-hazard country In: International Journal of Disaster Risk Reduction. Vol. 31, pp. 37–44, 2018.

[12] Bird, D. K., Gísladóttir, G., Dominey-Howes, D. Different communities, different perspectives: issues affecting residents’ response to a volcanic eruption in southern Iceland. In: Bull Volcanol. Vol. 73, pp.1209–1227, 2011, DOI 10.1007/s00445-011-0464-1.

[13] Intergovernmental Panel on Climate Change. Climate Change 2014. Impacts, Adaptation, and Vulnerability. Part B: Regional Aspects. Cambridge University Press. New York

[14] European Commission. Directorate-general for european civil protection and humanitarian aid operations. Regional cooperation in the field of civil protection within the union. The EU overview of risks. p.10. 2019.

[15] O’connor, A. et al., Final Report, Part A, RAIN Project - Risk Analysis of Infrastructure Networks in Response to Extreme Weather. Applied Research Project 2015/2017, 2017.

[16] Guba-Sapir, D., Hargitt, D., Hoyois, P. Thirty years of natural disasters 1974 - 2003: The numbers. Brussel: Louvain-la-Neuve, 190 pp., 2004.

[17] Luskova, M., Dvorak, Z., Leitner, B. (2015). Impact of Extreme Weather Events on Land Transport Infrastructure. Transport Means 2015. Transport Means - Proceedings of the International Conference. pp. 306-309.

[18] Ministry of the Environment of the Slovak Republic. Stratégia adaptácie Slovenskej republiky na zmenu klímy [Adaptation strategy of the Slovak Republic to climate change]. 2018. Available at: https://www.minzp.sk/files/odbor-politiky-zmeny-klimy/strategia-adaptacie-sr-zmenu-klimy-aktualizacia.pdf#page=82&zoom=100,0,264

# ORGANIZED CRIME ACTIVITIES ON THE ILLEGAL MARKET AND SECURITY IMPLICATION[i]

Full Prof. Bošković G. PhD.[1], M.Sc. Dmitrašinović S.[2]
University of Criminal Investigation and Police Studies in Belgrade[1]
Ministry of the Interior of the Republic of Serbia[2]

goran.boskovic@kpu.edu.rs

**Abstract**: This work is inspired by the current problems of confronting organized crime, which in part controls illegal markets. Thus, it is also aimed at highlighting the most significant aspects of the research into illegal markets, whose knowledge enables the creation of effective strategic preferences in the fight against organized crime, whose actions have a number of negative implications for state security. Modern criminal organizations are profitable and market-oriented, and the methods of acting used are combined with the criminal and method of the operation of contemporary business organizations. The knowledge of the organization's specifics and functioning of illegal markets enables the proper selection of methods to more efficiently counter the destructive actions of criminal organizations that control the illegal market. In fact, the destructive action of criminal organizations reflects directly on the state of security by increasing the level of corruption, the level of money laundering and the infiltration of organized crime into legal economic flows, the spread of illegal markets and the increase of the crime rate, but also the ability to generate criminal profits, increasing the economic power of criminal structures that is recursively used for influence on government holders.

**Keywords:** ORGANIZED CRIME**,** ILLEGAL MARKET, SECURITY, FUNCTIONED AND ANALYSIS OF ILLEGAL MARKETS

## *1. Introduction*

In contemporary conditions, criminal structures are based on organizational models that allow them to grow professionalism and efficiency. These organizational models are most often fostered according to a functional and market principle, building criminal networks that are adapted to the needs of dealing with illegal markets and in legal economic flows. Namely, we can designate the market as a comprehension of the offer-and-demand relations that affect the sale of goods and distribution of services at a certain time, so the market is an arena where goods are regularly and voluntarily exchanged for money, under competition conditions (Beckert, Wehinger, 2013: 6). The illegal market most frequently covers the market: illegal goods, their production, trade and possession; illegal trafficking of legal goods and illegal service providers (Weenink, 2004: 32).

Accordingly, the illegal market encompasses, first, the goods and services market, which violate positive legal regulations, purchasing transactions of goods and services that are otherwise allowed under the procedure codes — *gray* market or economy (alcohol, oil, cigarettes and so on), the second market of goods and services that are strictly prohibited or restricted by legal regulations and regulated by the economy foreign state institutions (arms, drugs, people and so on.) That is, we can talk about four basic types of illegal markets — markets whose illegality stems from the production of specific goods or services outside the legal provisions and regulations; illicit market exchange of illicit products; illicit market exchange markets as a consequence of traffic in stolen and counterfeit products; markets whose illegality stems from breaches of regulatory market norms (Beckert, Wehinger, 2012: Four.

The illegal market from the geographic space standpoint may be: local, regional, national and international. However, from a point of view of offer and demand, the illegal market is imperfect, as prices in this market are often formed under pressure from the stronger factor on the side of offer or demand, which in this case is the influence of dominant criminal organizations that create a monopolized position. The illegal market can be divided into buyers and seller markets. In the customer market, the buyer is dominated by the buyer, which appears as the end user of services or consumer of certain goods and this situation is possible because we have a bigger offer on the market than demand. In the case of retailers' markets, the backdrop is in which vendors are dominated by higher demand. By forming the aforementioned relationship in the dominated market, it is able to dictate the terms of the exchange.

Criminal organizations can offer illegal services and goods, can use violence, intimidation and corruption, capable of hampering their competition by infiltrating significant funds into the legal economy. The large quantities of illegally acquired assets, owned by criminals and criminal organizations, pose a potential threat to corruption in the legal business and operation of state-run authorities. They also allow for the inclusion of criminal organizations in the legal business, which can be particularly dangerous if used to support criminal activity, which altogether affects the security situation negatively. In these cases, criminal organizations combine their power and seek to corrupt, blackmail, murder, use of political contacts and other ways to achieve their interests by undermining the foundations of state security.

## *2. Illegal market operating mechanisms*

One of the first assumptions in examining the operation of illegal markets concerned the monopoly of criminal organizations against the illegal market (Chang, eds, 2005: 665) However, if we analyze the illegal market more closely, we will see that it represents a blend of opposing sides that seek to impose their own interests on others and control the illegal market. The illegal market connects one side of the criminal organization that is in rival relations (seeking to increase their share in the market) with, clients who create demand in the illegal market. On the other hand, new criminal organizations are trying to enter the market and generate criminal profits. Then, criminal organizations that are the biggest suppliers of the market tend to impose the conditions, businesses" that answer and monopolize the market's supply. Authorities in charge of suppressing organized crime are trying to prevent the activities of criminal organizations and effectively counter certain types of crime. The illegal market responds to the increased functioning of competent state authorities by increasing the price of goods, which is conditioned by the increased risk of criminal activity detection and reduced bids.

The general rule is that criminal groups that are more violent and more enforcing corruption are taking the lead role in the

illegal market. It was similar in the prohibition period in America. Its beginning allowed the release of a vast amount of violence that was a specialty of various gangs. Physical protection against rival groups and armed robbers suddenly became more important than protection by the law, in this sense, the prohibition of a criminal gang turned into real small empires (Abadinsky, 2003: 67.

In the event that the illegal market is developing of criminal organizations are expanding their criminal activities and achieving higher criminal profit rates. Thus, the activities of state-run law enforcement authorities can influence relations in the illegal market between rival criminal organizations. For example, after police killed Ramon Arellan Felix, who headed the Tijuana Cartel in Mexico in 2002. In the year, his dealings are taken over by Ismael Zambada-Garcia Sinaloa, the leader of a rival criminal organization and boosts market share thanks to the increased volume of drug trafficking (Small & Taylor, 2006: 8)

For a better understanding of the relationship in the illegal market between the opposing parties, the study is also interesting about the illegal drug trade market in Italy, Germany and Russia (Paola, 2001: 31). The surveyed drug markets are open markets, the links between drug-dealing criminal organizations look more like rival relations than consensual activities. Actually, there's no limit to entering the illegal market. Although some suppliers (the Italian mafia and Dr.) occasionally create monopoly that they have over other local (usually smaller) markets, in most European countries and Russian cities, drug-dealing criminal organizations prefer to accept the price than they set it. This means that none of them are able to influence significantly the price value by changing the quantity of the offer. When there are many customers and suppliers in the market, no providers or customers can determine the price.

In trade, in little on the illegal market, demand and possibilities for achieving criminal profits are affecting market developments. In the illegal market, there are few criminal organizations that completely rule the market and maintain the monopoly; there are few criminals who enter the market on their own. Most criminals join in a network or hierarchy to strengthen their position among market competitors. Joining forces with other criminals increases the market share and creates an additional value that participants share (Pérez, 2007: 123).

Another study that studied the Colombian drug trade market shows there are rival market sites (Kenney, 2007: 235). In fact, the association that sets the fixed price has never dominated the Colombian drug trade. And so in the cases when Medellin and Cali cartels were at their peak, the production and export of cocaine from Colombia were highly competitive. There were independent criminal organizations in more than 10 towns that smuggled large quantities of cocaine into US and European markets. However, most of these criminal organizations have been arranging their activities with Pablo Escobar, Orch brothers and other well-known drug traffickers in order to control prices and monopolize the market. Different criminal groups at times uniting their funds to complete major drug shipments. Despite the existence of contacts between criminal organizations, the majority has persistently sought to retain their own supply, financing and clientele.

Market mechanisms set a fixed price on the market based on both offer and demand. Suppliers are willing to sell more products if the price is higher and consumers will buy more if the price is lower. Thus, the price hike in products leads to an increase in demand, and a decline in demand. Wrong offers and demand will be changed due to changes in the price and amount of goods in the market. For example, if a criminal group is eliminated from the illegal market by competition, the amount of products decrease in the market and price increases is plunged. However, this situation is not held for long because new criminal organizations are entering the market attracted by extra-profit, and soon there is a stabilization of the offer through the availability of large quantities of products and falling prices. Demand in illegal markets determines the high number of factors. Consumers can depend on goods coming into the market as is the case with many intoxicating drugs, but consumers can be willing to look for what is the case with those seeking sexual favors.

Illegal markets are becoming global in contemporary environments that create opportunities to increase the rate of criminal profit. Free trade of goods and services, people, money, modern technology, the demolition of traditional borders between states affects the expansion and globalization of illegal markets (Boskovic, Marinkovic, Laic, 2015: 25) Price elasticity, offer and demand will vary from market to market. For example, in the narcotics market where consulates are completely dependent on the daily dose, elasticity can be very low, whatever the cost is not reduced in demand to meet market needs. Drug addicts are not selecting funds to obtain daily drugs and are willing to pay high prices as well. Of course, the height of the drug price may affect the expansion of the market and availability of new consulates, but also the increased interest of new criminal organizations in participating in the illegal market attracted by high levels of criminal profit.

Although the traditional purchase, which means direct customer contact and seller, remains a key form of illegal traffic, virtual markets have formed an alternative source of supply to illegal goods and services, allowing users worldwide to appear in the market in one click on the keyboard. In fact, individuals or groups dealing with the trafficking of illicit goods can be accommodated at any geographic location, while at the same time being directly connected to users around the world thanks to the Internet. In this way, the importance of the traditional physical intermediary in trade affairs was relatively established and replaced by a virtual mediator. For example, drug users no longer have to go out on the street and contact a drug dealer instead, drugs can order on the internet and wait for their delivery to their home address.

## *3. Illegal market analysis*

In order to better understand what's going on in the illegal market, some areas that are important for its functioning should be analyzed. Market analyzes comprise the most frequently found areas of consumer analysis, market analyzes, market competition and market share, namely, a model of market analysis that is installed can be applied to illegal markets (Beckert, Wehinger, 2013: 5-30. During the organizational analysis, weak points of the criminalist processing facility are identified, so that relevant state authorities could take adequate measures to prevent the damaging consequences of the organization's analyzed activities.

The consumer analysis focus is on developing a segment scheme, dividing the market into various composition areas composed of different consumer groups (drug addicts, sex services beneficiaries...). Analysis of market actors addresses questions of recognition of modalities for optimal and rational use of the criminal organization's resources in achieving the goals. Competition analysis covers compiling detailed profiles of each competitor on the illegal market, focusing especially on their weaknesses and strengths. Depending on the specific needs, assessments of the criminal organization's goals, power distribution within the organization, human and technical resources, decision-making processes and others can be conducted. The market share is either a percentage or part of the overall available market or part of it supplied by a criminal organization. We can express it as revenue from the sale of a criminal organization divided by the net income of sales available on this illegal market. We can also express it as a single amount of the single sale of a criminal organization divided by the total amount of units sold on the criminal market. In cases when the overall market quantity is expected to decline, some may increase

their market share, maintaining their volume of sales. For example, if we look at the sexual service market as long as "sex trafficking" is illegal, organizers and clients are breaking the law. Criminal organizations dealing with the trafficking of women in order to engage in sexual exploitation on the illegal market share their interest zones with each other. In the event that police eliminate one of the criminal organizations from the criminal market with their activities, it allows others to increase their share of the market. Increasing the market share is one of the most important goals used in the legal business, but it also serves as a priority goal for the activities of criminal organizations.

The survey, which studied the illegal cigarette market in the Netherlands, found out that the market there is relatively open to the possibility of entering the market (van Diyck, 2007: 165) According to the survey, the market's market share of untaxed tobacco was estimated in 2003 year to be 3% in 2005 in the year 5%, while total tobacco consumption in the Netherlands has been falling. Illegal cigarette trade in Holland relies on limited networks consisting of one or two suppliers and about a dozen wholesale buyers. In these conditions, the rate of criminal profits in the market is high, and the risk is relatively low.

Also interesting is the study, the black cigarette markets in Estonia (Marquina, 2007: 204). The share of the untaxed tobacco market in Estonia is estimated to be much higher than it is in the Netherlands. This is due to neighboring states, such as Russia, which have cheaper tobacco and therefore tobacco prices are rising faster in Estonia than in the Netherlands. In order to join the EU, Estonia had to apply tax on cigarettes and other tobacco goods very quickly. For an ordinary smoker, it meant an incredible increase in the price of cigarettes for a relatively short time. As a result, many smokers have sought alternative supply sources and found them on the black market. A survey in Estonia found that about 60% of respondents are ready to buy illegal cigarettes and due to the high price of cigarettes in the legal market. While the box of legal cigarettes cost 2.05 euros in 2007. In the year, the boxing of illegal cigarettes cost 0.57 euros. The places where illegal cigarettes were sold are well-known to Estonia's public. Customers illegally bought cigarettes either directly from street vendors (53%) or from vendor’s home (35%). The majority of illegal cigarettes are trafficked.

Illegal markets are expanding beyond state borders, because demand is present in several countries and the offer is unsatisfactory. Thus, for instance, illicit trade is underway from the region of Northeastern Europe, given the highly taxed products especially in and outside Nordic countries; Southwest Europe is linked to illegal immigration, cocaine, cannabis trade which is further distributed to the European Union; In particular, Southeast Europe is linked to drug trafficking, illegal immigration and human trafficking, and these activities are transferred to the entire European Union. How profitable the production and traffic of drugs is the business is that the data that a kilo of cocaine in the jungles of Colombia can be purchased for $2200, $5500-7000 in Colombia's ports is the best thing to do in the U.S. Market, reaching $2400-205 to Europe. $3000, $55000. In Australia, his price is $200000 dizzy. Prices per gram of cocaine are between $100-150 in Europe $130-185 and Australia $250-500 (Stewart, 2015).

The market share has the potential to increase profits given the positive or no market change. An increase in the market share allows criminal organizations to change the structure at the rival game of forces in the illegal market. Namely, a significant increase in the share on the illegal market implies a decrease in the influence of competitive crime organizations, clients, suppliers and new criminal organizations. In economic terms, increasing the market share is part of market management, which focuses business discipline on the practical application of market techniques and management of funds and activities of a market organization. Structures by criminal organizations are often aimed at analyzing the impact of levels, times and the makeup of customer demand in a way that will meet the organization's goals. In a market competition against a criminal organization besides legal business methods, they also use criminal methods (threats, blackmail, violence, corruption and dr.) to increase their share in the illegal market. Criminal organizations develop a market strategy based on objective understanding of their own, business" and analyzing the markets they operate on.

## *4. Conclusion*

Criminal organizations, profit *generated* in the illegal market, are often used as an economic lever of power for infiltration of the political system by funding political structures and thus by gaining the political power recursively used to increase the economic power of criminal organizations, undermining the foundations of state security. Large quantities of illegally acquired funds that are owned by criminal organizations pose a potential threat to corruption in legal business and state authorities, undermining the integrity of financial institutions and money laundering enable inclusion in legal business, which has direct implications for the economic security of the state.

The efficiency in the realization of criminal intentions, organized crime achieves by using expert knowledge, criminal and legal methods and adapting the structures of criminal organizations to the specialties of global and local illegal markets. In contemporary conditions, criminal structures are based on organizational models that allow them to grow professionalism and efficiency. These organizational models are most often fostered according to a functional and market principle, building criminal networks on an international agenda that are adapted to the needs of dealing with illegal markets and in legal economic flows, which has negative implications on international security.

The suppression of illegal markets, or discovering and proving illegal activities on them, has hampered the very nature of such markets. As in the legal market, there are two complementary activities in the illegal market — offers and demand, or two co-noble subjects — seller and buyer. The participatory relationship, including the middleman, defines the fact that they are addressed to each other, making themselves a symbiosis of their own. After all, it's a feature of every market, whether it's legal or not. In the sphere of illegal goods or services, the presence of the seller of illegal goods or services in the market is motivated by profits, while in the case of the buyer the motive is inherent in the effort to obtain goods or services, which, as a rule, cannot be found on the legal market or require special permission. The mutual interest of purchasing participants has resulted in mutual preservation from the organs of state repression — neither the seller nor the buyer will give up their partner, they act by consent, without coercion. That is why activities in illegal markets fall into the category of consensual crime, including victimized crimes. It is the acts of a necessary acquittal, in which, unlike property crime, reports of illegal activities on law enforcement are missing, and are characterized by a high dark number.

Contemporary criminal organizations are spreading spheres of influence on all areas of social life and becoming a danger to national and international security. Research into the illegal market creates the basis for better understanding the nature of contemporary organized crime that controls illegal markets. The knowledge of the organization's specificity and the functioning of illegal markets enable the proper selection of methods to more efficiently counter the destructive actions of criminal organizations, which is the basis for developing preferences in creating security strategies for effectively countering this phenomenon.

## *5. Literature*


1. Abadinsky H., *Organized Crime*, Belmont, 2003.

2. Beckert, J., Wehinger, F., In the shadow: illegal markets and economic sociology, *Socio-Economic Review*, Volume 11, Issue 1, 2013, 5–30.

3. Bošković, G., Marinković, D., Laić, O., *Finansijske istrage organizovanog kriminala*, Kriminalističko-policijska akademija, Beograd, 2015.

4. Stewart S., From Colombia to New York City: The economics of cocaine, *Business Insider*, Jul. 16, 2015; http://www.businessinsider.com/from-colombia-to-new-york-city-the-economics-of-cocaine-2015-7

5. Chang, J.J., Lu, H.C., and Chen, M., Organized crime or individual crime? Endogenous size of a criminal organization and the optimal law enforcement. *Economic Inquiry* 43 (3), 2005, 661–675.

6. Kenney, M., The architecture of drug trafficking: Network forms of organization in the Colombian cocaine trade. *Global Crime* 8 (3), 2007, 233–259.

7. Markina, A. (2007). Cigarette black market in Estonia. In Crime business and crime money in Europe: ά e dirty linen of illegal enterprise, Eds. P.C. van Duyne, A. Maljevic, M. van Dijck, K. von Lampe, and J. Harvey, 195–208. Nijmegen, The Netherlands: Wolf Legal Publishers.

8. Paoli, L., ά e "invisible hand of the market": ά e illegal drugs trade in Germany, Italy and Russia, Third Colloquium on Cross-border Crime, Police Academy Bratislava, Slovak Republic, 2001, 19–38.

9. Pérez, N., *Crime networks*, Job Market Paper, University of Maryland, College Park, 2007.

10. Small, K. and Taylor, B., State and local law enforcement response to transnational crime. *Trends in Organized Crime* 10 (2), 2006, 5–17.

11. van Dijck, M., Cigarette shuffles: Organising tobacco tax evasion in the Netherlands. In Crime business and crime money in Europe: ά e dirty linen of illicit enterprise, Eds. P.C. van Duyne, A. Maljevic, van Dijck, M., K. von Lampe, and J. Harvey, 157–194. Nijmegen, The Netherlands: Wolf Legal Publishers, 2007.

12. Weenink, A., *Crime without frontiers: Crime Pattern Analysis Eastern Europe*, 2002-2003, Driebergen. Netherlands: Korps Landelijke Politiediensten, 2004.


[i] This work is the result of the realization of the research project *Development of institutional capacities, standards and procedures for combating organized crime and terrorism in the conditions of international integration*, funded by the Ministry of Education, Science and Technological Development of Republic of Serbia for the period 2011-2019 and is implemented the University of Criminal Investigation and Police Studies in Belgrade.

# SYSTEMIC APPROACH TO THE DEVELOPMENT OF SECURITY SYSTEMS FOR CRITICAL INFRASTRUCTURE PROTECTION AS A RESEARCH METHODOLOGY APPLIED AT THE CENTER OF COMPETENCE *QUASAR*

Chief Assistant Dr. Eng. Panevski V.S.
Bulgarian Academy of Sciences, Institute of Metal Science Equipment and Technologies with Hydro- and Aaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria
panevski@ims.bas.bg

***Abstract:*** *Ensuring the security of the population is one of the fundamental policies of the European Union. Various approaches are being implemented in this area, one of which is the creation of critical infrastructure security - national and European.*
*In this regard, trough the development and operation of intelligent security systems, with a focus on critical infrastructure, is expected to improve the security of the population in EU Member States. Precisely the synergy of efforts of the scientific and industrial communities in our country for performance of specific models of security systems through the establishment and operation of centres of competence is at the core of this paper.*
***Keywords****: CENTRE OF COMPETENCE; INTELLIGENT SECURITY SYSTEMS*

## *1. Introduction*

Essentially, Centres of Competence (CoC) are structural cooperation units, comprising scientific and business organizations empowered to undertake strategic market-oriented research for the benefit of the industry. The initiative of the CoC is to achieve a competitive advantage in the industry through access to innovative capacity of the research community. These joint research organizations are the "*new hope"* for our country, as all participants will benefit from shared intellectual property and research, and the national industry will benefit from the knowledge gained and retained both in our country, so are those currently being generated abroad.

*How can researchers benefit?*

Primarily, the dynamic interaction with industry will ensure the applicability of applied scientific research. A functioning CoC provides a long-term financing mechanism for the rational use of time to achieve planned results, as well as alleviate continuity problems. It should not be overlooked that CoC's access to larger financial flows for the development of research infrastructure will not allow the use of other research schemes. For example, Europe's programme for small and medium-sized enterprises (COSME) provides enhanced access to finance in different phases of their lifecycle: creation, expansion or business transfer. It is precisely through the funding of these activities that research support can be assured.

*How will benefit industry?*

Through the functioning of the CoC will be provided an opportunity to participate in riskier, long-term market research that, when resolved, can bring a competitive advantage. Access to intellectual property will allow an earlier impact on the exploitation of developed products and systems. Last but not least, networking with leading and influential researchers would help to participate in research initiatives and projects at national and European level. Researchers' access to EC programs such as "Horizon 2020" and the "Marie Curie Program", which form brilliant researchers, plays a key role in the knowledge-based economy Europe is aiming for.

At the same time, EC policy documents on research and innovation state that a *systematic approach "... will ensure that challenges can be tackled while also giving rise to new competitive businesses and industries, fostering competition, stimulating private investments and preserving the level playing field in the internal market*"**[1]**.

Particular attention will be paid to ensuring a balanced and broad approach to research and innovation, which is not only limited to the development of new products and processes and services based on scientific and technological knowledge, but also incorporates existing technologies into new applications and continuous improvement and non-technological and social innovation. The right direction in this area is jointly, research and industry organizations, to build and develop a research and innovation knowledge infrastructure, as well as a mechanism for the open distribution and sharing of products developed for market realization.

For the better understanding of the following text, I will make the following clarifications, namely:

- *"center of competence"* - definition:

*„... top-level scientific complexes, in which the scientific studies are performed following the best world standards and practices"***[2]**;

- *"systematic approach"* - definition:

„*A process used to determine the viability of a project or procedure based on the experiential application of clearly defined and repeatable steps and an evaluation of the outcomes"***[3]**.

The systematic approach is the most sophisticated approach where each system or object, in this case the CoC, is seen as a set of interconnected components having an output coupled to the target and input connected with resources and communication with the outside environment (industry and market), i.e. feedback.

The aforesaid is directly related to the construction of *Center of Competence "Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar)* and its contribution to the of critical infrastructure security development.

## *2. Quasar and intelligent security systems development*

The development of Intelligent Security Systems within the scope of the CoC is closely related to *Work Package 2: "INTELLIGENT SECURITY SYSTEMS"* (WP2) which is headed by the Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A. Balevski" (IMSETHC-BAS). WP 2 includes certain activities and stages that ensure its correct and timely implementation (Fig. 2.1).

Within WP2, an analysis of current trends in the development of means to ensure security through the security systems of critical infrastructure (CI) will be done. Carrying out a study of the conditions and algorithm of work in the elaboration of operational procedures for the operation of various modern models of security systems will contribute to a higher level of security and protection of developments. Integration between the organization's business continuity management processes (critical infrastructure, sites of national, regional and local importance) and the development of intelligent security systems by modeling their integration into the organization's management system is essential. All this is provided through the activities and stages for implementation of WP2 **[4]**.

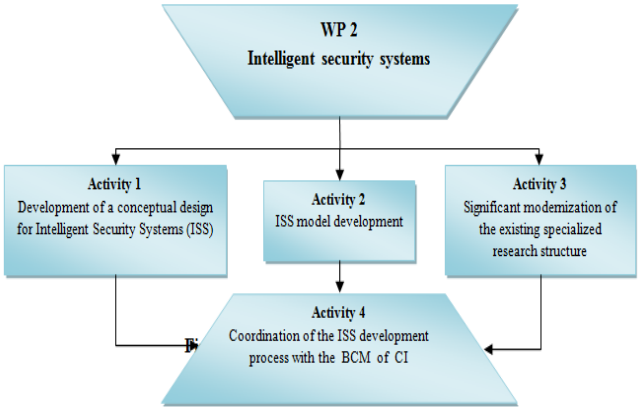



***Fig. 2.1:*** *WP 2- general structure*

***Activity 1: Development of a conceptual design for Intelligent Security Systems (ISS)***

The activity involves a research of existing contemporary ISS approaches and practices. The specifics of the national critical infrastructure will also be studied, and particularly the objects of national, regional and local significance.

Stages:

– Stage 1. A study of existing contemporary ISS approaches and practices;
– Stage 2. An analysis of the national critical infrastructure, and particularly the objects of national, regional and local significance;
– Stage 3. Development of ISS conceptual design (security system models).

***Activity 2: ISS model development***

The complexity of this task involves: development of hardware for ISS sensor elements, tools for wireless data transmission, tools for data visualization and for system cyber security. Development of ISS operation software for: ISS sensor elements, wireless data transmission tools, data visualization tools, system cyber security tools, for decision-making in complex risk situations, as well as software for comprehensive system management and for the production of documents needed in the ISS functioning.

Stages:

– Stage 1. Development of hardware for the ISS model(s);
– Stage 2. Development of software for the ISS model(s);
– Stage 3. Development of functional documents for the ISS operation;
– Stage 4. Developing a business model for managing research and innovation in the organisation.

***Activity 3: Significant modernization of the existing specialized research structure***

Closely related to Activity 1 and Activity 2, Activity 3 is aiming a significant upgrade of the existing research structure, i.e. the Laboratory for Smart Sensor Systems and Technologies and the Laboratory for 3-D Modelling and Rapid Prototyping.

Stage:

– Stage 1. Substantial upgrade of the Laboratory for Smart Sensor Systems and Technologies and the Laboratory for 3-D Modelling and Rapid Prototyping.

***Activity 4: Coordination of the ISS development process with the Business Continuity Management (BCM) of critical infrastructure***

All activities in the process of creating an ISS model (or models) are inextricably linked to an uninterrupted operation of critical infrastructure. The ISO Technical Committee (ISO/TC 292 Security and Resilience) has laid down the main BCM principles in ISO 22301 “Societal security - Business continuity management systems – Requirements”; ISO 22300 "Societal security - Terminology"; ISO 22313 “Societal security - Business continuity management systems – Guidance” and ISO / TS 22317 “Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA)”. The development of a concept for the specific interactions between these processes will provide data for their modelling and automation. This innovative approach is expected to contribute to a significant reduction of operating time and financial costs in the development, maintenance and upgrade of the organisation's security system.

Stages:

– Stage 1. Analysis of the organisation's BCM, including adopted and standardized international approaches in order to determine the stages/processes providing the input data for ISS development;

– Stage 2: Development of a conceptual model of the integrity between ISS features and BCM processes;

– Stage 3. Development of a concept of the scope of automation and coordination between BCM and ISS models.

Internal links between the WPs and the proper coordination of partners' activities play an essential role in the building up and future development of the security systems development process. This process is discussed in the next section.

## *3. CoC internal links facilitating the development of ISS*

These WPs form the core elements of the functioning of the CoC as a system. The activities included in the work packages and the results planned to be achieved indicate internal links through which the synergy of research and applied science activities are expected.

Within Quasar will be realized four work packages (WP) as follows: WP 1 „Quantum communication“; WP 2 „Intelligent security systems“; WP 3 „Risk management“ and WP 4 „Innovative sensor technologies with multi-purpose application“ (Fig. 3.1)

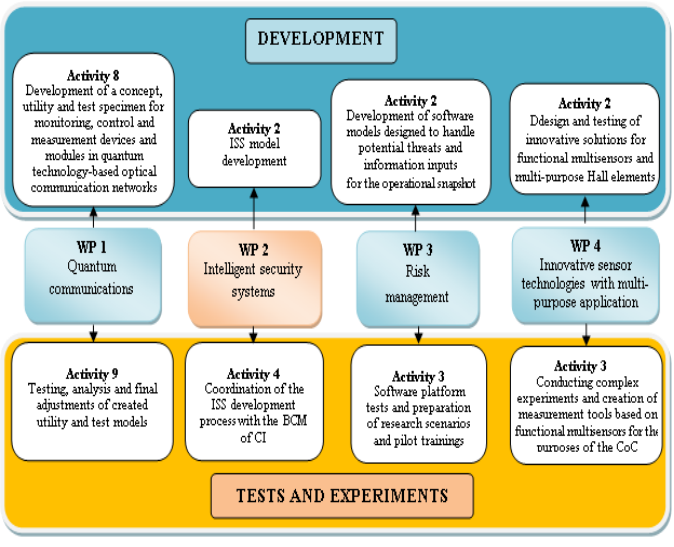



***Fig. 3.1****: CoC Quasar general structure*

The activities set out in *WP 2* "Intelligent security systems" have a leading role in the development of ISS. The research methodology under this WP includes the implementation of a systematic approach in the process of analysis, evaluation, formulation and proposal, with regard to improving the process of security enhancement and protection of critical infrastructure objects by security zones building, taking into account the specifics and interactions between their elements, as well as between them, and creating models ISS, with a focus on all aspects of CI management. Also of particular interest is the link with the research into the quality of critical infrastructure protection systems carried out so far [5], which facilitates the achievement of a comprehensive approach to developing security systems.

ISS models development, in accordance with the specifics of security objects, will require the development of modern, fast-acting and fully autonomous sensor subsystems, to test the functionality of which test and simulation systems need to be developed. In this way, at a relatively low cost, through modern innovative scientific developments, the desired level of compliance will be achieved and thus – security.

*Basic internal links to support of ISS development*

The main areas of interaction between work packages (Fig. 3.2), related to the development of ISS, are carried out at the stages of the preparation of concepts, models and specifications of hardware and software. This ensures the technological and functional compatibility between them and avoids duplication of activities and resources.

For example, quantum communications (*WP1*) provide physically unconditional security to the network when transmitting information between sensor models built in critical infrastructure and models of managed / situational decision points that must be protected against copying or eavesdropping, and authenticity between communicating parties to be guaranteed.

Also the development in *WP3* of unified, integrated hardware and software of simulation environments to upgrade existing ones and to create new models and data for the real environment, will allow research and training in the field of security and crisis management of different nature. Creation and installation in the information environment of simulation models of objects from the national critical infrastructure, objects of strategic importance, from the technical infrastructure, etc. important for national security will facilitate the development of appropriate ISS models.

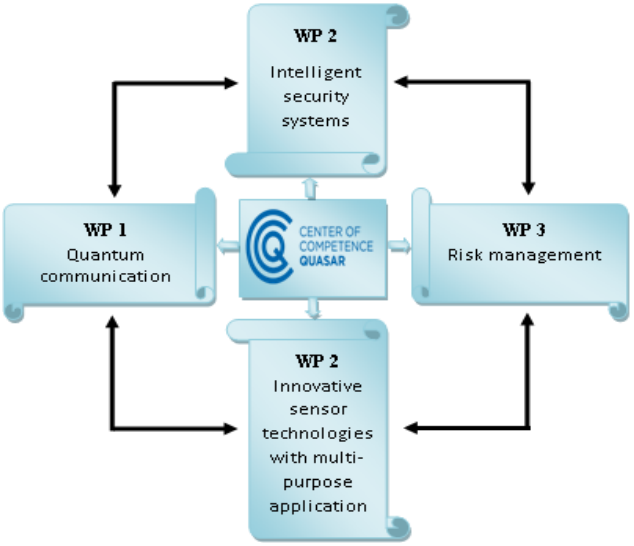



***Fig. 3.2:*** *ISS development - basic internal links*

As a result of the implementation of *WP4*, innovative sensors will be created to record environmental and security factors for critical infrastructure sites. Innovation activities within WP4 involves the establishment of an objective database and models to predict / anticipate catastrophic earthquake processes and phenomena through a fundamentally new approach - emission of nanoparticles. This will extend the scope of ISS, contributing to the "added" reality of simulated processes.

At the same time, joint testing and experimentation of hardware and software developed in the scope of work packages will facilitate their integration to achieve the set goals and in particular for the ISS development. Removal of the found inconsistencies in the conditions of joint tests will reduce the time for correction, reduce the costs for it and achieve the planned results for timely realization on national and international markets. It is important to note that the testing of ISSs is also linked to the verification of the results obtained. Therefore, a number of approaches are known to determine the quality indicators of of critical infrastructure for protection systems **[6]**, the implementation of which guarantees compliance with the technical and operational requirements of ISS elaborated.

Last but not least, all activities in the "Development" and "Tests and Experiments" areas (Fig. 3.2) *referring to ISS models* are closely related to the good European and world practices in the sphere of Organization's Business Continuity Management (BCM). BCM "… is a sector of business practice with a long tradition of formal elements and requirements in international standards and a number of national regulatory documents with internationally recognized institutions and a network of means of disseminating best practices, many of which are an integral part of these requirements in the process of updating the standards and normative requirements against which individual companies organize and carry out their activities and achieve planned business objectives" **[7]**.

An alternative way of thinking is that BCM should adopt an "All Hazards Approach". This approach focuses on how to continue / recover services, following the materialization of risk. This in a specific way means that Resilience Evaluation (RE) should also be carried out as a result of the CI risk assessment. RE "…is the overall modeling activities, and analysis of critical infrastructure systems aimed at evaluating the ability to prevent, absorb, adapt, and recover from a disruptive event, either natural or man-made"**[8]**.

*Technical and interoperability between the products or processes envisaged for substantial improvement and related research to support the development of ISS*

During the development of the major areas in the structure and functioning of the CoC, the following internal links were introduced to ensure compatibility in the design and operation of the intended results. I would like to emphasize that these are only the main areas that ensure compatibility in the development of security systems models.

- *Transfer of protected information, received from ISS;*

The construction and successful commissioning in *WP1* of one or more new optical quantum channels using linearly polarized photons for quantum key-sharing will ensure that the final information transmitted between the main centers (mobile or fixed sensor security systems and points of contact) management) will be transferred to where it is and to whom it is needed, without third parties being able to access it.

- *Development of technical and operational requirements for ISS models;*

Developed in *WP3* software models and data from the real environment for conducting research and training in the fields of security, safety and crisis management of a different nature in urban / industrial / transport medium in the marine environment in the air will reduce the time and cost of financial funds in developing related ISS. The corresponding simulation models, including the methodology for assessing the risks and deciding on preventing or

counteracting will ensure compatibility between products and systems for collecting, processing, automation, verification and transmission of any credible information regarding intelligent security systems and their management.

- *Extended ISS coverage.*

The established and tested *WP 4* forecast models, algorithms and recording geodynamic modules of the modern sensor system for predicting catastrophic phenomena by emission of nanoparticles would help to expand the scope of ISS and improve their complex efficiency.

These areas are expected to contribute to the development of comprehensive research and innovation capacity, the integration of planned research with the development of contemporary and emerging ISS technologies.

## *4. Conclusion*

The implementation of WP 2 activities will contribute to the development of an innovative, multifunctional, basic, sensory system providing security of critical infrastructure and objects of national, regional and local importance, as well as capacity building for significant modernization of existing specialized research capabilities. In this way it is expected to ensure improvement of the social security in our country, significant modernization of existing specialized research infrastructures, necessary to meet the needs of the employees in the field of research and innovation, and structuring of processes and business models for the management of the research and innovation activities in the interest of organizations/enterprises in order to increase their competitiveness.

It is through the implementation of the systematic approach and the coordination of activities between participation of different work packages that the complete research and innovation capacity will be built, the integration of the planned research with the development of new and emerging technologies and the optimization of the possibilities for implementing the research results for the development of the innovative ones. This will create mid-term competitive advantages for organizations participating in the Center of Competence "Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar), engaged in research and innovation, as well as for those who apply their contemporary developments.

## *Literature*:

**[1]** COM(2018) 436 final, „ANNEXES to the Proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation";

**[2]** „SCIENCE AND EDUCATION FOR SMART GROWTH OPERATIONAL PROGRAMME 2014-2020", Version 2.0 / Approved by EC on 11/11/2018 /, page 51;

**[3]** http://www.investorwords.com/19342/systematic_approach.html;

**[4]** " PROJECT JUSTIFICATION under the competitive project selection procedure CREATION AND DEVELOPMENT OF CENTRES OF COMPETENCE" (Creation and Development of a Center of Competence "Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar);

**[5]** Георгиев Н. Л., Анализ на един клас специализирани сензори за защита на обекти от критични инфраструктури. 2015, ISBN:978-619-90310-4-9, 170 стр.

**[6]** Georgiev Nikolai, "Quality criteria for critical infrastructure protection systems", International Journal of Economics, Commerce and Management, vol VI, issue VI, ISSN 2348-0386, 2018, p. 265-271;

**[7]** Kiril Stoichev, Risk Analysis for Business Continuity Management of NPP, International Journal for Economics, Commerce and management, Vol. VI, Issue 11, November 2018, ISSN 2348 0386, 459-476;

**[8]** Associate Professor Ph.D. Dimitrov D. L., "CRITICAL INFRASTRUCTURE RESILIENCE EVALUATION – RESILIENCE APPROACH, RESILIENCE MODEL AND RESILIENCE INDICATORS", International Scientific Journal Security & Future, 1/2018, ISSN 2535-0668, p.p. 7-10.

# HUMAN SECURITY AND CROSS-BORDER COOPERATION

Assistant Prof. Dafinka Sidova, Ph.D.
Department of National and International Security – New Bulgarian University, Sofia, Bulgaria
dsidova@nbu.bg

***Abstract:*** *Cross-border cooperation (CBC) is a unique and effective instrument of European Union that has the potential to influence on human security in a positive way. This paper analyses the role of CBC between Bulgaria and Greece in the context of human security. The analysis is focused on the Right to Life, and especially, on the right to health and social welfare. The comparative analysis represents CBC results and benefits from two programming periods: 2007-2013 and 2014-2020. The expected outcomes of cross-border projects (by 2023) are also being explored, outlining the main trends and prospects for developing the cross-border partnership.*

**Keywords**: HUMAN SECURITY, CROSS-BORDER COOPERATION, HEALTH AND SOCIAL WELFARE, BULGARIA, GREECE

## *1. Introduction*

Cooperation is a prerequisite for success. Actually, it gathers together knowledge, experience, skills and abilities of different participants to achieve common goals [1]. Protection and better condition of human security [2] is a such common and very important goal. Furthermore, quality of life is highly correlated with the level of security for all people and for each individual. In conditions of a sufficient level of security, the development of a human personality is better and more effective. [3]

As one of the three types of European territorial cooperation, cross-border cooperation (CBC) takes an important place in the Cohesion Policy of the European Union (EU). Its main goal is to promote a harmonious economic, social and territorial development of the Union as a whole. Admittedly, CBC is a key factor for sustainable growth. It facilitates the effective capacity building (including managerial, administrative and material) of the involved countries. Moreover, CBC offers a wide range of opportunities to enhance human security, and in the context of this paper, Right of Life, or the right to health and social welfare, in particular.

For the 2014-2020 programming period Greece-Bulgaria CBC includes seven Prefectures in Greece and four Districts in Bulgaria (Fig. 1). By November 2019, a total of 51 projects are awarded a total of €92,2 million (€78,4 million ERDF funding). These are 85% of the total €130,3 million (€110 million ERDF funding) budget for the The Cooperation Programme INTERREG V-A "Greece-Bulgaria 2014-2020" [4].




***Fig. 1*** *Map of the Cooperation area [4]*

First and most importantly, in this report, the main object is the Bulgarian-Greek CBC, and the main subject is its effectiveness in improving human security, in the context of health and social living conditions. The main purpose is to create an appropriate research environment for the partnership to be compared (by November 2019) and to outline its future development in the long term (by the end of 2023). To achieve this, a comparative analysis is structured, incorporating specific criteria. It can be used to trace the trends of the CBC development, to bring out the main benefits, and to outline the prospects for development.

At the same time, there are some limitations in this study by:

- territorial limitations – Greek-Bulgarian cross-border cooperation area;
- time limitations – from 2007 to 2023;
- a number of good practices – three cross-border projects for programming periods 2007-2013 and 2014-2020;
- a number of comparison criteria – two criteria: number of projects and project budget;
- number of projects with expected benefits - two projects in implementation by 2023.

The applied methodology includes the following approaches: deep, complex, structural-functional and dynamic. Also, it is applied data processing and analysis method and comparative analysis.

## *2. Good Practices*

The Cooperation Programme INTERREG V-A "Greece-Bulgaria 2014-2020" enables beneficiaries from the Greek-Bulgarian cross-border cooperation area to implement projects in four priority axes (PA) [3]:

- PA 1: A Competitive and Entrepreneurship Promoting Cross-Border Area;
- PA 2: A Sustainable and Climate Adaptable Cross-Border Area;
- PA 3: A Better Interconnected Cross-Border Area;
- PA 4: A Socially Inclusive Cross-Border Area.

According to the Programme document [5] Greek-Bulgarian cross-border cooperation area health status indicators has not been satisfactory for a long time despite the satisfactory levels (in terms of quantity) of healthcare infrastructure in the area. It is indicated a lack of effectiveness in the application and/or distribution of such resources. The rise of poverty has placed more pressure on health care systems. Improving their effectiveness is hence of paramount importance.

Also, the Programme document underlines that the rise of poverty has placed vulnerable groups at increased risk of peril. Social entrepreneurship has been successfully used to alleviate such problems in other EU regions/Member States but has not been sufficiently developed in the Greek-Bulgarian cross-border cooperation area. Social entrepreneurship can address issues of reduced service delivery to special populations subject to or threatened by social exclusion and – at the same time - provide a vehicle for these populations to gain access to employment.

Turning to these health and social issues, it could be positively changed by investment priorities and specific objectives of the fourth PA A Socially Inclusive Cross-Border Area:

- Investing in health and social infrastructure which contributes to national, regional and local development, reducing inequalities in terms of health status, promoting social inclusion through improved access to social, cultural and recreational services and the transition from institutional to community-based services. Specific objective: to improve access to primary and emergency health care (at isolated and deprived communities);
- Providing support for social enterprises. Specific objective: to expand social entrepreneurship.

Besides, PA 4 A Socially Inclusive Cross-Border Area has a total budget of €18,4 million ERDF support. During the current programming period 2014-2020, by November 2019, the total number of finalized projects is 22, with a total budget of €16,7 million (€ 13,5 million ERDF funding or 73% implementation).

The first good practice, which results enhance the right to health and social welfare, is "e-Social Health Care". The project budget is approximately €0,8 million (€ 0,65 million ERDF funding). Lead partner is Municipality of Nestos, and the co-partners are Municipality of Topeiros and Municipality of Zlatograd. The e-SOHECA project idea stems from the fact that the partners are located in remote locations and far away from large medical centers, thus the habitants of those areas face severe difficulties regarding the accessibility and quality of fundamental healthcare. The issue amplifies especially when it comes to disabled citizens and habitants who reside in areas that are located away from the urban centers of the municipalities of Nestos, Topeiros and Zlatograd (such as villages and remote settlements), thus increasing the risk of those people to be left without proper healthcare in case of emergency. Overall, the habitants of the cross-border locations often become victims of social discrimination and are excluded of their social rights. This project is tackling these challenges by establishing a responsive e-social health care system which includes advanced medical equipment connected to a web based system, in order to provide ad-hoc healthcare to anyone in need. The overall objectives are summarized as follows:

- to create web medical files for the habitants of the area, where all of the data from the measurements be uploaded and stored, and made accessible at any time via the system by doctors, volunteers etc.;
- to provide health and social care services to elderly habitants and disabled people;
- to give incentives to network participants, which will guarantee project success and sustainability;
- to eliminate social discrimination and promote equal treating and social inclusion of people no matter where they live.

The e-SOHECA system has an indirect effect which facilitates the prevention of medical emergencies and will also contribute to any studies regarding the medical situation of the area, as it will have the capacity to store the measured data (securely, anonymously) in order to provide vital demographic measurements and data for future use. [6]

The second example of a good practice is "Receive Emergency/Daily needed HEALTHcare through innovations in the cross border area". Its total budget is €1,4 million (€1,2 million ERDF contribution) and beneficiaries are Center for emergency care Kardzhali (Lead Partner), General Hospital of Kavala and Medical Association of Kavala. The E/HEALTH project offers improved healthcare across the border region through the application of new technologies. Telemedicine equipped in mobile road vehicles and in hospitals can help overcome the problem of distances and difficult access routes to health care and provide adequate capacity for a number of medical professionals to respond to emergencies caused by transport and/or natural disasters. Some of the goals achieved are:

- Delivery of early diagnostics and therapy equipment and a mobile diagnostic center;
- Supply of specialized equipment for reaction life-threatening emergencies and emergency situations caused by transport and/or natural disasters.
- Specialized seminars for doctors, nurses and paramedics and for emergency management;
- Establishment of a network for exchange of experience and cross-border cooperation to minimize the consequences of incidents in these regions;
- Surveys for Consumer Satisfaction Survey Studies and Analysis Using Advanced Methods;
- Standards for Health and Safety of Workers in Healthcare Structures;
- Campaigns for healthy lifestyle prevention and prevention with early diagnosis measures and exercise/simulation for emergency preparedness. [7]

Another successful project is "Improving quality and accessibility of social health care services in cross-border regions" with a total budget of €1,1 million (€ 0,96 million ERDF funding). Lead Partner is Regional health inspection - Blagoevgrad and the other partners are: "Papageorgiou" General Hospital Center for emergency medical care – Blagoevgrad; Office of Social Protection, Solidarity and Sports and Education of Lagadas Municipality; Organisation of Social Protection and Solidarity of Municipality of Chalkidona. The main objective of the project is to improve the accessibility and quality of medical services to the population in restricted areas and vulnerable populations in order to increase the capacity and effectiveness of the primary care system for better territorial and social coverage for deprived from high quality health services and isolated communities. Project activities focus on actions that promote the quality and efficiency of value-added primary health services and activities such as telemedicine and mobile health services, enhancing cooperation capacities, efficiency and effectiveness for emergency response in the cross-border area, and increased access to healthcare for vulnerable groups (specific to cross-border areas) and/or residents of hard-to-reach border areas.

What is more important, some of the tangible (increased capacity) and visible results (facilitated access for vulnerable groups) are:

- Improving the quality and effectiveness of primary health care for the most deprived areas;
- Enhanced access to healthcare for vulnerable groups in disadvantaged areas with high cross-border mobility;
- Delivery of: 1 pc. mobile unit for healthcare with mobile medical equipment and apparatus, 1 pc. telemedicine equipment; 1 pc. car; laboratory equipment for Regional Health Inspectorate;
- Organization of: seminars for capacity building; programs for training of personnel resources; training modules on telemedicine and on the "Emergency Response Plan and Protocols in Crisis Situations". [8]

Similarly, during the 2007-2013 programming period, the following three projects [9] can be indicated as examples of good practice for protection of the right to health and social welfare:

- Investment in the health and the prosperity of the children in the Bulgarian - Greek region - total budget: €1,8 million (€1,5 million ERDF contribution). Partners: Municipality of Belitsa (Lead) and Region of Eastern Macedonia -Thrace. The project focuses on prevention of the disease among children and youths where it is necessary to build up strong healthy habits and to replace the "online game" with a real sport game. *Outputs:* Building and equipment of a sports hall in the village of Kraishte, with capacity of 50 athletes, 150 seats; joint cross - 10000 parents and 10000 children from the Drama-Blagoevgrad district; 50 municipal and district servants in 2 cross-border seminars. *Results:* ensuring of access to sport facilities for 3500 youths from the Belitsa, Yakoruda and Garmen; ensuring the participation of 100 youths in international sport contest and promoting sports as a prerequisite for physical education and strengthened health;

• Voluntary Blood Donation in Rhodope - total budget: €0,9 million (€0,34 million ERDF contribution). Partners: Region of Eastern Macedonia - Thrace (Lead), District Administration of Haskovo and Region with administrative Centre city of Kardzhali. The project concerns the development of cross border co-operation on the great issue of preventing the transmission of diseases derived from blood transfusion. Two mobile units are purchased in the framework of the project, in order to implement voluntary blood donations, but also to raise awareness on safety issues, through brochures, audio visual materials, seminars and public campaigns. *Outputs:* Purchase of equipment and staffing of two mobile information units, a scientific congress, workshops, actions for informing/sensitizing the local population, informative events in places of education and work, voluntary blood donation, study of best practices, etc.

• Targeted Interventions for the Prevention and treatment of Tuberculosis (TB) and Hepatitis B – total budget: €0,4 million (€0,76 million ERDF contribution). Partners: Region of Eastern Macedonia - Thrace (Lead) and Regional Inspectorate for Protection and Control of Public Health – Smolyan. The main objectives are to define demographical and risk factors that affect and influence the distribution of TB and Hepatitis B, to gather knowledge on the magnitude of the problem and implement preventive measures for the population, to get diagnosis and therapy by case of TB and Hepatitis B, to observe the effectiveness of therapy, to investigate epidemiologically for limiting the spread to family, work, social and extended environment of these diseases, to implement prevention activities. *Outputs:* upgrade scientist interest and obtain technological know-how which will allow for the implementation of activities in general social groups; improve the access and provide health care to individual; improve the effectiveness and efficiency of Public Health Services; protect the health of the individuals; develop common scientific activities towards a continuous exchange of data in the spread of diseases and take joint actions.

## *3. A Comparative Analysis*

Then, in order to research the Greek-Bulgarian CBC effectiveness in enhancing the right to health and social welfare, a comparative analysis is made, containing specific comparison criteria. Therefore, the first criterion is the number of contracted projects - $K1_{projects}$.and the second criterion is the budget needed for the implementation of the projects - $K2_{project\ budget}$.

To illustrate, the collecting and processing data results from the two programming periods 2007-2013 and 2014-2020 are presented at Diagram 1. As a result, the emerging trend is an increase of 14%.

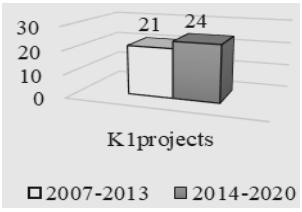



***Diagram 1*** *Number of contracted projects [4;9]*

In the same way, Diagram 2 shows the effectiveness development of CBC between Bulgaria and Greece, in the context of $K2_{project\ budget}$. On the contrary, there is a negative trend of 27% decreasing of the cross-border initiatives total budget, as well as the ERDF funding, contracting for project implementation in the present programming period.

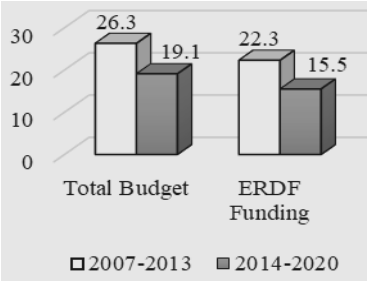



***Diagram 2.*** *Project Budget [4;9]*

## *4. Expected Results and Benefits*

The next task is to summarize the expected results and benefits of the cross-border projects that will be completed by 2023. After all, only 8% of the 2014-2020 cross-border projects are still ongoing its activities. Its budget represents 13% of the total budget and of the ERDF funding for the implementation of all 24 projects with the potential to enhance the Right to Life, and especially, on the right to health and social welfare. (see Diagram 3).

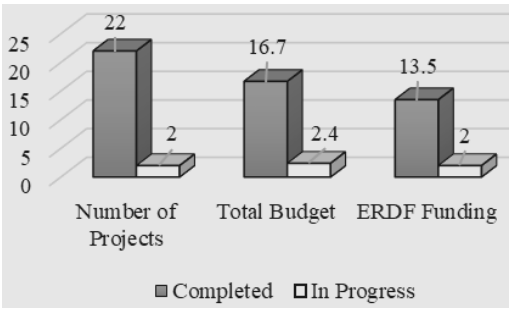



***Diagram 3.*** *Expected results by 2023 [4;9]*

For instance, one of these two cross-border projects is "Reducing access inequalities in primary healthcare for socially significant diseases at CB Area's deprived communities". The Lead Beneficiary is General hospital of Thessaloniki "G. Papanikolaou" - Organic Unit Psychiatric Hospital of Thessaloniki. The other beneficiaries are Cardiology Society of Northern Greece, Diagnostic and Consulting Center "Aleksandrovska" Ltd, Intermunicipal Agency of Western Countryside of Thessaloniki "Nefeli"; Multispecialty Hospital for Active Treatment Devin JSC and Regional Health Insurance Fund of Blagoevgrad. The total budget is €1,2 million (€1 million ERDF funding). The general objective is to reduce health inequalities in cross-border area by protecting citizens from socially sensitive diseases, promoting health prevention, foster supportive environments for healthy lifestyles and encouraging innovation in health. The project will focus on the following categories of diseases:

• main non-communicable diseases (NCDs) mainly cardiovascular diseases (including cholesterol), chronic respiratory diseases and diabetes 40% of the population affected;

• Psychiatric (mental) diseases.

Both of the above categories of diseases are related to deprivation, poverty, inequality and other social and economic determinants of health. Some main delivered outputs are:

• 1 joint "Observatory equal2health for socially significant diseases";

• 2 mobile units for providing medical exams and prevention awareness campaign;

• awareness campaign to main target population and to Medical Staff and Autorities;

• policy recommendation on reducing health inequalities and dealing with the commonly and socially significant diseases. [10]

Likewise, the other one project in progress is "SMART MEDICINE" with the same total budget as the project above. Beneficiaries are: Municipality of Dimitrovgrad (Lead), Eastern

Macedonia and Thrace Institute of Technology and Department of Nursing Paranesti Municipality Legal Entity of Social Solidarity, Pre-school and Education.

The overall objective of the project is to invest in health infrastructure which contributes to regional and local development, reducing inequalities in terms of health status. The purpose of the Project is to improve the effectiveness of the primary health care system and indirectly manage to provide better health coverage to deprived communities shifting from the institutional to community-based services.

The cross-border primary healthcare initiative encompassed in the project will cover the broad range of primary prevention and primary care services within the community. The networked health care providers will have a common base on health promotion and disease prevention, diagnoses, treatment and management of chronic and episodic illness and rehabilitation support. The project involves the coordination and provision of integrated care provided by a range of health providers, including nurses, social workers, pharmacists, dietitians, public health practitioners, physicians and others in a range of community settings including people's homes, healthcare clinics, physicians' offices, public health units, hospices, and workplaces. It is delivered in a way that is person- and population-centered and responsive to economic, social, language, cultural and gender differences. [11]

## *5. Results of discussion*

In brief, the comparative analysis results indicate that the Greek-Bulgarian CBC's effectiveness is not sufficient in the context of $K2_{\text{project budget}}$. Nevertheless, the outputs, results and benefits of the cross-border projects have a substantial impact on the on the Right to Life, and especially, on the right to health and social welfare.

As follows, three main tasks are implemented in this paper:

- Examining CBC achievements in two programming periods;
- Comparing these achievements by two criteria;
- Outlining CBC effectiveness development in a long term period.

## *6. Conclusion*

To sum up, by implementing these tasks, the main goal is achieved. Even more, it does focus attention on good practices with added value in terms of the right to health and social welfare. Moreover, Greek-Bulgarian CBC has a proven European added value in terms of building critical mass, strengthening excellence and exercising a catalytic effect on human security.

In particular, this study provides a methodology that could be used and applied to other cross-border cooperation programmes, on the one hand, and to other human rights, on the other hand.

## *7. References*

*[1] Бахчеванов, Георги. РЕГИОНАЛНОТО ВОЕННО СЪТРУДНИЧЕСТВО В ЮГОИЗТОЧНА ЕВРОПА. В Коларов, Т. (състав. и науч. ред.). Югоизточна Европа: новите заплахи пред регионалната сигурност: Сборник с материали от международна конференция, 2-3 юни 2015 г. Наука, образование, сигурност : Т. 3., С., НБУ, 2016, ISBN 9789545359071, стр. 287*

*[2] "…to protect the vital core of all human lives in ways that enhance human freedoms and human fulfillment. Human security means protecting fundamental freedoms – freedoms that are the essence of life. It means protecting people from critical (severe) and pervasive (widespread) threats and situations. It means using processes that build on people's strengths and aspirations. It means creating political, social, environmental, economic, military and cultural systems that together give people the building blocks of survival, livelihood and dignity." Commission on Human Security. 2003. Human Security Now: Final Report, New York, p.4*

*[3] Радулов, Николай. Сигурност 4.0. Сигурността и четвъртата промишлена революция. В Сборник доклади от Начуна конференция „Актуални проблеми на сигурността", 25-26 октомври 2018 г.,Т.5. Научни направления „Мениджмънт на защитата на населението и инфраструктурата" и „Управление на ресурси и технологии за защита на населението и инфраструктурата". Издателски комплекс на НВУ „Васил Левски" ISSN 2367-7465, стр.25-26*

*[4] Interreg Greece-Bulgaria 2014-2020 [Official site available at http://www.greece-bulgaria.eu/com/4_A-few-words-about-our-Programme, last visited November 5, 2019]*

*[5] Cooperation Programme INTERREG V-A "Greece-Bulgaria 2014-2020" [Online document available at http://www.greece-bulgaria.eu/gallery/Files/2nd%20call-1st%20Phase/1st%20info/Programme_2014TC16RFCB022_2_1_en.pdf, last visited November 5, 2019]*

*[6] e-Social Health Care [Official site available at http://e-socialhealthcare.eu last visited November 5, 2019]*

*[7] E/HEALTH [Official site available at https://ehealth-gr-bg.com/en/ last visited November 5, 2019]*

*[8] Healthcare Center [Official site available at http://healthcarecentre.eu last visited November 5, 2019]*

*[9] European Territorial Cooperation Programme "Greece-Bulgaria 2007-2013" [Official site available at http://www.greece-bulgaria.eu/old/ last visited November 10, 2019]*

*[10] KEEP [Official site available at https://www.keep.eu/project/20361/reducing-access-inequalities-in-primary-healthcare-for-socially-significant-diseases-at-cb-area%25E2%2580%2599s-deprived-communities, last visited November 10, 2019]*

*[11] Ibid. [available at https://www.keep.eu/project/20391/smart-medicine , last visited November 10, 2019]*

# ELECTRONIC ADMINISTRATION OF UNMANNED AVIATION WITH PUBLIC KEY INFRASTRUCTURE (PKI)

M.Sc. Vránics D. F.[1], Dr. Palik M. PhD[1], Dr. habil. Bottyán Zs. PhD[1]
Department of Aerospace Controller and Pilot Training – National University of Public Service, Hungary [1]
vranicsd@gmail.com, bottyan.zsolt@uni-nke.hu, palik.matyas@uni-nke.hu

***Abstract:*** *As Unmanned Aircraft Systems (UAS) are converging an Internet of Things-like infrastructure, always connected to the internet, cryptographic security becomes a primary concern to ensure confidential, but even more importantly tamper-proof transport of data. Another emerging problem is the high number of unregistered drone flights, with no regard towards airspace regulations. The well-established and standardized processes of Public Key Infrastructure (PKI) can be utilized for electronic identification of drones and associating them to the owner, while providing encryption and integrity protection of data. Nowadays various companies provide PKI for drones. This material summarizes the trends, challenges, possibilities of hardware-based on-board secure storage of secrets and describes a possible solution for government-level electronic administration of drones and owners.*
**Keywords**: UAS, DRONE, PKI, CRYPTOGRAPHY, SECURITY

## 1. *Current state and challenges of Unmanned Aircraft Systems*

Civilian drone systems came a long way since their mass introduction to the public market around 2010. Their battery life and flight range multiplied, their payload reduced in physical size and improved in capabilities. From the simple remote-controlled drones, the focus shifted to "smarter", semi-autonomous, high-stability aircraft, equipped with high definition cameras or other advanced payload for various applications for example 3D scanning lasers, multi-spectral cameras or gas composition detectors. [1]

Issues of unrestricted flight and numerous safety incidents sparked DJI's GEO Zones [2] implementation of no-fly zones enables restriction of drone operations in sensitive geographical locations, to prevent traffic collision or prohibited area intrusion incidents by providing a map representation and an underlying database of no-fly zones with flight authorization.

Not all UAS requires heavy user interaction. Agricultural application saw drones mapping fields [3] in an autonomous way, or planting seeds [4] in a recent crowdfunding campaign. With increasing autonomous unmanned traffic and denser airspace, the computation-heavy task of path planning and collision avoidance shifts from on-board to ground-based subsystems in the unmanned flight ecosystem. With the introduction of the latest technology in telecommunication, control and telemetry communication channels get more efficient and reliable, autonomous aircraft can always be tracked or connected in a way during flight. Apart from telemetry, position data and control commands, meteorological data may also be collected in-situ using UAVs. Assimilation of real-time data [5] into a Weather Research and Forecasting (WRF) model can highly improve forecast precision – this being the main scope of our research subproject, codenamed *UAS_ENVIRON* under project GINOP 2.3.2-15-2016-00007, *"Increasing and integrating the interdisciplinary scientific potential relating to aviation safety into the international research network at the National University of Public Service - VOLARE"*. The upcoming introduction of 5th generation mobile networks address the needs of such applications, not only the use case of autonomous unmanned flight, but the Internet of Things (IoT) concept in general, where every device can be connected to the internet.

The IoT architecture usually involves devices, gateways, management service and applications. [6] See Fig. 1. for a hierarchical representation of the IoT infrastructure. Devices collect sensor data, or act upon commands received. Devices are connected to gateways via a comparatively small-range connection (to spare power consumption). The gateways themselves are connected to the management services via internet, where the heterogenous data is processed, aggregated, stored and distributed to consumers. Consumers include other services, or end-user applications, where further processing or visualization of data happens.

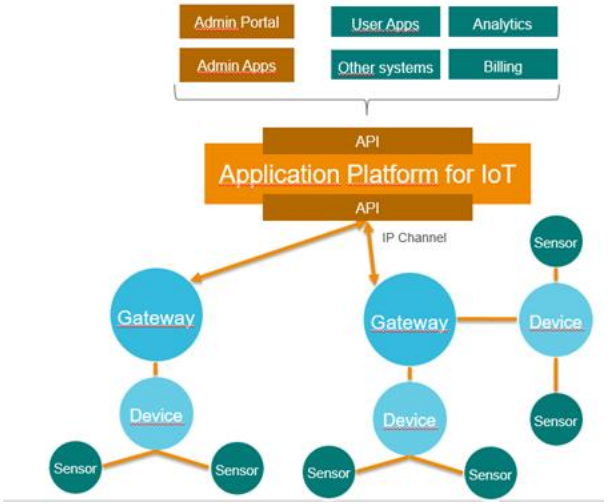



***Fig. 1*** *Ericsson Application Platform for Internet of Things (AppIoT) overview. [7]*

It is not hard to notice similarities of the layers in IoT and remotely tracked UAS. The autonomous drones have on-board positioning devices that produce location data. In some solutions, this data is transmitted to ground stations, which act as the gateway, that sends this data to the central servers, from which it can be visualized on a web-based map display. (Notice that this solution is like traditional offline autonomous drone operation, where the ground station itself acted as the map display.) Another variant is when the internet gateway is located on-board the Unmanned Aerial Vehicle (UAV). In this case, the autopilot integrates the functionality, or an external "modem" is connected to the autopilot module, as demonstrated on Fig. 2.

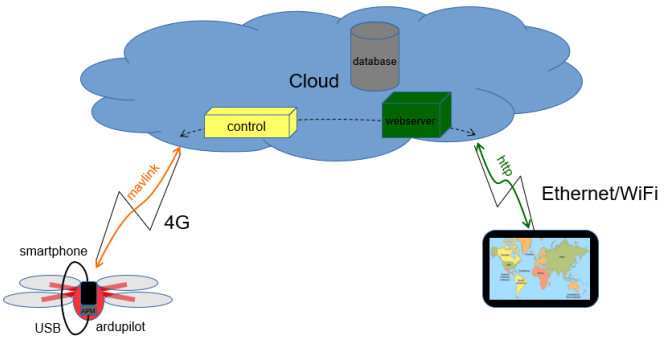



***Fig. 2*** *Schematic drawing of the Author's prototype cloud-controlled Unmanned Aircraft System.*

The above mentioned first, ground-based gateway concept is like the Open Glider Network concept, a tracker system that is

openly available for the glider community, with a low weight radio transmitter solution that already has been experimentally adapted to drone-borne application. See Fig. 3 for an overview of the OGN.

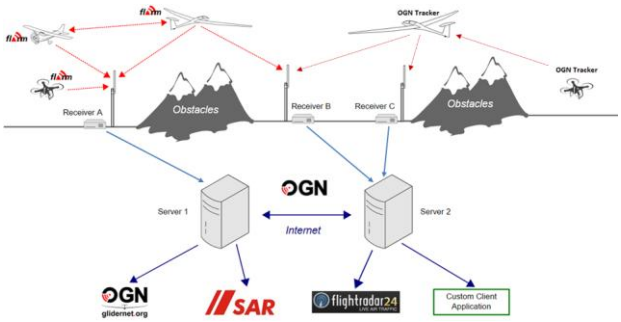



***Fig. 3*** *The Open Glider Network overview. [8]*

Each of the above solutions and systems, IoT, internet-enabled UAS and OGN all require a secure communication channel to ensure the data integrity or in some cases confidentiality. It is easy to recognize that position data and control messages must be sufficiently protected against tampering to avoid hijacking the drones or cause disturbance in traffic control services. Even if the control messages are authenticated and the drone can not be taken over directly, successful spoofing of position information may cause sophisticated traffic avoidance subsystems to command the drone to change its course. This way, a similar outcome can be achieved as in December 2011, when Iranian forces captured a US RQ-170 unmanned aerial vehicle by blocking the communication channels and spoofing the GPS signal and forced it to land in Iranian territory. [9]

Same applies to future systems where UAVs could plan and update their routes based on real-cast and measured meteorological conditions on-the-fly, to avoid thunderstorms and other dangerous meteorological phenomena. If the meteorological data gets corrupted in transit, the model gets poisoned with false data that can leave the UAVs fed with false safe routes to follow in the long run.

The version 2.0 of MAVLink, a common UAV communication protocol supports a way to digitally sign of each message. One immediate observance is that the length of the signature can be compared to the size of the signed data itself, which is not economical for traditional low throughput telemetry channels.

The limited bandwidth is also the reason why the OGN does not support signature of data, as message sizes were optimized for size constraints, and this would be broken by the size of a considerably safe signature field.

For IoT-based drone systems or mobile broadband enabled UAS solutions however, asymmetric key encryption can be a way forward.

## 2. *Basics of Public Key Infrastructure*

This chapter revisits the basics, components and roles in a Public Key Infrastructure (PKI). The concept relies on asymmetric key encryption, a mathematical procedure which involves two keys, a public key and a private key. Together, they are referred to as a key pair. The public key is free to distribute among communication parties, the private key is kept secret by every party. Special mathematical construction of the key pair and related algorithms ensure that data encrypted using one key can only be decrypted with the other key in the pair (i.e. in an asymmetric way), and vice versa.

When A and B are communicating, A can encrypt data with B's public key, and only B with the appropriate private key can decrypt it. When A signs a message using A's private key, B can verify that the message was created by A using A's public key to verify the signature.

The above works between A and B, only if they can ensure that the public keys get exchanged in a completely secure way, otherwise a third-party M can facilitate a Man-In-The-Middle (MITM) attack and eavesdrop the communication between A and B by acting as the opposing party. See Fig. 4. for illustration of the setup.

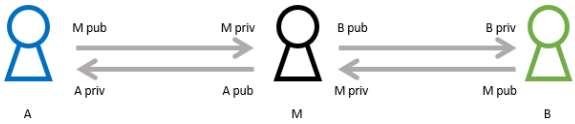



***Fig. 4*** *Setup of a Man-In-The-Middle attack within an asymmetrically encrypted channel.*

To ensure the authenticity of the other party and public key, the concept of Public Key Infrastructure was born.

In an everyday scenario, A can be a person with a browser, who wants to connect securely to a website. B can be the website's web server. For A to be sure it is communicating with B, A must reach a level of trust in the system and infrastructure. To achieve this, B first generates its public and private keys. The private key is stored securely, and the public key is attached to some other data that identifies B. This is called a Certificate Signing Request. This is then sent to a Certificate Authority (CA) or an external Registration Authority (RA), who verifies B's identity, in this case, that B's domain is owned by a legit company, and they are the ones who issued the CSR (in other scenarios, for example an email address can be bound to a person after identifying themselves).

After this, the CA signs B's certificate with its own private key. If A trusts this CA, A can then verify B's certificate and they can commence the secure communication. But how does A know that it can trust a CA? Usually on the highest trust level, the so-called Root CA's certificates are signed by themselves, during a ceremony involving bunkers, armed guards, rolling cameras etc. to ensure the legitimate process and store their private key in the highest possible security. This ceremony understandably is very costly to perform in case of a possible breach of the private key, and all the certificates issued by the CA would be considered compromised. To mitigate this cost, intermediate CA's can be certified by the Root CA's. The Root CA's also work together with big software manufacturers that deploy the root certificates embedded with their software (e.g. browsers, operating systems). This way, A already has root certificate installed in its browser to verify B's certificate, or if B's CA was not a Root CA, then the chain of trust can be verified (as B's certificate was signed by an intermediate CA, whose certificate was signed by a Root CA, whose certificate is available in A's browser by "factory".) A can then be sure that it is B who A is communicating with.

There are still a couple of cases when A could not trust B at this point. B's certificate could have expired, or B's certificate could have been revoked. If B's private key gets compromised, B can contact the CA to revoke the certificate, to prevent impersonation of B, then request a new certificate. In this case, the old certificate gets appended to a Certificate Revocation List (CRL), which can be accessed by A to check if the certificate is still valid. This can be done by reading through the publicly available CRL of an issuer on a CRL Distribution Point or contacting the service via Online Certificate Status Protocol (OCSP), the latter being the less resource demanding way.

If B does not notice the private key getting compromised, the expiration date of the certificate still limits the time an attacker can misuse it for impersonation. The expiration period is usually one- or two-years span. The expiration date is included in the certificate, so A can check this field locally.

The processes involved in PKI are well-standardized, in IETF [10] and Public Key Cryptography Standards (PKCS).

## 3. UAS specific PKI

The main idea is to use client-side certificates on internet-enabled drones to connect securely to the ground-based servers. This way their identity can be electronically verified. To get the certificate, the owners would need to contact an RA in person, which can administer an official identity verification process thus legally linking the drone to the owner.

*"The main problem for a PKI to solve is key distribution and management, which is comparatively easy in closed military environments but very difficult in the open and worldwide system of civil aviation, also tying into the point on compatibility requirements." [11]*

From key management and key distribution point of view, there are two main ways to handle the secret private keys. One is to have the owners generate the keypair themselves, then fill and send a CSR manually to the authorities. This way the only the user possesses the private key, so not even the authorities can tamper with or impersonate the owner – but the owner needs to go through a less user-friendly process to generate the keypair and ensure the secure storage of the private key on the device. The other way is when the authority or a legal proxy generates the keypair and distributes it towards the user in secure ways. These may include distribution of SIM cards or SD cards, USB thumb drives that can be connected to the gateway device, direct configuration of the device (e.g. eSIM), or generating and handing out the keypair in the physical presence of the owner, ensuring it cannot be recovered later. This method takes the burden of keypair generation and upload off the shoulders of the owner but leaves opportunities to compromise the private key during the process.

As quoted above, this process is easier to cover in an isolated, private PKI than integrating the solution to the existing world-wide PKI. To satisfy market demand, multiple companies provide different solutions.

Infineon and PrimeKey have teamed up to provide PKI with secure elements, using OPTIGA™ Trust X and a NC1023 (eSIM). [12] The system is not only capable of authenticating a drone, but also provides means of software attestation, for example, to prevent tampering with the drone's software to circumvent no-fly zone restrictions or altering the autopilot software. DigiCert and AirMap introduced their own solution, which provides a publicly trusted certificate, codenamed DroneID. The solution is first available for drones built with Intel® Aero Platform for Developers, including the Intel Aero Ready to Fly Drone. [13] The solution is mainly aimed towards secure authentication and communication within the UAS.

As for military application, for IoT and UAV identification and attestation purposes, PKI was also considered as a viable solution. Colleagues of the Norwegian Defence Research Establishment considered utilizing PKI and Trusted Platform Module (TPM) chips for hardware-based secret storage and integrity protection apart from their experiments with Gismo IdM identity management system. [14]

On the field of standardization, ITU-T and ISO collaborates on establishment of a new UAV identifier. [15] Object Identifiers (OID) [16] is the proposed solution to be utilized in future, presumably also for the International Civil Aviation Organization (ICAO). Existing ANSI standard describes serial numbering convention of UAS. [17]

## 4. A possible European approach

"*Registration of UAS operators & certified drones becomes mandatory. Starting from June 2020 all drone operators shall register themselves before using a drone." [18]*

Apart from requiring registration of operators, The European Union regulations define different categorization based on the nature of the operation [19] and characteristics of the UAS. [20] For UAS categories C1, C2 and C3 a unique ANSI/CTA-2063 serial number [17] is required, which is physically and electronically represented on the drone itself, and is also electronically broadcasted during operation. During the registration process, serial number, manufacturer and owner data are uploaded to the drone or an external identification module.

To frame the regulations into Public Key Infrastructure concept, the required data could also be used to construct a certificate for electronic identification of internet-capable UAS together with a generated public key. The registration process could take place electronically after adequate authentication of the owner (i.e. via an e-governance portal), or personally in government-certified drone clubs. The e-governance portal or the club would act as a Registration Authority in PKI terms. The Certificate Authority role could be fulfilled by infrastructure on national level, European level (as root or intermediate CAs) or worldwide (ICAO being the root CA). The root CA certificate(s) would also be installed to the drone or tracker system. This way the drone itself could verify other systems certified by the same authority, such as the controller servers and other aircraft on the network during direct communication. The drone's own certificate would be used to authenticate the aircraft in the network before arming and taking off. Depending on the drone platform, the private key could be stored on the device itself in PKCS12 file format, embedded in a SIM card or eSIM, or sealed in a TPM chip or other Hardware Security Module (HSM).

## 5. Conclusion

The need to track and identify autonomous and remotely piloted Unmanned Aircraft Systems before flight is obvious if we observe the standardization and regulation efforts in the European Union or around the globe.

Supporting and expanding the possibilities of the EU regulation framework, Public Key Infrastructure could help secure the communication channels in an UAS to prevent hijacking or disrupting drone operations, while making electronic identification possible.

To achieve this, multiple vendors offer Commercial Off-The-Shelf (COTS) solutions that could integrate the existing regulation framework, while the military also considers internal PKI for IoT and drone applications.

## 6. References


[1] A. Shah, G. Allen, J. Pitt, H. Ricketts , K. Kabbabe, P. Williams, B. Leen, J. Helmore , J. Shaw, P. Hollingsworth, M. Bourn: *Methane flux quantification using UAV sampling*. In: ISARRA Conference, Lugo, 2019, online 15.11.2019.: http://www.isarra.org/wp-content/uploads/2019/08/ISARRA_2019_Wed_Shah.pdf

[2] DJI: *FLY SAFE GEO ZONE MAP*. Online 15.11.2019.: https://www.dji.com/hu/flysafe/geo-map

[3] DroneDeploy: *Drone & UAV Mapping Platform | DroneDeploy.* Online 15.11.2019.: https://www.dronedeploy.com/

[4] Mark Rober: *Using Drones to Plant 20,000,000 Trees.* Online 15.11.2019.: https://www.youtube.com/watch?v=U7nJBFjKqAY

[5] A. Z. Gyongyosi: *Meteorological Data in the Open Glider Network (OGN).* In: ISARRA Conference, Lugo, 2019, online 15.11.2019.: http://www.isarra.org/wp-content/uploads/2019/08/ISARRA_2019_Tue_Gy%C3%B6ngy%C3%B6si.pdf

[6] K. K. Patel1, S. M. Patel: *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.* IJESC Volume 6 Issue No. 5 pp. 6122-6126, 2016, DOI 10.4010/2016.1482

[7] Ericsson: *Overview – Device & Data Management*. Online 15.11.2019.: https://docs.ddm.iot-accelerator.ericsson.net/?page_id=7391

[8] Open Glider Network: *Open Glider Network - Open Glider Network Project.* Online 15.11.2019.: http://wiki.glidernet.org/

[9] L. A. Faria, C. A. M. Silvestre, M. A. F. Correia, N. A. Roso: *Susceptibility of GPS-Dependent Complex Systems to Spoofing*. J Aerosp Tecnol Manag, 10: e0218. doi: 10.5028/jatm.v10.839

[10] Internet Engineering Task Force: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* RFC 5280 Proposed Standard, Fremont, May 2008.

[11] K. Hartmann, K. Giles: *UAV Exploitation: A New Domain for Cyber Power*. In: 2016 8th International Conference on Cyber Conflict, Cyber Power, N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.), NATO CCD COE Publications, Tallinn, 2016

[12] PrimeKey: *Drone safety via security – PKI in action.* Online 15.11.2019.: https://www.primekey.com/blog/2019/05/23/drone-safety-via-security-pki-in-action/

[13] DigiCert: *AirMap, DigiCert Introduce First-Ever Digital Identity Certificate for Drones.* Online 15.11.2019.: https://www.digicert.com/news/2016-12-13-digicert-partners-with-airmap-for-drone-id/

[14] A. Fongen, F. Mancini: *Integrity Attestation in Military IoT*. In: IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, 2015, DOI: 10.1109/WF-IoT.2015.7389102

[15] A. Rutkowski: *ITU-T Takes Lead on Drone IoT Identification in 2019.* Online 15.11.2019.: http://www.circleid.com/posts/20190103_itu_t_takes_lead_on_drone_iot_identification_in_2019/

[16] International Telecommunication Union – Telecommunication Standardization Sector: *Identification mechanism for unmanned aerial vehicles using object identifiers.* ITU-T X.677 (ex X.uav-oid) work item, Geneva, 2019.

[17] American National Standards Institute: *Small Unmanned Aerial Systems Serial Numbers.* CTA 2063-2017 (ANSI standard), Washington, 2017.

[18] European Union Aviation Safety Agency: *Civil drones (Unmanned aircraft).* Online 15.11.2019.: https://www.easa.europa.eu/easa-and-you/civil-drones-rpas

[19] European Commission: *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance.)* EUR-Lex, Document 32019R0947, Brussels, 2019.

[20] European Commission: *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.* EUR-Lex, Document 32019R0945, Brussels, 2019.


## 7. Funding

This work was supported by the European Regional Development Fund (GINOP 2.3.2-15-2016-00007, "Increasing and integrating the interdisciplinary scientific potential relating to aviation safety into the international research network at the National University of Public Service - VOLARE"). The project was realised through the assistance of the European Union, and co-financed by the European Regional Development Fund.



# COUNTERACTION TO SMOLDERING CRISES IN THE NATIONAL SECURITY SYSTEM

Markov N.
Department of National and International Security – New Bulgarian University, Bulgaria
nmarkov@nbu.bg

***Abstract:*** *A model of integrated approach for indication, analysis , correction and sustainable management under the conditions of a smoldering crisis*

**Keywords**: SMOLDERING CRISIS, SECURITY SYSTEM MANAGEMENT, INTERNATIONAL SECURITY, SYNERGETIC EFFECT;

## *1. Introduction*

What characterizes the management of the processes under crises conditions is the implementation of specific methods, plans and decisions. This type of management is based on an empirical set of preventive measures for overcoming crises and on the controlled consequences of their implementation.

The classical approach to overcoming a crisis by means of security system management bears its own peculiar features. They can be described as having a typical and temporary but also very strong inclination for breaking some of the general principles of the security system. This stems from the very peculiar environment, the types of tasks and the way in which each crisis in the management sector arises and presents its unique features.

There is no connector between the process of mastering a crisis and an adequate, effective and integrated methodology , which must recognize the preconditions for the crisis in a chronological order. Most of the preconditions are results from already existing smoldering crises in management. The so needed Revolution in the expert and professional consciousness, connected to the way of perceiving a smoldering crisis ; the integrated approaches for research, the understanding, the interaction and the main features of the environment , where they are generated and established, are the fundamentals for the sustainability of the security system management under the particularly risky conditions.

The understanding of a crisis as an emergency situation and the symptoms of a smoldering crisis as an integral part of a real crisis – this is where the danger for overcoming this intricate process lays. The effective management of the various resources, needed for the proper correction and control as well as the time for their implementation are key elements of the initiative for imposing stability. The surplus value of the modern crisis management models is also the opportunity to profit from this hazardous condition.

There is a natural connection between the national and the international security systems. It is a result of logical processes, which are consequences of implementing agreed situational algorithms within specific conditions and environment. The possible threats for breaking this interconnection originate in the lack of unified assessment, timely indication , definite levels of analysis and control, as well as an incessant monitoring of latent phase crisis.

## *2. Analysis*

### *2.1 Preconditions*

The profound scientific research and the expert definition of the potential and precise weaknesses in the security system management model together with the parallel account of the potential and obvious risks and threats as consequences of a management smoldering crisis, are the prerequisite for the urgent and reformed decision-making. The general precondition in this case is the secret yet permanent distrust of the state administration towards the structural units of the national security system and the threatening possibility to be caught in a deliberate interdependence and manipulation.

There is a mistake in the widespread belief that if the structural unit activities of the system are innovated it will necessarily lead to a change in its nature as a whole. In fact, lacking an integrated mechanism for incessant control and correction to guarantee the effective and objective use of resources, can deeply damage the quality and the value added.

A substantial administrative challenge to the existence of a sustainable management under the conditions of a smoldering crisis is the frustrating inadequacy of the political class, which impels the system retrogression – a result of the political class ineptness to define and use the results of the national and international security systems work reasonably and confidently.

We face the existence of an inevitable problem in the established law order to prescribe a communication between the political and the expert lack of experience.

But there is a permanent lack of balance on the field of the international relations too, despite the incessant claims for restoring the balance. But the mere observation of the past and the foreseeable future processes leads us to the conclusion that the international relations will stay as they are – in a dynamic and uncertain phase, which is contrary to the expected synergetic effect from the collaboration in the field of international security.

In such an international background the tension among the global political and economic agents will mount and lead to hidden and obvious confrontation. More and more of the present regional powers like Turkey, Iran, Israel etc. will have military and political claims to be recognized as global powers. This process will go hand in hand with the deliberate retreat from the already signed and acknowledged treaties and contracts.

In particular, it will become more difficult to create a unified definition of a potential and specific threat together with a joint definition of our mutual interest. The specialized joint operations can only reach the level of a regional political-military cooperation or combined efforts against the organized crime, which involves the protection more of national interest than of international ones.

Bearing in mind the recent management crises, the current crises indicators do not give timely account of the real processes because of the lack of a unified measurement system both at a national and an international level.

If we give a complex recognition to these preconditions, the concept of stable management of the national system security is left out of its own potentials in the hypothesis of a modern, flexible, pragmatic and effective security.

### *2.2 Means of resolving*

The innovative models of management set the question about the possibilities and direct benefits from every crisis. The reflection of these models can be seen in many of the developed countries strategy documents which are an expression of defined social characteristics.

The security system management under a crisis conditions would go through a severe trial without an integrated approach and an intelligent analysis system of the preconditions for smoldering crises. This implies the creation of a new type of a security infrastructure, as well as the methods and forms of its realization:

- New quantity and quality of the security system, based on some unpopular technologies and well- developed potential possibilities for their effective application;
- Preventive activities and operations, reflecting the internal and external smoldering crises and the development of flexible mechanisms for preventing the existence of external control over the preconditions;
- A total security system management and control, fulfilled with some specialized team resources – experts and scientists, so that flexible and stable models, based on the development of the human artificial intellect could be created;
- A short-time access, processing and analysis of huge information bases with practically no subjective factors influence;
- The creation of synergic quasi-models, constructed over some methods of destructive usage of the counter-forces and means for adding an own additional value;
- The determination of the logistic apparatus of the security system;
- A preventive indication, objective assessment and a quick reaction to each and every crisis, with a special emphasis on the segment in a lethal phase;
- Aim-directed resources for providing of an adequate and innovative base for specialists education and training;
- New implementation of the fundamental sciences in a combination with the capacity and the technical abilities of the high technology integrated artificial intellect;
- Foresight of the potential abilities for an adequate and effective reaction as a tendency to entering the conditions of a partial or a full security system decentralization;
- Operational abilities for shrinking and enlargement, depending on the challenges as well as the existence of some private capacity to guarantee the steady autonomy regime work;

## *3. Conclusion*

The international structures as cyber-trusts , quasi-states, private armies / G4S, Wal-Mart, Unity Resources Group, Erinys, Asia Security Group, DynGorp, Triple Canopy, Aegis Defence Services, Academi, Defion International, Vagner/ and financial trusts, managing more than half of the international capital in the field of the informal economy as well as some specific forms of work of the non-governmental organizations, achieve the synergetic effect which , to this moment, exceeds the possibilities of each state.

The achievements of the automation and the following high-tech robotization are capable of changing the philosophy of the whole strategy towards a flexible and steady management of the national security system under the conditions of smoldering crises.

The next half a century will mark the beginning of the competition between the machines, which will change the ways of using personnel. Some global means of intelligence, a controlled influence over the environment and some “laboratory created” conflicts will be realized by logistic centers with minimum of operators but with maximum of effectiveness.

The indication, reflection and the reaction against diverse smoldering crises will turn out to be the next essential science for survival, stability and prosperity.

## *References*

[1] Drucker, Peter. Managing for the future., New York: Harper Collins, 1992;

[2] Radulov, N., Security 4.0. Part One: Security and the Forth Industrial Revolution, Int. sciantific jurnal Industry 4.0, STUME, 2019;

[3] Radulov, N., Artificial Intelligence and Security, Int. sciantific jurnal Security & Future, STUME, 2019;

[4] Dunning, David; Johnson, Kerri; Ehrlinger, Joyce; Kruger, Justin (1 юни 2003). "Why People Fail to Recognize Their Own Incompetence". Current Directions in Psychological Science;

[5] Kissinger, Henry**;** *World Order* (New York: Penguin Press, September 9, 2014)

[6] James, Hayes Erica and Wooten, Perry Lynn; “Crisis leadership and why it matters”; European financial review, 2011;

[7] Institute for crisis management; Annual Crisis Report, 2018;

# AN ATTEMPT TO SUMMARIZE THE PSYCHOLOGICAL PORTRAIT OF PERPETRATORS OF ORGANIZED CRIME

Assoc. Prof., Madzharov, E. A.,PhD, Academy of the Ministry of the Interior, Sofia, Republic of Bulgaria
e.madzharov@abv.bg

***Summary**: The summary psychological portrait of organized crime perpetrators includes a synthesized characteristic of their motivation, attitudes and values. It presents the specifics of their self-esteem, mental states and personal defences. The report analyses empirical data of organized crime individuals obtained through the Dark Triad questionnaire.*
*The overall psychological portrait of organized crime perpetrators is oriented towards supporting the operative-investigative, investigative-judicial and penitentiary activities with them.*
***KEYWORDS**: ORGANIZED CRIME, VALUES, MOTIVES, ATTITUDES, MENTAL CONDITIONS, PERSONAL DEFENCE, MACHIAVELLIANISM, NARCISSISM, PSYCHOPATHY.*

## *1. Introduction*

In today's high-tech and global society, organized crime is successfully adapting, effectively and illegally possessing and managing considerable financial and material resources, corrupting many governmental and municipal officials. [7, 8 ,5]

The tasks related to scientific and applied psychological research to support the police, investigative and penitentiary activities, which are directly involved in counteracting and limiting the scope of organized crime, are becoming increasingly relevant and socially important. In this context, an important place is occupied also by the study of personal and psychological specifics of persons from organized crime groups and the creation of a comprehensive, integrated portrait thereof to facilitate the hard and strained work of operative officers, investigating policemen, magistrates and penitentiary employees.

## *2. Prerequisites And Ways To Solve The Problem*

Various attempts have been made and different approaches have been implemented to describe, analyse and interpret the individual-personal characteristics of organized crime persons. [14, 12, 20, 22, 17]
A number of publications [22, 23, 13, 19] emphasize the importance of the group context for the structuring and functioning of organized crime, but its full, consistent and meaningful impact on the offender's personality is not sufficiently clarified.
Most authors [10, 16, 21, 18] make a functional criminological and sociological characteristic of the organized criminal group. In this presentation of its phenomena, the personality is blurred and disappears in the group, and its psychological specificity is not interpreted. In fact, it functions in a group context that enhances or suppresses some of its specific qualities, characteristics and behavioural features. Undoubtedly, the organized criminal group creates a sense of security, initiates and maintains high claims, self-respect and self-esteem. It increases risk and adventurism aptitude, increases aggression and cruelty, helps to intensify mercenary and utilitarian motivation, develops loyalty and identification with the other members.
In most criminal-psychological publications [10, 21, 17, 12] on organized crime groups, the personal characteristics of the persons involved therein are reduced to presenting the personal qualities and characteristics of their leader. Most often they are characterized as inventive, ambitious, decisive. The leader of an organized crime group is fast in finding ways in the situation and making decisions in complex situations. Under the guise of benevolence and decency, they often conceal their cruelty, prudence, injustice, vindictiveness. The leaders of an organized crime group are able to influence its members and obey them at will. They seek out and establish socially prestigious contacts with reference persons. This type of criminal leaders try to hold on to their position, maintain their image, displaying refined manners and communication skills in different situations. [10]
We can assume that the analysed leaders express a number of qualities inherent in the people of the organized criminal group and in this sense their personal characteristics are universal. To some extent, this statement may be true, but in the creation of a generalized portrait of the offender of organized crime, some of the personal characteristics will disappear, others will not play a leading role. All this is important in order to direct the police, judicial and prison staff immediately involved with specific offenders more accurate.
Organized crime publications [15, 17, 12, 20] address personal psychological characteristics, but do not refer to an overall portrait of the offender, which includes many interconnected components that influence the unfolding of criminal activity. Particular attention is paid to the motives for participating in various organized crime groups. A priority in this area is to emphasize the role of beneficial incentives, expressed in the pursuit of fast and unscrupulous enrichment, greed, parasitism or hopeless financial condition, due to lack of means of subsistence, multiple debts, the acute need for financial resources due to the need to satisfy alcohol or drug addiction.
An important motivation for the participation in organized criminal groups is the dependence on an influential person from the group associated with the sense of duty, fear of retribution, wish to obtain criminal authority, friendly relations, striving to support a particular group member, common spending of time, shared entertainment, increased sensitivity to risk and adrenaline experiences, infestation with criminal romance.
Some of the members of organized crime groups are motivated by the seeking of self-affirmation, the acquisition of autonomy, proving that they are no worse than others, the emphatic desire for revenge, earlier promises made, the specific obligations of the individual from other influential participants in the group. [15]
Studies by individual authors [6, 2, 7, 8] explicitly or implicitly promote the idea that individual psychological and behavioural characteristics typical of traditional crime have more intense and hypertrophied manifestations of organized crime offenders.
Differentiation of personalized roles in organized criminal groups leads to highlighting the personal characteristics of their holders [11, 19, 23, 13]
Despite the peculiarities of their group status, functional roles and commitments, the participants in organized criminal groups have common universal personal features, qualities and characteristics that to a certain degree are typical of them all. In our opinion, based on existing research, conceptual statements, practical observations and numerous publications, the universal, generalized personal features and components inherent in the psychological portrait of the offender of organized crime should be formulated in priority. Once this has been done, passing from the general to the private, we can seriously work to their further specification, with due regard for the role of the group context.

## *3. A Solution To The Studied Problem*

The complete generalised psychological portrait of an organized crime offender should include the following interrelated components:
* The value orientations of the persons of organized criminal groups are mercenary utilitarian. [1] They are dominated by hypertrophied

consumer attitudes that are structured based on nihilistic attitude towards others' property and the pursuit of luxuriant life and parasitism of a compensatory nature because of experienced shortage, misery and narcissistic trauma. [9]

The mercenary values tendency positively corresponds to the features of narcissism and Machiavellianism in persons of organized criminal groups. [4] Therefore, they tend to overestimate their uniqueness, to disrespect property rights and personal autonomy of others, to combine violence and cruelty with manipulation in order to achieve criminal goals;

* The mercenary motivation of enrichment is actually an expression of the desire for domination, power, control and retribution. It is characterized by elitist attitudes, representing involvement with the elect, for whom criminal activity is a profession and a way of life that they systematically pursue because they are protected, inaccessible and secure in their actions. The high motivation for material prosperity and well-being masks, and in fact provides, a large space for the realization of great egocentricity, the strong desire to emphasize one's own uniqueness, superiority and elitist orientation;

* Self-esteem of persons from organized crime groups is compensated and inadequately increased due to their criminal status and activities and the financial resources, property and ownership acquired with their help. Maintaining high self-esteem is a leading and sustainable motive among organized crime participants, actively using the material and financial attributes received from the criminal activity;

* The problematic socialization of offenders from organized crime groups, the specifics of their motivation and self-esteem condition the frequent occurrence of such mental states as high social anxiety, frustration, anger, affectation. Organized crime representatives are in a compensatory vigorous search for relaxation, emotional excitement and adrenaline experiences, both in the high risks of criminal activity and in the violent-sadistic behaviour towards their victims.

* Organized crime persons apply a number of psychological protections typical of them in their criminal activities and interactions. They do not subdue or retain their negative emotions, but rather easily direct them to the people with a lower social status around them. Representatives of organized crime groups quickly shift, transform and rationalise their negative experiences. They are able to quickly reduce their own guilt and pass it on to the victim, the situation and the law enforcement system. Offenders of organized crime groups strongly reject any attempt to identify themselves as a criminal.

* Our research [4] on the personal features of convicted organized crime prisoners in Sofia prison showed that in conditions of isolation and external control, their high narcissism and psychopathy (disregard for existing legal and moral standards) manifest in indirect and conspiratorial forms. They disguise and express themselves through their inherent high Machiavellianism representing their tendency to manipulate other people and treat them primarily as a means to achieve their own goals.

## *4. Results And Discussion*

Mercenary-utilitarian value orientation of offenders of organized crime determines their greed, covetousness and mercantilism which materialise in their destructive attitudes to property of others and sustainable antisocial desire for its seizure and possession. [3] These personal features and attitudes express the outer and peripheral layers of the value orientations of the analysed group of offenders. In its deeper and central layer, the basic values of superiority, uniqueness and elitism can be identified. These generalized and poorly reflected value constructs are the result of the compensation for the difficulties, deficits and traumas of the sensitive periods of socialization of persons in organized crime groups. [9]

Mercenary-utilitarian value orientation of offenders of organized crime is related to the entire spectrum of mercenary motivation whose presence is found in intensive user-consumer attitudes, the underlined striving to ensure luxury, material prestige and in the rigid fixation on the external attributes of material status and prosperity. All these tendencies are the external projection of the motivation for self-assertion, domination, control and achievement of retribution. The specified types of motivation are based on the final results achieved. However, in the organized crime groups there is also a game type of motivation, where the offender is focused primarily on the very process of the criminal activity and the risks and dangers causing adrenaline experiences involved therein.

Organized crime perpetrators' self-esteem is sustainably maintained as being inadequately heightened to offset inferiority experiences, personal insecurity and social anxiety. In reality, this is achieved by actively engaging in criminal actions, risky adventures, by identifying with the group, by demonstrating their own pretentiousness and by successfully coping with various difficulties.

The psychological protections of persons from organized crime are generalized, but more flexible and cognitively complex than traditional criminal offenders. They are structured and function on the basis of a positive self-image, serious group support and inadequate heroization of this type of offenders in the criminal world as well as in society and the media.

The psychological protections of individuals from organized crime reflect their philosophy about their prestigious business activities, their significant public role, and their presence in the community as respectable citizens.

Representatives of organized crime in the course of their criminal activity develop effective coping strategies, transformation of their negative emotional and guilty experiences into positive, affected and ensuring their internal comfort. Thus, they contribute to the stabilization of self-esteem and the successful unfolding of criminal motivation and the exculpation defences of organized crime representatives.

Organized crime group persons possess high Machiavellianism, Narcissism and Psychopathy. At their communication with police, court, and prison officials, they tend to conceal and disguise these personal specifics. Then Machiavellianism comes to the fore, through which narcissism and psychopathy receive mediated and indirect expression. [4] Thus, offenders of organized crime realize some more socially acceptable behaviours, allowing them to secretly and consistently perform their criminal conceptions in penitentiary facilities as well.

## *5. Conclusion*

Mercenary and utilitarian values representing the personal significance through the possession of other people's property and hypertrophied consumption are leading among organized crime persons. Personal significance is embodied in the experiences of utilitarianism and superiority, which fully function as the elitist attitudes characteristic of organized crime groups.

The utilitarian-mercantile motives for ownership, possession and parasitic consumption in their real psychic nature express the desire for self-assertion, which we identify in the desires for ruling, domination, control and influence of participants in organized criminal groups.

Even in cases of retribution, which we consider to be a specific asocial form of self-assertion, there are ruling intentions and the exercise of control and influence.

Self-realization motives are another important part of utilitarian-mercantile motivation. They, more than the motives for self-affirmation, are fixed on the criminal process itself. An essential part of them are game motives, thanks to which we observe risky adventures, ingenious and heuristic solutions in criminal activity and the enjoyment thereof.

The self-esteem of the organized crime groups representatives is compensatory inflated and its maintenance is a kind of self-motivation, closely linked to criminal activity.

Inadequately high self-esteem determines pretentiousness, high self-respect, positive self-image, demonstration of well-being and prosperity. In most cases, it is based on engaging in long-lasting and successful criminal activity, identifying with a prestigious

community and group and receiving protection, approval, support and solidarity therefrom.

Representatives of organized crime are both able to relax their negative emotional states and successfully transforming them into emotional and adrenaline experiences.

The mental protections of offenders from organized crime groups are cognitively complex, plastic and ensuring their successful exculpation. They function through the mechanisms of rationalization, projection, substitution and negation.

The mental defences of persons from organized crime groups guarantee their positive self-perception, keeping distance from the identification with the criminal role, and their legitimate social presentation in society.

The offenders of organized crime are characterized by high scores on the scale of Machiavellianism, narcissism and psychopathy. In the event of difficulties and dangers in their criminal activity arising from their specific interactions with police, judicial and prison system they tend to disguise their high manifestations of narcissism and psychopathy behind their Machiavellianism.

The uniqueness, superiority and elitism of organized crime representatives support their high motivational standards for self-affirmation and self-realization. They are also the basis of their increased self-esteem, which stimulates aggressiveness, adrenaline experiences and successful relaxation in the course of the organized criminal activity realization.

Mental protections, with their orientation, way of functioning and flexibility, preserve the asocial values, motivation and high self-esteem. Thus, they contribute to the sustainable reproduction of criminal activity that is typical of participants in different types of organized crime groups.

The uniqueness, desire for superiority, elitism, the motives for self-affirmation and self-realization, inadequately inflated self-esteem, aggression-adrenaline experiences, flexible adaptive and exculpatory defences directly correspond, nurture and receive expression in Machiavellianism, narcissism and psychopathy in organized crime offenders.

The proposed generalized psychological portrait of organized crime offenders is not just a theoretical abstraction, it is a synthesized conceptual model, reached through the analysis of numerous publications, empirical studies and practical observations. In this sense, it can be widely used in the development of various methodological aids and didactic forms, directly oriented to support the operative-investigative, investigative-judicial and penitentiary practice with representatives of organized crime.

## *6. Literature*


1. Aydarov, J., Criminology. S. Ciela, 1998, p. 164
2. Karakashev, V., Criminology. S. ROMINA, 1998, pp. 282-283 (Karakashev, V., G. Georgiev, P. Tsankov)
3. Madzharov, E., Psychological portrayal of offenders. S. Ciela, 2006, p. 288
4. Madzharov, E., The Study of Organized Crime Persons with the Dark Triad Questionnaire. Psychological Research №1, 2019 (under print), p. 2, p. 7 (Madzharov, E., V. Tsanov, D. Georgieva)
5. Paunova, L., Organized crime. S. Ciela Soft & Publishing AD, 2010, p. 238 (Paunova, L., P. Datsov)
6. Pushkarova, I., Forms of organized criminal activity under the Criminal Code of the Republic of Bulgaria. S. „St. Kliment Ohridski", 2011, p. 112
7. Stankov, B., Organized crime. S. Albatross, 2002, p. 10, p. 175
8. Stankov, B., Criminology. Types of crime. Varna. Chernorizets Hrabur VSU, 2003, p. 290, p. 300
9. Stoychev, N., Violence. Psychological analysis of the crime scene. S. Trud, 2016, p. 19, p. 49
10. Aminov, I., Legal psychology. M. UNITI-DANA, 2012, pp. 132-133
11. Gyurov, A., Professional Crime: Past and Present. M. "Legal Literature", 1990, p. 54
12. Dedulin, D., Psychological means of detecting false testimony in the process of questioning suspects (accused) of economic crimes. M. "Academy of Economic Security of the Ministry of Internal Affairs of Russia", 2011, p. 13
13. Korneeva, G., Organized crime as a negative socio-psychological phenomenon. Applied Legal Psychology. No. 3, 2008, p. 102.
14. Kudryakov, Yu,. Identity of the person convicted for mercenary crimes. V: p/p Mokretsova, A., V. Golubeva, A. Shamisa. Working book of a penitentiary psychologist. M. "VNII of the Ministry of Internal Affairs of Russia, GUIN of the Ministry of Internal Affairs of Russia", 1998, p. 129
15. Pastushenya, A., Kinds and psychological characteristics of criminal groups. Psychological characteristics of the criminal subculture. V: p/p Furmanova, I., I. Metlitskiy Criminal psychology. Minsk. Minsk Institute of Management, 2007,181.
16. Pastushenya, A. Legal Psychology. Minsk, Ministry of Internal Affairs Academy, 2015, p. 88 (Pastushenya, A., A. Urbanovich)
17. Romanov, N., Criminal groups and the criminal subculture. Psychology and law. No. 1, 2013, p. 35
18. Stolyarenko, A., Applied legal psychology. M. UNITI-DANA, 2001, p. 64
19. Stolyarenko, A., Applied legal psychology. M. UNITI-DANA, 2005, p. 93
20. Sorochan, V., Legal psychology. M. "MIEMP", 2010, p. 60
21. Shikhantsov, Legal Psychology Maggazine, "Mirror", 1998, p. 38
22. Chufarovskiy, Yu., Legal psychology. Questions and answers. M. Exmid, 2005, p. 194, p. 320
23. Chufarovskiy, Yu., Legal psychology, M., Prospect, 2015, pp. 280-281

# DEFINING THE STRATEGIC CENTER OF GRAVITY OF HEZBOLLAH

Ph.D. student: Faisal Warikat of Security Studies in National University of Public Service
Email: Faisal.Warikat@uni-nke.hu

**Abstract**: *This article is about the strategic center of gravity of Hezbollah; Hezbollah is one of the toughest, and persistent semi-state actors. The author claims that Hezbollah's state-sponsorship by the Islamic Republic of Iran is its strategic center of gravity (CoG). For identification, this paper starts with the definition of the CoG; lists the main possible CoGs ,and then determining the closest one to be the strategic CoG.*
***KEYWORDS**: CENTER OF GRAVITY, HEZBOLLAH, ISRAEL, 2006 WAR*

## 1. Introduction

Semi-state actors (SSA) are those non-state actors whose status is less than state and more than non-state, they try to have rights and privileges to challenge states and provide services to citizens equal to the offered services by the legitimized rules, they have at least de-facto international legitimacy. Hezbollah is a clear example of non-state actor playing the role of semi-state actor.

This paper intends to investigate the strategic CoG of Hezbollah, taking into consideration its history of wars with Israel, and its capability inside the Lebanese communities.

Most of the similar studies tend to highlight ideology as the main CoG for such organizations, while this paper acknowledges the importance of ideology, nevertheless ideology can be sacrificed by those organizations if it contradicts with their survival and adopts political pragmatism instead.

The second uniqueness of this paper is that it starts with identifying the pillars of strength ( broader than the definition of critical capabilities), and suggests that this concept applies to most of semi-state actors.

The assumed definition of the pillar of strength is the capability that is owned by the non-state actor that gives it the ability to survive and influence other actors.

In July 2006, Israel waged War against Hezbollah with all its military might, during which it launched more than fifteen thousand air sorties to target over (7000) targets inside tiny Lebanon.

That War, was the longest in Israel's history, at the end, Israel failed to fulfill some of its announced targets, which were: build the image of deterrence, safe return of the two abductees soldiers, destruction of the Hezbollah's military capabilities, return of sovereignty to Lebanon's government, and assist it in taking its responsibility over the southern part of Lebanon in accordance to the UN security resolution 1559[1].

At the end of that War, Israel failed to put an end to Hezbollah's military capabilities, Hezbollah succeeded in building a de-facto model of the possibility of defeating Israel when it managed to survive the massive number of Israeli artillery shells and the extreme use of Israel of its Air Force capabilities augmented by three divisions on the ground. Hezbollah managed to keep and gain the sympathy of the Arab population by its effective use of media especially the Al-Manar TV station, also convinced ordinary Arabs that their states' models are not credible competitors to the Israeli army, when with less than that force Israel defeated three Arab armies within six days. The concept of center of gravity was mainly developed by the Prussian military practitioner and theorist Carl Von Clausewitz in his book 'On War.' Clausewitz provided an insightful study for this concept, but his main contribution is that his idea is still triggering modern military researchers to find solutions for some points of that concept, one brilliant point of Clausewitz center of gravity was his writing in Chapter four:

*In countries subject to domestic strife, the center of gravity is generally the capital. In small countries that rely on larger ones, it is usually the army of their protectors. Among alliances, it lies in the community of interest, and in popular uprisings, it is the personalities of the leader and public opinion. It is against these that our energies should be directed* [2,3]

Theorists of Joint operations later developed the Clausewitzian concept, it is still valid, but needed some reconstructions, that enhances its ability to tackle contemporary issues like the 4th generation of warfare.

Defining of CoG is not a straightforward, linear task, as it looks for some, but it is part of the art of military design, which makes it different from one perspective to another according to the angle of their perspective, even when correctly defining the CoG, still proper planning is needed to deal with it, in compliance with the strategic military and political objectives.

Questions like: do we want to destroy the CoG, neutralize it, does the neutralization leads to the ultimate destruction of it, or the objective of its determination is merely to avoid targeting it.

A good example of this is the US missile targeting of the Syrian Shairat military base as a result of the Syrian regime use of chemical weapons in Khan Shaikhon in a blunt defiance to the US red lines.

The CoG could be the Bashar al-Asad, but the US administration did not have in its mind to cause the collapse of the regime, they even were reluctant about the targeting as it could at that moment of history accelerate the undesirable regime's collapse.

In this research, the focus is narrowed to the strategic CoG of Hezbollah. Hezbollah has its uniqueness. The main definitions that relate to the CoG are [4] :

**Critical capabilities**: the primary abilities essential to the accomplishment of the objective that merits a COG to be identified as such within a given context.

**Critical requirements**: essential conditions, resources, and means that the COG requires to perform the critical capability. These are things that are used or consumed to act, enabling a critical capability to function wholly.

**Critical vulnerabilities**: critical requirements or components thereof that are deficient or vulnerable to neutralization, interdiction, or attack in a manner that will achieve decisive results.

## 1. Methodology

The method to be used is extracted from Eikmier [5] and Dr. Strange's method[6] with modification so that it can reflect the case of non-state actor like Hezbollah..

The start is with the identification of Hezbollah's primary objective, which is its desired end state, then the ways that the group can use to attain that end state, later out of his pillars of strength, selection of the most appropriate one by which Hezbollah can do the required action and use the proper means in order to achieve the goal.

## 2. Analysis

This research deals with the CoG of Semi-state actor, which is more difficult to describe than states and their conventional armies; the difficulties are in the existence of more than one CoG for these organizations, the other point is that they morph from one shape to another. In this case of study, the main pillars of strength of Hezbollah (Requirements) are:

a) Political Leadership
b) Military Capabilities
c) Financial assets
d) Public support
e) Ideology
f) Alliances or state-sponsorship

The desired end state of Hezbollah is controversial , but it is believed that nowadays that it lies in providing Iran with a deterrence tool from instigating any war against it, other suggested objectives can be the destruction of Israel which seems to be an unrealistic objective, third proposed objective can be the building of an Islamic state inside Lebanon which was main point of the 1985 Hezbollah's open letter, but that objective was canceled by the arrival of Hassan Nasserallah as Secretary General of the Party of God.

The ways to attain those strategic objectives are through: building strong military capabilities, recruit agents, provide social support to Shia community, build ties with Palestinian movements. In order to manage those ways, Hezbollah is in need for high level support which cannot be provided by less than sponsorship agreement with Iran.

Hezbollah provides consultation and training services to multiple armed organizations in the region, and has a direct control by the Iranian Qudos Brigade. The CoG of Hezbollah can be one of the above mentioned pillars of strength.

**Political Leadership**

The political system of Hezbollah is manipulated by the Shoura Majlis, Political bureau, and charismatic leader who does not have competitors. Still, Hezbollah, with its organizational maturity, developed the system of the sustainment of the leadership in the face of leadership targeting that Israel embraced against it.

**Financial Assets**

Hezbollah has a network of social organizations, which means that it does need economic support, Iran acts as a financial supporter of many of Hezbollah social activities.

**Armed Forces**

Hezbollah enjoys an excellent armed force which can be considered as an operational CoG, yet cannot be regarded as the strategic CoG.

**Ideology**

Counter-terrorism researchers like to focus on ideology and consider it as one of the utmost privileged factors for survivability, though this is not the real case. At times of existential threats, Shia ideology allows practicing Toqiya (Religious dissimulation), where they can better survive the ostensible threats. Besides, Hezbollah practice of political pragmatism to attain his objectives.

**Financial Assets**

This point is connected to the state-sponsorship to a small extent, but the organization is also diversified its resources, it gets one-fifth from its supporters annual revenues. It has local supports and from abroad, especially Lebanese Shia in *Côte d'Ivoire*, other African and Latin American states. At the time of finance decrease, the organization will most likely drop many of its social-economic activities and prioritize its expenditures on defense budget issues. Hezbollah also gets financial support from non-governmental Iranian organization, and from Iranian Revolutionary Guard (IRGC) , mainly from al-Qudos Brigade liaisons officers inside the group.

**Alliances**

Clausewitz said that alliances could serve as a CoG, in this case, its alliance with Syria and Iran.

## 3. Results

From the abovementioned discussion, it is clear that semi-state actors rely on public support for the mobilization it needs.

Hezbollah maturity decreases the effects of leadership targeting of its leaders, if the organization was deprived of its leadership, it would sustain a heavy loss, however, that is not going to affect it on the long term. The armed force of Hezbollah is more dependent on the economic requirements, at the end the Iranian role is essential in the survival of Hezbollah , not only for financial support , but also for the training services and the ideological coverage it provides to the cadres of the party.

## 4. Conclusions

This research provides an insightful study to the strategic CoG of Hezbollah , it claims that the strategic CoG is its alliance with Iran, as nothing can be more influential on Hezbollah than that relationship mainly because of its ideological nexus. Iran is the main actor who is responsible of the sustainment of Hezbollah , the limitations of the research is that case of Hezbollah cannot be generalized to other semi-state organizations like Hamas.

**References**

[1] United Nations Security Council Resolution 1559 (2004): Calls upon all remaining foreign forces to withdraw from Lebanon; Calls for the disbanding and disarmament of all Lebanese and non-Lebanese militias; Supports the extension of the control of the Government of Lebanon over all Lebanese territory

[2] Knud Bartels, (1994), "The Center of Gravity," in An Anthology of Doctrinal Papers (Carlisle Barracks, PA: Department of Military Strategy, Planning, and Operations, US Army War College)13-

[3] Carl von Clausewitz, On War, edited and translated by Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), pp. 75, 77

[4] Schnaubelt, et al.; Vulnerability Assessment Pocket Guide; (2014); https://www.rand.org/content/dam/rand/pubs/tools/TL100/TL129/RAND_TL129.pdf

[5] Dale C. Eikmeier, "COG Analysis," Military Review, July-August 2004, (accessed February 17, 2006).

[6] Joseph Strange and Richard Iron, "Centers of Gravity & Critical Vulnerabilities," Quantico, Virginia: The Marine Corps Association: 1996, pp:1-12.

# CROSS-SITE SCRIPTING ATTACKS AND THE SECURITY OF WEB APPLICATIONS

Ass. Prof. Dr. Petar Halachev
Department of Informatics
University of Chemical Technology and Metallurgy – Sofia, Bulgaria
x3m@mail.orbitel.bg

***Abstract:*** *This report focuses on vulnerabilities on web-applications and web-sites from Cross-Site Scripting attacks (XSS). The different types of XSS attacks are examined: DOM-based, active and passive attacks. The spread of XSS attacks across platforms - government and financial institutions, transportation companies, hospitality and entertainment has been analyzed. Research and analysis of the security of corporate websites and their resistance to XSS attacks have been carried out. The basic guidelines for preventing valuable data theft and unauthorized access to websites and applications from XSS attacks are reviewed and systematized.*

**Keywords**: WEB-APPLICATION, WEB-SITE, CROSS-SITE SCRIPTING ATTACKS, VULNERABILITY, SECURITY

## *1. Introduction*

Cross-Site Scripting (XSS) is a widespread attack that affects many websites and web applications. XSS vulnerabilities have evolved significantly in the recent years [1]. The number of the DOM-based vulnerabilities, mXSS vulnerabilities [2] and expression-language based XSS attacks increases [3].

Characteristic of the XSS attack is the implementation of malicious code on a page of a website visited by the user who interacts with the server of the attacker. The attacks are realized by luring the user to the infected site through: social engineering; waiting for the user to visit the site himself and more. The results of the XSS attacks are: redirecting users to malicious sites; theft of cookies or credentials; data modification; replacing links or displaying your own ad on the site in question; destruction of the site. Developers often overlook the dangers of XSS attacks because they usually do not require specific user interaction, but only a visitation of the infected site.

The main purpose of the XSS attack is the theft of cookies by users in order to further obtain information and use it for subsequent attacks. The attacker does not attack the user directly but through the vulnerability of the website he is visiting by implementing JavaScript code. XSS executable code is usually written in popular programming languages like JavaScript, Vbscript, and more. The user sees this code in the browser as a part of the site. The visited resource is a conduit for the XSS attack.

If the attacker hits the administrator's cookies, they can access the control panel of the site or to its contents.

A number of popular sites - Facebook, Twitter, MySpace, eBay and Google can be targeted by such attacks.

Compared to SQL injections, the XSS attack is safe for the server but a threat to users of infected pages.

While SQL injection attacks database information from the back end, XSS attacks focus on stealing data from the front end of the website [4]. According to OWASP, the following syntax can be used to perform an XSS attack to steal cookie data, if validation of input data is not used:

```
<SCRIPT type=”text/javascript”>
Var adr = ‘../evil.php?cakemonster=’ + escape(document.cookie);
</SCRIPT>
```

According to P. Wurzinger et al. technically, XSS attacks leverage insufficient input/output validation in the attacked Web application to inject JavaScript code, which is then executed on the victim’s machine within the exploited Web site’s context, thus bypassing the same origin policy. The attacker can craft the injected script such, that it discloses the victim’s confidential information, e.g., a session ID. Then, by hijacking the session, the victim can be impersonated. Also, XSS enables the construction of very powerful phishing pages, since the page contentis actually deliveredby the correct, trusted site [5].

## *2. Distribution of XSS attacks*

Positive Technologies publishes on June 26, 2019, a study of the purpose and distribution of hacking attacks against web applications and sites in various sectors [6]. The main goals of the attacks are: spreading malware, stealing data, posting advertisements and forbidden information, fraud or intrusion. The analysis of statistics on hacking attacks in different sectors could assist security professionals in assessing the risks to which corporate websites are exposed (***Fig.1***).

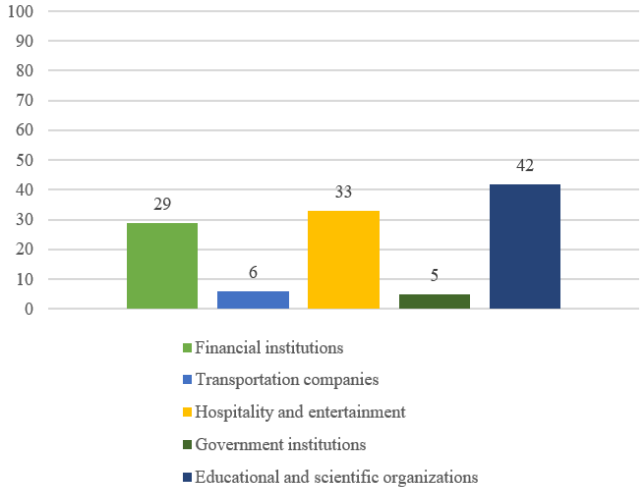



***Fig. 1****. Distribution of XSS attacks*

Financial institutions. The XSS attack is one of the most common web application attacks in 2018 - 29% of all attacks. Through e-banking, consumers can manage their finances: paying bills; savings; obtaining loans; transfers and more. In some cases, the bank's official website is also used to distribute malware or stage phishing attacks, and the bank's customers are amongst the first vulnerable.

Transportation companies. XSS attacks are around 6% of the total number of attacks. Sites of transport companies contain forms for registration with personal data of customers, support online payments for reservations and ticket purchase, etc. An example is the theft of customer data by British Airways in August and September 2018. Attackers modify the script on the company's website by adding their own code (called JS sniffer), leading to data theft, including card information of approximately 380,000 customers .

Hospitality and entertainment. About 33% of all attacks against these sites are XSS. Hotel websites contain reservation forms on which the customer enters their personal details and payment information. In this sense, all customer-oriented web applications and their user data should be treated as a valuable asset.

Government institutions. Cross-Site Scripting and SQL Injection are typical attacks on government sites - about 5% of all

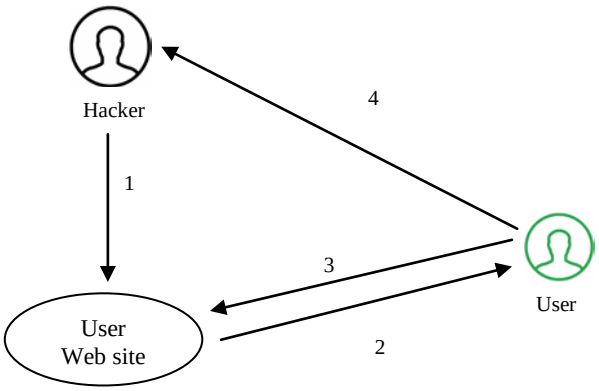
attacks are XSS. In 2018, remote code execution attacks were implemented to gain control of the server. According to Positive Technologies, there are also attacks designed to retrieve information about web applications, as well as many attempts to access .svn or .git directories that store the current source code of the application.

Educational and scientific organizations. About 42% of all attacks against these sites are XSS. Not only the personal data of the students and employees of the organizations, but also information about new studies and research is being attacked.

## *3. Implementation of XSS attacks*

Implementing the XSS attack and implementing malicious JavaScript code is only possible in the user's browser, so the site he visits should be vulnerable. To launch an attack, the attacker initially checks the XSS vulnerability resources through automated scripts or manual search. These are usually standard forms that can send and receive requests (comments, searches, feedback, etc.). Pages with input forms are collected and each one of them is scanned for vulnerability. For example, if there is a "search" on the site's page, to confirm the XSS vulnerability, the following query is sufficient:

*<script>alert("cookie: "+document.cookie)</script>*




1 – Inject with script
2 – Visit
3 – Inject script
4 - Malicious action

***Fig.2.*** *Cross-Site Scripting attack*

If a message appears on the screen, there is a risk of security breaks. Otherwise, the system displays a page with the search results. Popular CMS systems don't have such problems, but because of the ability to extend their functionality through modules and plugins created by external developers, the risk of XSS attacks is increasing (in systems such as Joomla, Drupal, Bitrix, WordPress, etc.). Most of the XSS vulnerabilities are tested in Internet Explorer.

Another possible option for finding vulnerabilities is to use pages that process GET requests. If we have a request of the type:

*http://example.com/search?page=8*

In the address bar, instead of the identifier (8), a script is added

*"><script>alert("cookie: "+document.cookie)</script>,*

Resulting in such an address:

*http://example.com/search?page= "><script>alert("cookie: "+document.cookie)</script>.*

If there is an XSS vulnerability on the webpage, a message will appear on the screen in the same way as in the first case. There are a huge number of tools, scripts and queries available to look for site vulnerabilities, and if none of them shows that the site is vulnerable, then the resource is protected from such attacks. In ***Fig. 2*** is a schematic of a cross-Site Scripting attack.

## *4. Classification of XSS Attacks*

The XSS attack can be classified into three major types (persistent XSS, non-persistent XSS, and DOM-based XSS [7], [8].

-DOM based XSS - when the injected data remains in the browser and modifies the DOM environment. In this model it is possible to use both reflected XSS and stored XSS. Q Zhang et a. notes that DOM-based XSS uses some DOM object operations of normal Ajax applications to attack user, entirely on client side. [9] DOM based XSS is implemented as follows:

1. The attacker creates in advance a URL that contains malicious code and sends it via email or otherwise to the user.
2. The user follows this link, the infected site accepts the request and executes the malicious code.
3. A code is executed on the user's page, and as a result a malicious script is loaded and the attacker receives cookies.

-Reflected (non-persistent) XSS – According to V. Malviya In reflected XSS attacks the injected code doesn't reside on the web server [10]. The malicious code executes as soon as it is injected and acts as a user request to the infected web site:

1. The attacker creates a URL link in advance that contains malicious code and sends it to the user.
2. The user sends the URL request to the site by following the link.
3. The site automatically takes data from malicious code and places it as a modified URL response to the user's request.
4. As a result, the malicious script contained in the response is executed in the user's browser, and the attacker receives all cookies of that user.

-Stored (persisted) XSS - data is stored by the application and retrieved later in another context, e.g. user profile. One of the most dangerous threats is that it allows the attacker to gain access to the server and to manage malicious code (delete or change the code). Persistent/Stored XSS attack – The attacker injects the code into an input field which lacks proper data validation and sanitization system and which returns back the injected code to the same page or to another page of the web server [11]. Each time somebody logs in the site, a pre-loaded code is executed that works in automatic mode. Such vulnerabilities most often affect forums, portals, blogs where HTML comments are available without restriction. Malicious scripts can be easily embedded in text, in photos, or in pictures.

-Multi-step XSS - when the user have to perform some action on the application (most often in the navigation panel). Within multi-step exploits a vulnerability can be escalated to amore severe vulnerability. Detecting second-order ulnerabilities is crucial to improve the security of web applications [12].

-mXSS attack [13] is characterized by the attacker injecting code that looks secure but is rewritten and modified in the browser while processing the HTML structure of the page [14]. An attack of the type mXSS is difficult to detect and sanitize by the logic of the web site. For example, when changing the order of closing quotes or adding quotes to non-quotation parameters (CSS font-family font).

While the first three categories of XSS threats are well identified by automated Penetration testing tools such as Web application vulnerability scanners [15], Multi-step XSS is challenging for developers [16]. On the one hand, manual testing for XSS attacks becomes more difficult as the number of websites increases and they become more complex. On the other hand, modern automated web application threat detection techniques can test a large percentage of technical threats, but they are limited to evaluate web applications because they lack "any knowledge about the functional behavior and business logic of the application" [17].

There are two basic types of XSS attacks, of the mechanism of the performance [18], [19], [20].

A passive XSS attack requires specific action from the subject of the attack. In order the "malicious code" to be executed, the user

must follow a link. Social engineering is used for this purpose, such as sending an email with an appeal to follow the link or click on a specific area of the site. When the user clicks on the desired object, the malicious script is started. If the user is inactive, the code will not be activated. This type of attack is more difficult to perform because not only technical but also psychological knowledge is required.

With active XSS attacks, the attacker does not need to lure the user through special links, since the code is embedded in the databases or in an executable file on the server. No user activity is required. Typically, an event manager is installed in the input forms, which will activate automatically when you reach this page. As a result, users who click on this link fall victim to the attacker. The attacker is trying to find a vulnerability in the site filter. Using a combination of tags and symbols, the attacker creates a request to the server and, once a "security hole" is detected, malicious code is attached to the request to steal a cookie. An example of such a script is:

*Img = new image()*
*Img.src = http://site.gif?+document.cookie*

## *5. Results and discussions*

### *Researching corporate websites for XSS attacks and guidelines for preventing them*

The objects of this study are corporate web sites. Social engineering methods could embed a link with malicious code to the site's hosting and leak personal data, change the site's appearance, introduce its own ad via Javascript, and replace real links with malicious ones.

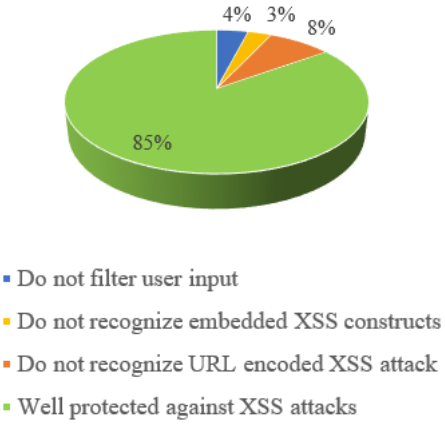



***Fig. 3.*** *Sites vulnerable to XSS attacks*

A small percentage of sites, approximately 4%, do not filter user input, 3% do not recognize embedded XSS constructs, and 8% do not recognize URL encoded XSS attack. Most of the sites, about 85%, are well protected against XSS attacks (***Fig. 3***).

To quickly scan the site for XSS vulnerability special services that scans the page automatically can be used. All URLs where user data is submitted (comment forms, feedback, search) must be verified. For example, http://xss-scanner.com could be used, as well as other similar tools. These services do not provide a full guarantee of safety, and manual verification is advisable, excluding all dangerous special characters and replacing them with safe <,>, `,' which contain all html requests and tags reserved by the language.

For example, the following code can be used to quickly filter and automatically change special characters <,>, `, ':

```
var lt = /</g,
    gt = />/g,
    ap = /'/g,
    ic = /"/g;
userData = userData.toString()
                   .replace(lt, "&lt;")
                   .replace(gt, "&gt;")
                   .replace(ap, "&#39;")
                   .replace(ic, "&#34;");
```

IBM recommend to protect an organization's network from XSS attacks, administrators can do the following [21]:

-Sanitize or validate input;

Theodoor Scholte et al. consider input validation as an additional layer of defense against XSS [22]. Further J. Snehi1 and Dr. R. Dhir considers that the best way to eliminate XSS vulnerabilities is to use defensive coding practices that validate and sanitize inputs to ensures that user inputs conform to a required input format. Replacement methods search for known bad characters and replace them with non-malicious characters and removal methods removes them. [23]

-Perform a thorough code review to identify possible vulnerabilities; Amiangshu Bosu et al. define steps to identify the vulnerable code thorough audit by thoroughly auditing the code [24];

-Disable HTTP trace, which can enable attackers to steal cookie data;

-Users can click on URLs directly when they have doubts about links in websites, emails or messages

One of the basic rules for protecting against XSS attacks is the useage of filters. In the study of corporate sites, almost all were protected, but there were sites that did not use any filtering of the data received (in PHP). Python frameworks (Flask, Django) have filters built in and they just need to be turned on.

The minimal filter protects against amateur attacks, but more serious site protection is required, with more detailed data filtering. The filter must be designed to recognize embedded structures. For example, in embedded construction, malicious JavaScript is placed at the lowest level. The filter blocks the upper level, but the lower one is executed.

When submitting data with incorrectly closed brackets, for example:

*>>>>><script{(alert("cookie: "+document.cookie))} ,*

the filter sees this and tries to close them, but the embed code executes. This query not only checks the filter for a different number of parentheses, but also determines how the filter responds to different characters, whether it blocks them or skips them. In the survey, some sites did not filter this type of attack.

Another vulnerability is related to the img tag. This tag has many parameters, including dynsrc, which may contain javacsript. This tag must be filtered. If photos will not be used on the site, it is better to exclude them.

Usage example:

*<img src="http://example.com/picture.jpg"*
*dynsrc=" javascript:alert(document.cookie)">*

When building a filter, it is necessary to consider the possibility of encoding attacks. There are a number of encryption programs that encrypt the attack so the filter cannot recognize it. In this case, it is necessary to use the filter decryption algorithm before the program executes the request code.

The example above can be encoded in URL notation as follows:

*%3Cimg%20src%3D%22http%3A%2F%2Fexample.com%2Fpicture.jpg%22%20%0Adynsrc%3D%22%20javascript%3Aalert%28document.cookie%29%22%3E%0A*

Encoding is needed not only to bypass the filter, but also for social engineering. The encoded code can be sent as a link. It is unlikely that anyone will check it. Thus, the attack is encrypted and the filter cannot recognize it. Therefore, it is necessary to use a filter decryption algorithm before the program executes the request code.
It is necessary the employees of the organization to be periodically instructed and informed about the rules for use of the Internet and the risk of XSS attacks, namely: not to open suspicious links; hosting and network administrators to check encrypted links and explore websites for vulnerability using JavaScript.

## *6. Conclusion*

This report examines the nature of the XSS attack, the different types of attacks, and the vulnerability of web applications and sites. A study has been conducted on the stability of corporate sites against XSS attacks. As a result of the security assessment, it was found that most of the surveyed corporate sites, about 85%, were protected by XSS attacks. A certain percentage of the sites surveyed are not well protected and could not withstand XSS attacks, as not all site owners want to invest resources and efforts in enhancing their security.

Following some basic rules could increase the security of web applications from XSS attacks.

The validation of the data entered by the user must be done both from the side of the web server and from the web browser.

Use secure connection via https certificates when user input is allowed on the website. According to A. Neagos turning off the HTTP TRACE can prevent the stealing stealing of cookies [25].

When using popular CMS - Wordpress, Bitrix, Joomla and others, a recent version of the kernel and all installed modules and plugins are required. The most common site management systems are protected by XSS attacks, but the addition of external (additional) plugins from untested sources may contain vulnerabilities.

## *7. References*

[1] Lekies S; Kotowicz, Krzysztof; Groß, Samuel; Nava, Eduardo Vela; Johns, Martin (2017). "Code-reuse attacks for the Web: Breaking Cross-Site Scripting Mitigations via Script Gadgets", CCS 17, October 30 - November 3, 2017, Dallas, TX, USA, pp. 1709-1723

[2] Heiderich M., Schwenk J., Frosch T., Magazinius J., Jang E. Z. mXSS attacks: tacking well-secured web-applications by using innerHTML mutations. In Proceeding of the 2013 ACM SIGSAC conference on Computer and communications security (2013) ACM, pp. 777-788

[3] Heiderich M., Mustache security wiki (online) https&//github.com/cure53/mustache-security.2014

[4] https://keirstenbrager.tech/sql-vs-xxs-injection-attacks-explained/

[5] Peter Wurzinger, Christian Platzer, Christian Ludl, Engin Kirda, Christopher Kruegelk, SWAP: Mitigating XSS attacks using a reverse proxy, Secure Systems Lab - Technical University Vienna, Institute Eurecom France, University of California, Santa Barbara, IWSESS '09 Proceedings of the 2009 ICSE Workshop on Software Engineering for Secure Systems

[6] https://www.ptsecurity.com/ww-en/analytics/web-application-attacks-2019/

[7] M. K Gupta, M. C. Govil, and G. Singh, "Static analysis approaches to detect SQL injection and cross site scripting vulnerabilities in web applications: a survey," in Proceedings of the Recent Advances and Innovations in Engineering (ICRAIE), 2014, pp. 1-5

[8] Vernotte A., Dadeau F., Lebeau F., Legeard B., Peureux F., Piat F. (2014) Efficient Detection of Multi-step Cross-Site Scripting Vulnerabilities. In: Prakash A., Shyamasundar R. (eds) Information Systems Security. ICISS 2014. Lecture Notes in Computer Science, vol. 8880. Springer, Cham DOI https://doi.org/10.1007/978-3-319-13841-1_20

[9] Qianjie Zhang, Hao Chen, Jianhua Sun, The 2nd International Conference on Software Engineering and Data Mining, 2010

[10] Vikas K. Malviya, Saket Saurav, Atul Gupta, 2013 20th Asia-Pacific Software Engineering Conference (APSEC)

[11]Cross-site scripting, Wikipedia, http://en.wikipedia.org/wiki/Cross-site_scripting

[12] Johannes Dahse, Thorsten Holz, Static Detection of Second-Order Vulnerabilities in Web Applications, USENIX Security Symposium, 2014

[13] Mario Heiderich, Jörg Schwenk, Tilman Frosch, Jonas Magazinius, Edward Z. Yang, mXSS Attacks: Attacking well-secured Web-Applications by using innerHTML Mutations, 20th ACM Conference on Computer and Communications Security (CCS), Berlin, Germany, November 2013

[14] Wang, Yi-Hsun, Ching-Hao Mao, Hahn-Ming Lee, Structural Learning of attack vectors for generating mutated XSS attacks, arxiv preprint arxiv: 1009.3711 (2010)

[15] Bau, J., Bursztein, E., Gupta, D., Mitchell, J.: State of the Art: Automated Black-Box Web Application Vulnerability Testing. In: Proc. of the 31st Int. Symp. on Security and Privacy (SP 2010), pp. 332–345. IEEE CS, Oakland (2010)

[16] Doupé, A., Cova, M., Vigna, G.: Why Johnny Can't Pentest: An Analysis of Black-Box Web Vulnerability Scanners. In: Kreibich, C., Jahnke, M. (eds.) DIMVA 2010. LNCS, vol. 6201, pp. 111–131. Springer, Heidelberg (2010)

[17] Vernotte A., Dadeau F., Lebeau F., Legeard B., Peureux F., Piat F. (2014) Efficient Detection of Multi-step Cross-Site Scripting Vulnerabilities. In: Prakash A., Shyamasundar R. (eds) Information Systems Security. ICISS 2014. Lecture Notes in Computer Science, vol 8880. Springer, Cham DOI https://doi.org/10.1007/978-3-319-13841-1_20, pp. 359

[18] https://testmatick.com/software-testing-glossary/cross-site-scripting/

[19] Smith M. A., Web application Security: XSS Attacks, Kansas State University, CIS 726, pp. 1-2, http://people.cs.ksu.edu/~mas3773/cis726/report.pdf

[20] Shailendra Rathore, Pradip Kumar Sharma, Jong Hyuk Park, XSSClassifier: An Efficient XSS Attack Detection Approach Based on Machine Learning Classifier on SNSs, Journal of Information Processing Systems, Vol.13, No.4, pp.1014-1028, August 2017, https://doi.org/10,3745/JIPS.03.0079

[21] IBM MSS, Cross-Site Scripting (XSS) Research and Intelligence report, Release data& December 15, 2014 by& Nikita Gupta, p.5

[22] Theodoor Scholte, William Robertson, Davide Balzarotti, Engin Kirda, SAC 2012 Proceedings of the 27th Annual ACM Symposium on Applied Computing, Pages 1419-1426

[23] Jyoti Snehi1, Dr. Renu Dhir, Jalandhar, India, International Journal of Computers & Technology Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

[24] Amiangshu Bosu, Jeffrey C. Carver, Munawar Hafiz, Patrick Hilley, Derek Janni, Identifying the characteristics of vulnerable code changes: an empirical study, FSE 2014 Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering Pages 257-268

[25] Adriana Neagos, Simona Motogna, Security Analysis Regarding Cross-Site Scripting on Internet Explorer, BCI, 2012, Citeseer

# CODE CONTRACTS VS INPUT VALIDATION

L.Petkova. PhD
University of Library and Information technology (UNIBIT)
lilyanapetkova92@gmail.com

***Abstract:*** *The unstoppable growth of security flaws makes the developers more patient in integrating different security defenses in the application development! Most of the security breaches are due to uninformed or unqualified developers! The good part is that Internet provides a large amount of rules/documentations/guidelines/tools free for use to help the developers in their work! But as the coin has two sides each web application needs to provide two parts of security flaws protection. The first level of defense is the well known protection from the outside world, called user input validation! And the second side is to ensure that the application works without a problem! Which means to protect it from inside out by integrating what is called code contracts! Even thought those two types of protection have similar purposes there is a difference which we are going to present in the research!*
***Keywords****: SECURITY, CODE CONTRACTS, CODE RULES, USER INPUT, VALIDATION*

## *1. Introduction*

Working with data should makes us paying attention to the way of managing it! Even though the development life cycle is limited in time and cost that does not mean that, we need to pass through the security of the application from each point of view. By starting from the very first phase of the SDLC until its last stage, we must develop an application, which should resist on the influence of the outside world. [1][2][3]

With this article, we want to introduce general information on two concepts of code validation, which can help in preventing some of the most serious security attacks: code contracts and input validation. Although, their characteristics are common, they have some significant differences, which we present in the current article.

The research is structured in three sections. In the first one, we are analyzing the input validation concept. We provide basic information on its purpose and damages it can cause and some of the most commonly used patterns to guarantee input data validation. The second part of the research contains information on code contracts. Firstly, we are presenting the code contracts idea by providing a classification based on the area of verification. Then we define some advantages of their use and some practices in order to achieve the best of them.

Finally, we are providing a comparison between those two concepts in data validation. As part of our research, so far we are achieving this by proving a code example for each of the provided validation concept.

## *2. Input Validation*

During the evolution of the application's development, we passed through static web site to web sites, which incorporate dynamic data. This data usually flows in two directions: it either comes from the server and is sent to the end user's browser, or the data is entered by the user and sent to the server to be processed or stored.[4][5][10]

Data coming from the server can be retrieved from many different untrusted data sources, including files and databases.

The other flow of data comes from the user and is sent to the server. The underlying principle of this data flow is basically the same in all scenarios — users enter data on a specific topic and then submit it to the server. [4][5][10]

Moreover, the best result in that case is a friendly message returned to the user that something is wrong with the data.

To prevent the application from receiving invalid data, it must be validated before further use! We have already mentioned some of those validation rules, which properly followed, will add the necessary layer of security to the application. [1][3]

Proper input validation can eliminate the vast majority of software vulnerabilities. Be suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user-controlled files. [1][3]

There are various services, managers, providers, stores which can help in validating the user input. In general, each application with a client interface and accessed from the outside world must have a proper implementation of validating the user input fields. [9][14][15][16]

The most frequently used validation pattern is the **exception throwing**. It consists of directly checking inputs and throwing exceptions. [14][15][16]

```
void FindUserById(int userId)
{
    if (userId <= 0)  throw new ArgumentException("UserId
must be a greater than 0");
//rest of the body
 }
```

***Example 1:*** *Exception throwing*

Other option is by applying some **regex patterns** to the user input to validate it against some rules. Even though it takes time coming up with a proper regex rule, it is worth the effort! And moreover there are various of rules in the Internet which are ready to be used! [14][16]

```
Regex.Replace(userInput, "[$&+,:;=?@#|'<>.^*()%!]", "")
```

***Example 2:*** *Regex Pattern for remove the special characters from a string*

## *3. Code Contracts*

The code contracts provide a method for expressing constraints and assumptions within the code, which can be validated at both compile time and runtime.

Code contracts have been profoundly used in .NET 4 framework. They have been abandoned as a validation mechanism for the past years. However, in the process of our research we found them really interesting and easy to use and understand. Which makes us want of further investigating them.

### *3.1. Classification*

The code contracts differ based on when they are verified:

***Preconditions.*** Verified when a function starts. [8]

Preconditions specify state when a method is invoked. They are generally used to specify valid parameter values. All members that are mentioned in preconditions must be at least as accessible as the method itself; otherwise, the precondition might not be understood by all callers of a method. The condition must have no side-effects. The run-time behavior of failed preconditions is determined by the runtime analyzer.

```
Contract.Requires<ArgumentNullException>(x != null, "x");
```

***Example 3:*** *Precondition contract[6]*

***Postconditions.*** Verified before a function exits.[8]

The postcondition is checked just before exiting a method. The run-time behavior of failed postconditions is determined by the runtime analyzer.

Postconditions express a condition that must be true upon normal termination of the method.

```
Contract.Ensures(this.F > 0);
```

***Example 4:*** *Postcondition contract[6]*

Unlike preconditions, postconditions may reference members with less visibility. A client may not be able to understand or make use of some of the information expressed by a postcondition using private state, but this does not affect the client's ability to use the method correctly.

***Object Variants.*** Verified after every public function in a class. [8]

Object invariants are conditions that should be true for each instance of a class whenever that object is visible to a client. They express the conditions under which the object is considered correct.

```
[ContractInvariantMethod]
protected void ObjectInvariant ()
{
   Contract.Invariant(this.y >= 0);
   Contract.Invariant(this.x > this.y);
   //rest of the body
}
```

***Example 5:*** *Object Variants[6]*

### *3.2. Advantages [11][7]*

- **Improved testing**: Code contracts provide static contract verification, runtime checking, and documentation generation.
- **Automatic testing tools**: You can use code contracts to generate more meaningful unit tests by filtering out meaningless test arguments that do not satisfy preconditions.
- **Static verification**: The static checker can decide whether there are any contract violations without running the program. It checks for implicit contracts, such as null dereferences and array bounds, and explicit contracts.
- **Reference documentation**: The documentation generator augments existing XML documentation files with contract information. There are also style sheets that can be used with Sandcastle so that the generated documentation pages have contract sections.

### *3.3. Best practices*

Depending on certain rules (preconditions) publicly offered by a service guarantees some results described in the postconditions. Which leads to the following necessary rules of each precondition in order to achieve the best results:

**Public**. The preconditions should be public so that they can be understandable before event start writing a line of code. [12]

The best way of achieving this is by specifying them at the top of the method's body:

```
public string GetPositionDetails(int position)
{
   Contracts.Require(position, x => x >= 0);
    // Rest of the body
}
```

***Example 6:*** *Publicity*

**Simplicity.** The preconditions should be easy to check which means that they should not be presented by writing complex algorithms to emulate them. [12]

In case of the need of complex contract, just provide separate methods for each precondition (*one of the best practices at all*).

```
public int Devote(int amount)
{
    Contracts.Require(() => CanDevote(amount));
     return DevoteCore(amount);
}
```

***Example 7:*** *Simplicity*

The precondition contracts should not rely on non-public methods or states because that will restrict client code in its ability to check them.

**Stability.** The preconditions should be stable. The precondition validation result should not depend on volatile classes or variables.

In the following example, the client depends on the existence of a file, which may be deleted or inaccessible but cannot be checked! That check cannot be defined as a precondition because it cannot be validated.

```
public string ReadFile(string filePath)
{
    Contracts.Require(() => File.Exists(filePath));
  // Rest of the method
}
```

***Example 8:*** *Stability*

In that case we deal with it by adding some exceptions as the one provided in the following code:

```
public string ReadFile(string filePath)
{
    if (!File.Exists(filePath)) throw new ArgumentException();
     // Rest of the body
}
```

***Example 9:*** *Stability*

## *4. Input validation vs Code Preconditions - results*

For the ordinary human being the contract preconditions can be described as a shield placed inside the code to secure the smooth workflow. On the other hand, the validation of the incoming data can be presented as a "defense" against the outside world. [12]

The red point from the Figure 1 represents invalid upcoming request from the outside and the green ones the valid ones.

The main goal of each developer is to take care of that red point to not reach the code!

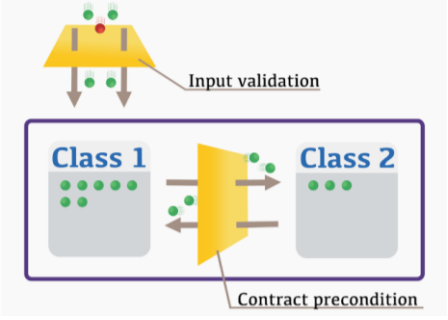



***Figure 1:*** *Input validation vs Contract precondition [12]*

In case the red signal appears inside the application, then it is either not validated input or bug generated in the code. Which from each point of view is must be fixed immediately.

In that case, the code contracts helps in stopping the red signals from spreading across the application shown on Figure 2.

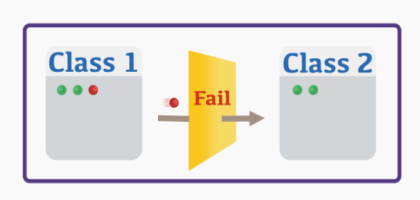



***Figure 2:*** *Precondition violation [12]*

The input validation protects the application from invalid input data, but not on the data coming in the application. Which makes it a valid situation with invalid data. [12]

On the contrary, the contract preconditions validate the data from inside the application, which makes it a bug in the system in case of data violation. [12]

For better understanding the difference between the input validation and the code contract, we are going to review an example of a method returning the difference between two integers.

The rules are as follow: [13]

- The minimal value should be greater or equal to 0
- The maximum value should be greater or equal to 0
- The minValue should be smaller than the maxValue
- The result should be smaller than the maximum value

With the following code from Example 10, we are providing the code concept of input validation:

```
public int GetNumbersDifference(int minValue, int maxValue)
 {
    if (minValue >= 0)
    {
       throw new ArgumentException("minValue");
    }
    if (maxValue >= 0)
    {
      throw new ArgumentException("minValue");
    }
   if (!(minValue < maxValue))
    {
      throw new ArgumentException("minValue, maxValue");
    }
  var result = maxValue - minValue;
   if (!(result <= maxValue))
  {
     throw new Exception("Something went wrong");
  }
 return result;
}
```

***Example 10:*** *Input Validation Example[13]*

With code contracts, the code from Example 10 would be converted to something like the code from Example 11:

```
public int GetNumbersDifference(int minValue, int maxValue)
 {
Contract.Requires<ArgumentException>(minValue >= 0);
Contract.Requires<ArgumentException>(maxValue >= 0);
Contract.Requires<ArgumentException>(minValue<maxValue);
Contract.Ensures(Contract.Result<int>() <= maxValue);
return maxValue - minValue;
 }
```

***Example 11:*** *Code Contract Example[13]*

At first sight, the second code provide much more readable and easy for the ordinary human to understand concept!

## *5. Conclusion*

The need of code validation is the most significant step in the developer's work. The two concepts presented in this research although common has their own characteristics. Moreover, although we have given the option to choose which one to use, one of those possibilities is now abandoned which is not recommended to use in production code bases! That of course does not allow the developer to abandon the protection of the application. As the code validation is the most protective step in the security integration of the application! Moreover, its need will always be in favor.

## References

[1] Petkova, L., SECURITY STANDARDS in software development, 2017
[2] Petkova, L., HTTP SECURITY HEADERS, 2018
[3] Petkova, L., CONTENT SECURITY POLICY VALIDATION, 2019
[4] Petkova, L., SEO SPAM AND MALWARE, 2019
[5] Petkova, L., SECURITY'S LEAKS IN SEO SPAMMING, 2019
[6] Mackey, Alex, Introducing .NET 4.0: With Visual Studio 2010
[7] Kolev, Rosen, Validation Rule Patterns in C#, FEBRUARY 2018
[8] Roque Alex, Web Application Programming, Lectures, 2016
[9] Code Contracts, Microsoft, May 2018
[10] Code Contracts User Manual, Microsoft Manual, January, 2012
[11] Albahari, Joseph, Code Contracts, 2007-2017
[12] Khorikov, Vladimir, C# code contracts vs input validation, February 2015
[13] Hakan Onur, Code Contracts – A brilliant way to do validation in your code and even do more, November 2010
[14] ICT Security Trends, Willian Dimitrov, Sofia, 2017, Avangard, ISBN 978-619-160-766-2
[15] Software testing, Willian Dimitrov, Sofia, 2017, Avangard, ISBN 978-619-160-765-5
[16] ICT Security Model, Willian Dimitrov, Sofia, 2018, Avangard, ISBN 978-619-160-950-5

# ON THE POWER TO DETECT ERRORS OF ONE ERROR-DETECTING CODE

Prof. Ilievska N. PhD.
Faculty of Computer Science and Engineering, "Ss. Cyril and Methodius" University, Skopje, Macedonia
natasa.ilievska@finki.ukim.mk

***Abstract:*** *When messages are transmitted through the communication channel, due to the noises in the channel, they can be incorrectly transmitted. Therefore, the receiver must ensure that it has the correct message. Similarly, the data stored in the storage media due to different circumstances can be corrupted. In order to check whether the data is corrupted or to check whether the receiver received the correct message, so-called error-detecting codes are used. When using such a code, it is important to know the power of the code to detect errors. In this paper we will analyze the ability to detect errors of one such error-detecting code. We compare the error-detecting capabilities of the code in a case when a quasigroup of order 4, order 8 and order 16 is used for coding for three different lengths of the redundancy. At the end we made a conclusion about the best choice of parameters from the aspect of the ability of the code to surely detect errors.*

**Keywords**: ERROR-DETECTING CODE, QUASIGROUP, CODED BLOCK, SYMBOL, ALPHABET

## *1. Introduction*

Nowadays, when we live in the age of fast communication networks through which huge amounts of data are transmitted on a daily basis, but also huge amount of data is stored on the storage media, it is important to ensure security and reliability (accuracy) of transmitted or stored data. In order to achieve this goal, the standard approach is the data to be first encrypted, then the encrypted data is coded and transmitted through the channel. The received data is first decoded and then decrypted. But also, there are some solutions in which it is made effort the encryption and coding procedures to be combined into one algorithm, so-called crypt-coding algorithm.

This paper is focused on the coding part of the communication system. The role of the codes is to ensure a reliability and accuracy of the data. This means that they are used in order to ensure that data is not corrupted during transmission through the channel (or while it is stored on some storage medium, when used in such medium).

In [1] we defined an error-detecting code. This code is defined using quasigroups. The performances of the defined code depend on the quasigroup used for coding. An important parameter that defines performances of the code from the aspect of the ability of the code to detect errors is the number of errors that the code surely detects. This number is the maximum number of incorrectly transmitted bits up to which the code will detect the error for sure. In this paper we compare the number of errors that the code surely detects when a linear quasigroup of order 4, order 8 and order 16 is used for coding.

The paper is organized in a following way: In Section 2 are given the basic mathematical definitions and the definition of the code. In Section 3 we compare the ability of the code to detect errors for sure when a quasigroup of order 4, order 8 and order 16 is used for coding. We consider the cases when the length of the redundancy is 8, 12 and 16 bits when the quasigroups of order 4 and order 16 are used for coding and redundancy of 9, 12 and 15 bits when the quasigroup of order 8 is used for coding. At the and we conclude the paper.

## *2. Code for error-detection*

Quasigroup is an algebraic structure that is used in coding theory and cryptography. The code that we consider in the paper is also defined using this algebraic structure. For that reason, first we will slightly explain this term.

Let $Q$ be a set and * is a binary operation. If $Q$ is closed under the operation *, i.e., if for all x, y∈Q, the quasigroup product $x*y∈Q$, then the structure $(Q, *)$ is called a groupoid. A groupoid $(Q, *)$ in which for all $u, v∈Q$, the equations $x*u=v$ and $u*y=v$ have unique solution by $x$ and $y$ is called quasigroup. Order of a finite quasigroup is the number of elements in the quasigroup. In this paper, if the order of the quasigroup is $n$, then we will take that the elements of the quasigroups are the integers from 0 to $n$-1, i.e., $Q=\{0, 1, 2, \ldots, n-1\}$.

In the code considered in this paper we use a so-called linear quasigroups. A quasigroup $(Q, *)$ of order $2^q$ is linear if there are non-singular binary matrices $A$ and $B$ of order $q\times q$ and a binary matrix $C$ of order $1\times q$, such that

$$(\forall\, x, y\in Q)\ \boldsymbol{x*y}=\boldsymbol{x}A+\boldsymbol{y}B+C \tag{1}$$

where $\boldsymbol{x}$ and $\boldsymbol{y}$ are the binary representations of $\boldsymbol{x}$ and $\boldsymbol{y}$ as $1\times q$ vector, $\boldsymbol{x*y}$ is the binary representations of the quasigroup product $x*y$ as $1\times q$ vector and + is a binary addition.

The code that we consider in this paper is defined in a following way. Let for coding be used a linear quasigroup $Q$ and let the input block be $a_0a_1\ldots a_{n-1}$ ($a_i\in Q$, for all $i\in\{0, 1, \ldots, n-1\}$). Then, the redundant symbols are defined in a following way:

$$\boldsymbol{d_i} = \boldsymbol{a_i}A^{n-2} + \sum_{j=1}^{n-2} \boldsymbol{a_{i+j}}BA^{n-j-2} + C\sum_{j=0}^{n-3} A^j,\ \ i=0, 1, \ldots, r \tag{2}$$

where $r\in N$ is the parameter of the code such that $1\le r\le n-1$, $\boldsymbol{a_i}$ is the binary representations of the information symbol $a_i$, $A$, $B$ and $C$ are the binary matrices that satisfy the equation (1) and + is a binary addition. With equation (2), the redundant symbols are obtained in a binary form.

Now, the redundant symbols are concatenated on the input block $\boldsymbol{a_0a_1\ldots a_{n-1}}$, which gives the coded block $\boldsymbol{a_0a_1\ldots a_{n-1}d_0d_1\ldots d_r}$. The coded block is in a binary form and is transmitted through a binary symmetric channel. Since there are noises in the channel, some symbols may be incorrectly transmitted. This may lead to situation in which the recipient receives inaccurate data.

When the receiver receives the output block, in order to check the accuracy of the data, it calculates the redundant symbols that correspond to the received information block. If the calculated symbols match with the received ones, then the receiver accepts the output block. If there is a mismatch in at least one symbol, the receiver does not accept the received output block and asks for repeated transmission of that block.

But, as with any error-detecting code there is a possibility that the code will not detect the errors in transmission, i.e., it is possible to have complete match of the received and calculated redundant symbols, although the block is not correctly transmitted. We started the investigation of the error-detecting properties of the code in [1] and [2] by obtaining the probability of undetected errors, and then we continue the research in a direction of the number of errors that the code surely detects ([3], [4], [5]).

## *3. Comparison and analysis of the power of the code to surely detect errors*

The number of errors that the code surely detects depends on the length of the input block, but also on the parameter $r$ of the

model and the quasigroup used for coding. In this section we will compare the results for the number of errors that the code detects for sure when a linear quasigroup of order 4, order 8 and order 16 is used for coding. We consider the cases when the length of the redundancy is 8, 12 and 16 bits (i.e., 9, 12 and 15 bits when the quasigroup of order 8 is used for coding).

First, for coding was used the following linear quasigroup of order 4:

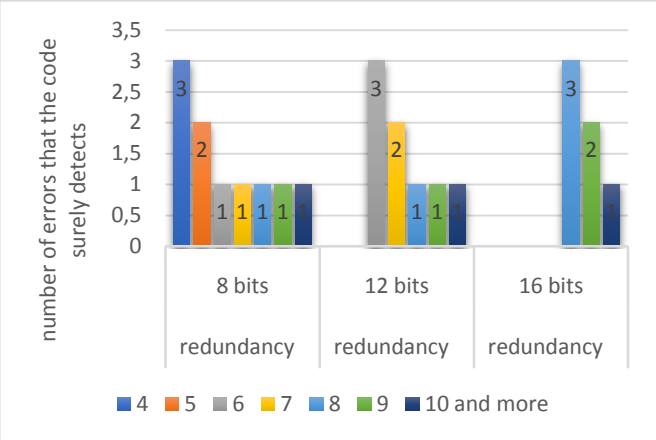
| * | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 3 | 2 |
| 1 | 3 | 2 | 0 | 1 |
| 2 | 2 | 3 | 1 | 0 |
| 3 | 1 | 0 | 2 | 3 |

Since this is liner quasigroup, there are binary matrices such that (1) is satisfied. This binary matrices $A$, $B$ and $C$ are the following:

$$A = \begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix}, B = \begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix}, C = [0 \quad 0]$$

The number of errors that the code surely detects when the linear quasigroup of order 4 is used for coding is given in Fig. 1 ([3]).

***Figure 1**: Number of errors that the code surely detects when the linear quasigroup of order 4 is used for coding.*




The length of the input block is expressed as number of characters from the quasigroup used for coding and is denoted with the color of the pillar. The blue pillar represents the input blocks with length 4 characters from the quasigroup, the orange is for the input blocks with length 5 characters from the quasigroup, the gray pillar is for input blocks with length 6 characters, the yellow for input blocks with length 7 characters, light blue is for the blocks of length 8 characters, the green one for blocks of length 9 characters, while the results for the input blocks of length greater than or equal to 10 characters are represented with the dark blue pillar. In the first section of Fig.1 are given the results when the redundancy is 8 bits, in the second section are the results when the redundancy is 12 bits and in the third section are the results when the redundancy is 16 bits.

The quasigroup of order 8 used for coding is:

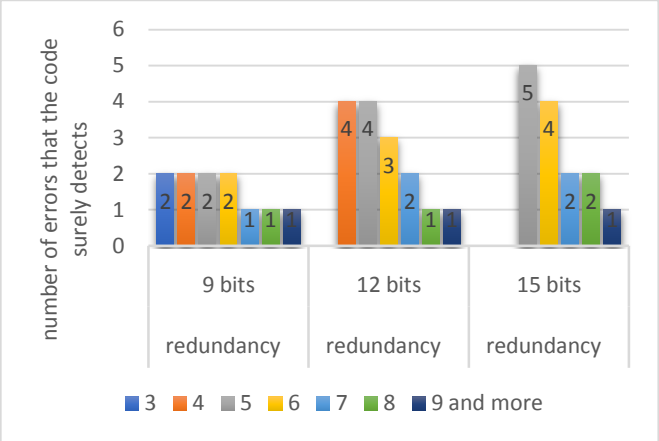
| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 5 | 7 | 2 | 3 | 6 | 4 | 1 |
| 1 | 7 | 2 | 0 | 5 | 4 | 1 | 3 | 6 |
| 2 | 3 | 6 | 4 | 1 | 0 | 5 | 7 | 2 |
| 3 | 4 | 1 | 3 | 6 | 7 | 2 | 0 | 5 |
| 4 | 5 | 0 | 2 | 7 | 6 | 3 | 1 | 4 |
| 5 | 2 | 7 | 5 | 0 | 1 | 4 | 6 | 3 |
| 6 | 6 | 3 | 1 | 4 | 5 | 0 | 2 | 7 |
| 7 | 1 | 4 | 6 | 3 | 2 | 7 | 5 | 0 |

This linear quasigroup is represented by the following binary matrices:

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, C = [0 \quad 0 \quad 0]$$

The number of errors that the code surely detects when this quasigroup is used for coding is given in Fig. 2 ([4]).

***Figure 2**: Number of errors that the code surely detects when the linear quasigroup of order 8 is used for coding.*




The linear quasigroup of order 16 used for coding is:

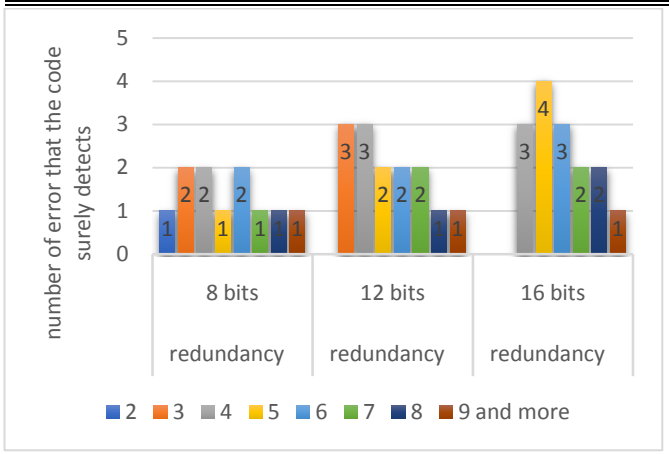
| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 7 | F | 8 | D | A | 2 | 5 | B | C | 4 | 3 | 6 | 1 | 9 | E |
| 1 | F | 8 | 0 | 7 | 2 | 5 | D | A | 4 | 3 | B | C | 9 | E | 6 | 1 |
| 2 | D | A | 2 | 5 | 0 | 7 | F | 8 | 6 | 1 | 9 | E | B | C | 4 | 3 |
| 3 | 2 | 5 | D | A | F | 8 | 0 | 7 | 9 | E | 6 | 1 | 4 | 3 | B | C |
| 4 | B | C | 4 | 3 | 6 | 1 | 9 | E | 0 | 7 | F | 8 | D | A | 2 | 5 |
| 5 | 4 | 3 | B | C | 9 | E | 6 | 1 | F | 8 | 0 | 7 | 2 | 5 | D | A |
| 6 | 6 | 1 | 9 | E | B | C | 4 | 3 | D | A | 2 | 5 | 0 | 7 | F | 8 |
| 7 | 9 | E | 6 | 1 | 4 | 3 | B | C | 2 | 5 | D | A | F | 8 | 0 | 7 |
| 8 | 7 | 0 | 8 | F | A | D | 5 | 2 | C | B | 3 | 4 | 1 | 6 | E | 9 |
| 9 | 8 | F | 7 | 0 | 5 | 2 | A | D | 3 | 4 | C | B | E | 9 | 1 | 6 |
| A | A | D | 5 | 2 | 7 | 0 | 8 | F | 1 | 6 | E | 9 | C | B | 3 | 4 |
| B | 5 | 2 | A | D | 8 | F | 7 | 0 | E | 9 | 1 | 6 | 3 | 4 | C | B |
| C | C | B | 3 | 4 | 1 | 6 | E | 9 | 7 | 0 | 8 | F | A | D | 5 | 2 |
| D | 3 | 4 | C | B | E | 9 | 1 | 6 | 8 | F | 7 | 0 | 5 | 2 | A | D |
| E | 1 | 6 | E | 9 | C | B | 3 | 4 | A | D | 5 | 2 | 7 | 0 | 8 | F |
| F | E | 9 | 1 | 6 | 3 | 4 | C | B | 5 | 2 | A | D | 8 | F | 7 | 0 |

The corresponding matrices are:

$$A = \begin{matrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{matrix}, B = \begin{matrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{matrix}, C = [0 \quad 0 \quad 0 \quad 0]$$

The number of errors that the code surely detects when the quasigroup of order 16 is used for coding is given in Fig. 3 ([5]).

***Figure 3**: Number of errors that the code surely detects when the linear quasigroup of order 16 is used for coding.*




In order to compare the results for quasigroups of different order and to see how the order of the quasigroups affect the number of errors that the code surely detects, we will express the length of the input blocks in bits. Each element from a quasigroup of order $2^q$ is represented with $q$ bits in the binary representation. This means that the element from a quasigroup of order 4 is represented by 2 bits, of order 8 by 3 bits, while the element from a quasigroup of order 16 by 3 bits in a binary form. Using this fact and the results represented in Fig. 1, Fig. 2 and Fig. 3, we obtain Table 1, Table 2 and Table 3.

In the first columns of Table 1 – Table 3 is given the length $n$ of the input block, now expressed as number of bits. In the second, third and fourth column is given the number of errors that the code surely detects when the linear quasigroup of order 4, order 8 and order 16 is used for coding, respectively. Since each element from a quasigroup of order 4 is represented by 2 bits, the length of input blocks in binary form when this quasigroup is used for coding is a multiple of 2. Therefore, there are values for the quasigroup of order 4 only on the positions that are multiple of 2. Similarly, since each element from a quasigroup of order 8 is represented by 3 bits in the binary form, in the case when the quasigroup of order 8 is used for coding the length of input blocks is a multiple of 3. Analogous, when a quasigroup of order 16 is used for coding, the length of the input block is multiple of 4. In order to compare the error-detecting capabilities of the code when quasigroups of different orders are used for coding, we should compare the number of errors that the code surely detects when code rates are equal. Therefore, we will compare this number when the lengths of the input blocks expressed in bits are equal and the redundancies also have equal length. In Table 1 are given the results when the redundancy is 8 bits (i.e., 9 bits when the quasigroup of order 8 is used for coding), in Table 2 are the results obtained when the redundancy is 12 bits and in Table 3 are represented the results for the number of errors that the code surely detects when the redundancy is 16 bits (i.e., 15 bits when the quasigroup of order 8 is used for coding).

***Table 1**: Number of errors that the code surely detects when the redundancy is 8 bits (i.e., 9 bits for quasigroup od order 8).*

| ***n*** | **quasi. order 4** | **quasi. order 8** | **quasi. order 16** |
|---|---|---|---|
| 8 | 3 | | 1 |
| 9 | | 2 | |
| 10 | 2 | | |
| 11 | | | |
| 12 | 1 | 2 | 2 |
| 13 | | | |
| 14 | 1 | | |
| 15 | | 2 | |
| 16 | 1 | | 2 |
| 17 | | | |
| 18 | 1 | 2 | |
| 19 | | | |
| 20 | 1 | | 1 |
| 21 | | 1 | |
| 22 | 1 | | |
| 23 | | | |
| 24 | 1 | 1 | 2 |
| 25 | | | |
| 26 | 1 | | |
| 27 | | 1 | |
| ≥28 | 1 | | 1 |

***Table 2**: Number of errors that the code surely detects when the redundancy is 12 bits.*

| ***n*** | **quasi. order 4** | **quasi. order 8** | **quasi. order 16** |
|---|---|---|---|
| 12 | 3 | 4 | 3 |
| 13 | | | |
| 14 | 2 | | |
| 15 | | 4 | |
| 16 | 1 | | 3 |
| 17 | | | |
| 18 | 1 | 3 | |
| 19 | | | |
| 20 | 1 | | 2 |
| 21 | | 2 | |
| 22 | 1 | | |
| 23 | | | |
| 24 | 1 | 1 | 2 |
| 25 | | | |
| 26 | 1 | | |
| 27 | | 1 | |
| 28 | 1 | | 2 |
| 29 | | | |
| 30 | 1 | 1 | |
| 31 | | | |
| ≥32 | 1 | | 1 |

***Table 3**: Number of errors that the code surely detects when the redundancy is 16 bits (i.e., 15 bits for quasigroup od order 8).*

| ***n*** | **quasi. order 4** | **quasi. order 8** | **quasi. order 16** |
|---|---|---|---|
| 15 | | 5 | |
| 16 | 3 | | 3 |
| 17 | | | |
| 18 | 2 | 4 | |
| 19 | | | |
| 20 | 1 | | 4 |
| 21 | | 2 | |
| 22 | 1 | | |
| 23 | | | |
| 24 | 1 | 2 | 3 |
| 25 | | | |
| 26 | 1 | | |
| 27 | | 1 | |
| 28 | 1 | | 2 |
| 29 | | | |
| 30 | 1 | 1 | |
| 31 | | | |
| 32 | 1 | | 2 |
| 33 | | 1 | |
| 34 | 1 | | |
| 35 | | | |
| ≥36 | 1 | 1 | 1 |

From Table1 – Table 3 we can see that for longer input blocks, the number of errors that the code surely detects is equal, regardless of the order of the quasigroup used for coding, but also regardless of the length of the redundancy. Namely, when the redundancy is 8 bits (i.e., 9 bits for the quasigroup of order 8) and the length of the input block is greater than or equal to 28 bits, the code surely detects 1 incorrectly transmitted bit regardless which of the three quasigroups is used for coding (Table 1). When the redundancy is 12 bits and the length of the input blocks is greater than or equal to 32 bit the code also detects 1 incorrectly transmitted bit for all three quasigroups (Table 2). The same conclusion holds when the redundancy is 16 bits (i.e., 15 bits for the quasigroup of order 8) and the length of the input blocks is greater than or equal to 36 bits (Table 3). But, for shorter input blocks, there is a difference in the error-detecting capability of the code, depending on which quasigroup is used for coding.

From Table1 – Table 3 we can see that whenever the input blocks have equal lengths, except when the length of the input

blocks is 8 bits and the redundancy is 8 bits, the number of errors that the code surely detects when the quasigroup of order 16 is used for coding is greater than or equal to the number of errors that the code surely detects when the quasigroup of order 4 is used for coding. But, in the case when the redundancy is 8 bits, when the input block has length 10 bits for quasigroup of order 4 the code rate is better (larger) than when the input block has length 8 bits for quasigroup of order 16, and also the number of surely detected errors is larger.

When comparing the quasigroups of order 4 and order 8, we see that the quasigroup of order 8 provides greater than or equal number of errors that the code surely detects than the quasigroup of order 4 always when the lengths of the input blocks are equal and lengths of the redundancies are equal. The quasigroup of order 4 is in advantage when the redundancy is 8 bits and the length of the input block is 8 bits, while the length of the input block is 9 bits for quasigroup of order 8 (equal code rates, but larger number of surely detected errors), but also when the length of the input block is 10 bits for quasigroup of order 4 and 9 bit for order 8 (better code rate for the quasigroup of order 4 while equal number of surely detected errors).

From all above we can conclude that for short input blocks, the quasigroup of order 4 gives smallest number of errors that are surely detected from the three considered quasigroups when the code rates are equal for a given length of the redundancy (except in the few indicated cases). But on other hand, if we want to achieve largest number of surely detected errors when the redundancy is 8 bits, we should use exactly the quasigroup of order 4 for coding and to divide the input message into blocks of length 8 bits and to code each of them separately. But then the code rate is 1/2.

The situation is not so simple when comparing the quasigroups of order 8 and order 16. In the cases of equal lengths of the input blocks, the quasigroup of order 8 provide greater number of surely detected incorrectly transmitted bits than the quasigroup of order 16 only in the case when the redundancy and the length of the input block are 12 bits. In all other cases, the quasigroup of order 16 gives greater or equal number of surely detected errors. But, on the other hand there are cases when for a given length of the redundancy, the quasigroup of order 8 achieves better code rate and larger or equal number of surely detected errors than the quasigroup of order 16. For example, when the redundancy is 8 bits, in the cases when the quasigroup of order 8 is used and the length of the input block is 9, 12, 15 or 18 bits the code rate is greater than or equal as when the quasigroup of order 16 is used and the length of the input block is 8 bits, but also the quasigroup of order 8 gives larger number of surely detected errors. Other such cases when the quasigroup of order 8 is in advantage are: When the length of the redundancy is 12 bits, the input block is 15 or 18 bits for quasigroup of order 8 and 12 bits for quasigroup of order 16, the input block is 18 bits for the quasigroup of order 8 and 16 bits for quasigroup of order 16, the input block is 21 bits for the quasigroup of order 8 and 20 bits for quasigroup of order 16; also when redundancy is 16 (i.e., 15) bits and the length of the input block is 15 or 18 bits for the quasigroup of order 8 and 16 bits for quasigroup of order 16. In these cases, the quasigroup of order 8 provide better code rate, but also higher number of surely detected errors or equal number of surely detected errors for better code rate.

When the redundancy is 12 bits, the best result is achieved when the quasigroup of order 8 is used and the length of the input block is 15 bits. The same number of surely detected errors is obtained also when the length of the input block is 12 bits, but since in this case the rate of the code is smaller, it is better to divide the input messages in blocks of length 15 bits. When the redundancy is 16 bits, the largest number of surely detected errors will be obtained if the input messages are divided in blocks of length 15 bits and the quasigroup of order 8 is used for coding. This is also generally the best choice of redundancy length, input block length and quasigroup for coding from all considered cases from the aspect of the number of errors that the code surely detects. In this case is achieved the largest number of surely detected incorrectly transmitted bits, i.e., the number of errors that the code detects for sure in this case is 5 bits.

## *4. Conclusion*

In this paper we compared the ability to detect errors from the aspect of the number of errors that it surely detects of one error-detecting code based on linear quasigroups in the cases when a linear quasigroup of order 4, order 8 and order 16 is used for coding and the redundancy is 8, 12 and 16 bits (i.e., 9, 12 and 15 bits for quasigroups of order 8). For longer input blocks, for each of the considered cases for the length of the redundancy, the number of errors that the code surely detects is equal, regardless which of the three quasigroups is used for coding. When the length of the redundancy is 8 (i.e., 9 bits) this conclusion holds when the input blocks have length greater than or equal to 28 bits. When the redundancy is 12 bits this numbers are equal when the length of the input block is greater than or equal to 32 bits, while when the redundancy is 16 (i.e., 15 bits) the conclusion holds for input blocks with length greater than or equal to 36 bits.

For shorter input blocks, the quasigroup of order 4 has smaller number of surely detected incorrectly transmitted bits than the quasigroup of order 8 and order 16 when the code rates are equal for given length of the redundancy. The quasigroup of order 4 has better performances than the other two quasigroups in only few cases.

For short input blocks, there is no general conclusion which of the quasigroups of order 8 and order 16 has greater number of surely detected incorrectly transmitted bits. It depends on the length of the input blocks. For some lengths one quasigroup yields better results, for some the other.

From the aspect of the number of errors that the code surely detects it is best to divide the input messages into blocks of length 15 bits and to code each block individually using the quasigroup of order 8, such that 15 redundant bits are added on each input block (i.e., to choose $r$=4).

## *5. References*

[1] Ilievska N., Gligoroski D., "Simulation of some new models of error-detecting codes," Proceedings of the 22nd Telecommunications Forum Telfor, Belgrade, Serbia, 2014, pp. 395-398.

[2] Ilievska N., Gligoroski D., "Simulation of a Quasigroup Error-Detecting Linear Code," Proceedings of the 38th International ICT Convention MIPRO CTI – Telecommunications & Information, Opatija, Croatia, 2015, pp. 483 – 488.

[3] Ilievska N., "Towards the Fixed Length Redundancy Code," Proceedings of the 27th Telecommunications Forum Telfor, Belgrade, Serbia, 2019, pp. 241-244.

[4] Ilievska N., "Modeling the number of errors that the code surely detects," Proceedings of the III International Scientific Conference Mathmodel, Borovets, Bulgaria, 2019.

[5] Ilievska N., "Towards the number of errors that the code detects for sure," Journal of Engineering Science and Technology Review, accepted.

# SECURITY OF THE B-MSS – THE NEW CHALLENGE FOR THE SATELLITE SYSTEM DESIGNERS

Assos. Prof. M. Sc. Demirev V.B. Ph.D
Technical University-Sofia, Bulgaria,
e-mail:demirev_v@tu-sofia.bg

***Abstract:*** *The Broadband Mobile Satellite Services (B-MSS) are extremely important not only for government (army and police), but for many civil applications as car, aero, railway and ship communications. Probably they will be part of the future 5-G network development and their security work is very important too. The solving of the main B-MSS security problems needs entirely new approach. The aim of this paper is to analyze two new radio-communication principles, named Spatial Correlation Processing - Random Phase Spread Coding, from security point of view. They were proposed by the author a decade before as antenna transmit-receive beam forming methods with many applications in microwave frequency bands too.*

**Keywords:** SECURITY, MOBILE, SATELLITE, SPATIAL, CORRELATION, RANDOM, PHASE, SPREAD, CODING

## *1 Introduction*

The Broadband Mobile Satellite Services (B-MSS) are extremely important not only for government (army, police, emergency care, disaster operations), but for many civil applications as car, aero, railway, ship and recreation vehicles communications. Probably they will be part of the future 5-G network development and their security work is very important too.

One of the biggest technical problems of the Vehicle Mounted Earth Stations (VMES), a very important segment of the B-MSS, is the antenna system. The tracking of a satellite in angular coordinates independently of mobile motion is an essential function for directional antenna systems in Ku and Ka frequency bands [1]. The angular tracking function needs two capabilities – beam steering and tracking control. A review of the beam steering and tracking control methods, used in B-MSS, is given in this report. Their advantages and disadvantages from security point of view are discussed too.

Another security problem for the B-MSS is the need to counter Space Terrorism. The most vulnerable components of the space systems are the VMES and the communication links. These components are susceptible to attack from widely accessible weapons and technologies.

Spatial Correlation Processing - Random Phase Spread Coding (SCP-RPSC) technologies were proposed by the author as antenna beam forming methods with many applications in microwave frequency bands. The possible improvement of B-MSS security is discussed too.

## *2 Satellite angular tracking and antenna beam steering in VMES*

### *2.1 Antenna beam steering*

The satellite angular tracking function needs two capabilities – antenna beam steering and tracking control [1].

There are two types of beam steering methods in microwave frequency bands. The first is mechanical steering, which physically directs the antenna to the satellite. The second is electronic steering, which directs the antenna beam by electronic scanning. A typical example of electronic steering is achieved through a phased array antenna. The main features of the two types of methods from security point of view are listed below:

- Mechanical steering

Advantages: Technically easy to fabricate; Wide beam coverage; Good axial ratios in wide beam coverage.

Disadvantages: Low reliability; Low speed beam scanning; Large in volume and heavy; Very high cost for civil B-MSS (in order of several thousand US $).

- Electronic steering

Advantages: Light and low profile; High-speed beam scanning; High reliability.

Disadvantages: Technically difficult to fabricate, especially in the future B-MSS millimeter wave bands; Narrow beam coverage, Narrow frequency working band, very important for the broadband systems; Poor axial ratios in wide scanned coverage, canceling the frequency reuse by orthogonal polarizations; Excessive feeder loss, reducing the receiver Figure of Merit G/T; Extremely high cost (in order of hundred thousand US $).

### *2.2 Satellite angular tracking*

There are also two methods to control tracking. The first is the closed loop method, which uses a signal from the satellite to search for and maintain in satellite direction. The second method is the open loop method, which does not use signals from a satellite. It uses compasses and rate sensors and is not applicable for B-MSS in Ku and Ka frequency bands, where high gain narrow beam antenna systems are used.

The tasks, performed by the VMES satellite tracking system, include satellite acquisition and automatic tracking [1]. The acquisition system acquires the desired satellite by moving the antenna around the expected position of the satellite. Automatic tracking is initiated only after the received signal strength due to the beacon signal transmitted by the satellite is above a certain threshold value, which allows the tracking receiver to lock to the beacon. The automatic tracking ensures continuous tracking of the satellite. Figure 1 shows the generalized block schematic arrangement of the closed loop satellite tracking system. The VMES antenna makes use of the beacon signal to track itself to the desired positions in both azimuth and elevation. The auto track receiver derives the tracking correction data that is used to drive the antenna. The tracking techniques are classified on the basis of the methodology used to generate angular errors. Commonly used tracking techniques include:

- Sequential Lobing

In sequential lobing, the beam axis is slightly shifted off the antenna axis. This squinted beam is sequentially placed in discrete angular positions, usually four, around the antenna axis. The angular information about the satellite to be tracked is determined by processing the received signals. The track error information is contained in the signal amplitude variations. The squinting and beam switching is done with the help of electronically controlled feed and therefore can be done very rapidly.

- Conical Scan

This is similar to sequential lobing except that in the case of conical scan, the squinted beam is scanned rapidly and continuously in a circular path around the antenna axis. If the satellite to be tracked is off the antenna axis, the amplitude of the echo signal varies with antenna's scan position. The tracking system senses the amplitude variations and the phase delay as function of scan position to determine the angular coordinates. The amplitude variation provides information on the amplitude of the angular error and the phase delay indicates direction. The angular error information is then used to steer the antenna axis to make it to coincide with the object location. The technique offers good tracking accuracy and an average response time.

- Monopulse Tracking

Monopulse tracking creates the required information for the angular error by simultaneous lobing of the received beacon. Monopulse tracking technique offers very high tracking accuracy and fast response time. Due to absence of any mechanical parts, the feed system requires very little maintenance. The disadvantages include high cost, large and complex feed system and need to have at least two-channel coherent receivers and good RF phase stability. It is commonly employed in large fixed earth stations, as well as in those earth stations that require accurate tracking of nongeostationary satellites.

The main disadvantages of the above listed closed loop tracking methods from security point of view are:

- The use of satellite signals as essential factor. This is because received signal levels from satellites are not stable because of the severe propagation environment due to fading, blocking, shadowing and active jamming;
- Long acquisition time period during the starting procedures, which is in order of minutes in real B-MSS systems. The same acquisition time is needed after the loose of the signal due to blocking in urban environment;
- The listed methods can be used for tracking only one communication satellite. In some cases, where very high security and reliability of B-MSS is necessary (Aeronautical B-MSS), the space diversity approach is used. It includes simultaneous communications and tracking of several satellites, obviously not achieved by the known tracking methods and systems;
- Ability to maintain pointing accuracy: Vehicles can abruptly accelerate and decelerate as well as travel in rough terrain. Under these conditions, the B-MSS VMES may find it difficult or impossible to maintain their pointing accuracy. Of greater practicality may be the ability of the antenna systems to automatically mute transmissions upon deviation from the target satellite;
- Danger of using ultra small antennas: Vehicles cannot accommodate the larger antennas that can be installed on ships. Thus ultra small stabilized antennas are more practical for VMES. However, smaller antennas have greater potential for interference to adjacent satellites because they have wider main and side lobes that can radiate more energy to satellites on either side of the intended satellite;
- Ability to track potential interference: Because of the ubiquity of vehicles and their unpredictable driving patterns, a method to identify and correct interference issues is paramount.

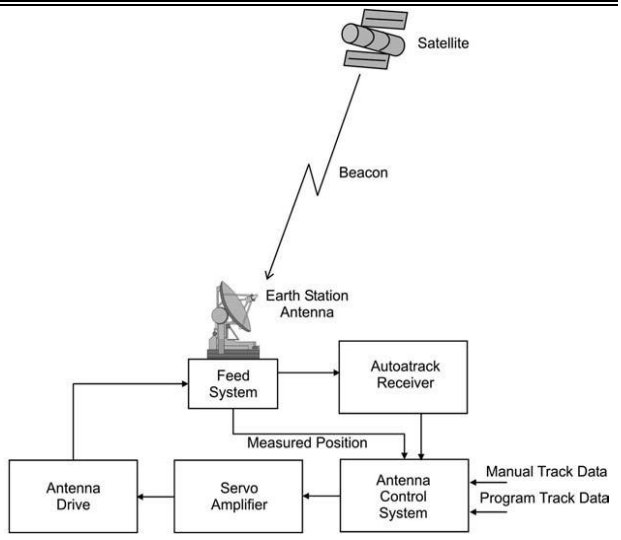



***Fig.1*** *Block schematic arrangement of closed loop satellite tracking system with mechanical steering*

## *3 SCP technology*

### *3.1 SCP approach system objectives*

The brief review of tracking antenna methods shows that the solving of tracking VMES problems needs entirely new approach. The name of the new technical proposal [1,3] is Spatial Correlation Processing (SCP).

The proposed SCP system objectives include:

- Receiving one or more radio signals coming from one or several spatially distributed sources (satellites), insuring high gain of the antenna systems of the fixed and mobile receiving terminals;
- Insuring spatial selectivity high enough to cancel the same frequency channel interference, coming from different space directions, using simple one-channel receiver and signal processing circuits.

The above mentioned SCP system objectives solve simultaneous the problems of virtually electronic antenna steering and multiple satellites closed-loop tracking system, providing the security requirements for the future government and civil B-MSS.

The objectives stated above are achieved by a method for radio communications, which proposes application of additional pilot signals transmitted in the band of information signals and available in the receiver by one of the known methods of access. The SCP receiver terminal Random Phased Antenna Array (RPAA) is with equal in amplitude and random in phase aperture excitation. The phase shifts of the signals, received by the different antenna elements, are random at the antenna output regardless of the information source direction. These phase spread signals correlate with the recovered pilot signals, phase spread in the same manner. Since the pilots come from the same direction and propagate in the same random environment to the antenna output they should have the same phase spread ("poly-phased" signature) as the information signals. The results of the correlation process are the recovered information signals at base band. The signals coming from other satellites will propagate from antenna aperture to the antenna output in different random environment. Their phase spreads will be different from these of the chosen pilots and they will not correlate during the signal processing. This lack of correlation insures the spatial and polarization selectivity of the SCP system.

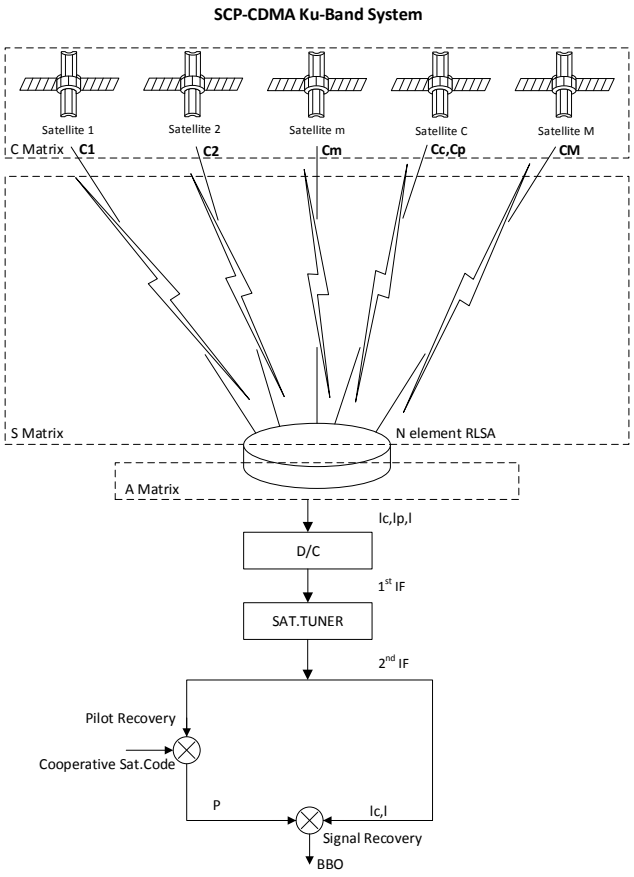



***Fig.2*** *The basic SCP system architecture*

## *3.2 The basic SCP system architecture*

According to the basic SCP system architecture [fig.2], the cooperative satellite is chosen for communications by means of synchronized Pseudo-Noise (PN) code and the well known Code Division Multiple Access (CDMA). This specific SCP feature is of great importance when short acquisition time of the mobile B-MSS SCGS is required. Code synchronization, similar to angular tracking, consists of two steps - acquisition and tracking.

The most widely used algorithm for code acquisition is based on serial search strategy. Here the phase of the local code is changed step by step, in equal increments, resulting in serial search of the code delay uncertainty region until the synchrony position is found. For each value of the phase of the local sequence, a correlation between the input signal and the local signal replica is formed and compared to a threshold. A high value of the correlation (above the threshold) indicates the synchrony position. The acquisition time period is reduced in the modern CDMA systems by well developed methods of parallel and combined search up to several tenths milliseconds. It is incomparable with the acquisition time of the above mentioned, used in Ku and Ka frequency bands, classical methods.

The theory of code tracking in the modern CDMA systems is very well developed too. Similar to acquisition procedures, it is made by software and does not need multichannel RF coherent receiver as it is in classical monopulse tracking. This approach gives the possibility of simultaneous tracking of several cooperative satellites, insuring space diversity and very high degree of communication security.

# *4 RPSC approach*

## *4.1 RPSC (SCP-transmit) – a new spread spectrum beam forming technology*

Reliability, availability and security of real time communications are imperative in the context of wireless communication services. A popular technique used in this scenario is Spread Spectrum (SS). For a communication system to be considered a SS system, it is necessary that the transmitted signal satisfy two criteria:

- The bandwidth of the transmitted signal must be much greater than the message bandwidth;
- The transmitted bandwidth must be determined by some function that is independent of the message and is known to the receiver.

In SS systems, the spreading process is accomplished using a spreading code. Conventionally, it is used Pseudo-Noise (PN) sequences. These sequences are periodic with a long period and they have properties similar to noise. Besides the conventional method of PN periodic sequences generation, others methods can be used in SS systems. A promising one is the use of chaotic sequences as spreading codes.

An important parameter that is sometimes useful in specifying the performance of a SS signal in the presence of interference is known as Processing Gain (PG). It is defined as the ratio of the signal bandwidth to the message bandwidth.

The recent developments of the broadband terrestrial and satellite wireless communication systems leads to new problems in the field of the conventional SS systems. Because the used values of PG are in order of 20 or 30 db, the SS signal bandwidth grows to unpractical high values for adequate signal processing and transmission. The most sensitive to the super wide bandwidth of the SS broadband wireless systems are the antenna beam forming networks.

A new principle to create broadband SS systems was proposed by the author [2]. It is based on transmission of broadband microwave signals in the open space by means of multi element random phased antenna arrays. The sum of the different antenna element signals in a given point in the space has Gaussian probability distribution and noise like properties. The sums in the different directions of the space are not correlated each other. In such way the proposed principle solves simultaneous the problems of the future sophisticated microwave B-MSS, dealing with signal spreading and beam forming.

## *4.2 Improvements of regulatory status of B-MSS VMES using RPSC antennas*

Satellite connectivity while driving traditionally has been possible by using handheld personal terminal equipment with low gain omnidirectional antennas. Recently, the new satellite interactive broadband communication systems use high gain satellite tracking antennas, installed on vehicles. The VMES currently can operate on conventional Ku-band frequencies (14 GHz Uplink, 11-12 GHz Downlink) but only on a secondary basis. This means VMES cannot claim interference protection from primary services such as fixed satellite systems and Earth Station on Vessels (ESV). A co-primary allocation of VMES in the conventional Ku-band would be in the public interest, as it would address a growing commercial demand for on the move services. However, a co-primary allocation would also have to be conditioned on strict adherence to interference avoidance mechanism, which in the best way obviously is satisfied by the RPSC technology.

### *4.3 RPSC technology – the new approach to protect satellite communications from space terrorism*

The European Space Policy Institute (ESPI) issued an article, titled "The Need to Counter Space Terrorism - a European Perspective", arguing for studies to introduce effective counter measures to protect satellites. The article lists several examples of jamming and piracy events that occurred in the commercial satellite sector. One of the conclusions is that the most vulnerable components space systems are the ground stations and communication links. These components are susceptible to attack from widely accessible weapons and technologies. The ESPI agrees with this and says policy makers must consider the system architecture as a whole.

SCP-RPSC technology is one the best technologies, satisfying the above mentioned requirements, as follows:

- SCP in down-links

In this particular case the down-links are well protected from jamming, coming from the side-lobes of the Spatial Cross-Correlation Function (SCCF). SCCF is the virtual SCP antenna pattern at baseband. As it was shown in [1], the level of the side-lobes is very low (in order of -25, -30 db). It leads to good protection rations of SCP down-links against ground based terrorist jamming.

- RPSC in up-links

In this particular case up-links are protected against jamming, coming even from points, close situated to the earth stations – in the main lobe of the satellite up-link receiving antenna. The receiving RPSC circuits will not recovery the jamming signals because of the lack of correlation between the jamming signals, transmitted by conventional high gain antennas, and the recovered random phase spread pilot signals. Situation is similar to the case of CDMA protection against narrowband interference.

The main features of the RPSC technology, when it is used in the up-links of the B-MSS, additionally include:

- Omni directivity for the cooperative satellite, but high equivalent (at base-band) Equivalent Isotropic Radiated Power (EIRP);
- Selection of different terminals and polarizations by Pseudo-Noise (PN) codes;
- Soft handover and virtual multi-beam features;
- The coherent demodulation by means of pilots (specific property of SCP technology), cancelling the Doppler shift and phase jitter, introduced by local oscillators in the satellite systems;
- Compatibility with the existing bent-pipe satellite transponders;
- RPSC up-link protection against active jamming, coming even from points, close situated to the earth stations;
- The SCP-RPSC approach is a breakthrough technology, leading to unpredictable increase of the frequency reuse factor in B-MSS. Close situated B-MSS terminals could communicate with satellites, using the same frequency channel without interference. The isolation among the RPSC and convenient terminals is provided by their specific random phase spread coding.

## *5 Conclusion*

The practical SCP-RPSC principles implementations in transmit and receive mode will drastically change the existing paradigm in the B-MSS communication business in general. Many of the existing problems of the proposed LEO, MEO and GSO satellite systems, dealing with frequency and orbital resource sharing, beam shadowing, terrorist jamming etc., will be solved successfully. In such way the B-MSS reliability and security will drastically be improved.

## *6 References*

1. Demirev V., "Spatial Correlation Processing – the New Approach in the Broadband Satellite Tracking Systems", Journal of Electrical and Control Engineering, Volume 3, Issue 5, pp. 49-54, October, 2013.

2. Demirev V., "Random Phase Spread Coding – the New Way to Communicate with Noise Signals at Microwaves", Journal of Electrical and Control Engineering, Volume 4, Issue 2, pp. 1-9, April, 2014.

3. Demirev V., "SCP-RPSC – the Key Technology for the Next Generation Microwave Communication Systems", Machines, Technologies, Materials, pp. 13-16, N 6, 2015.

# OPTIMIZATION OF THE DESIGN OF FRAGMENTATION WARHEADS FORMING AN AXIAL FLOW OF PREFORMED FRAGMENTS

MSc Petkov, P.S. and Assist.-Prof. Dr. Eng. Tumbarska, A.

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

***Abstract:*** *Constructive variants of warheads forming an axial flow of propagation of preformed elements have been designed. Tests have been carried out on experimental units with varying thickness of wall and shape of the barrier between the preformed elements and the bursting charge. Obtained results show the formation of a high-speed axial flow of a large amount of striking elements of one and the same type having sufficient kinetic energy to hit the targets. Thus, by changing the wall thickness and the barrier shape, it is possible to increase the effectiveness of the fragmentation action by 35-40 % and to provide coverage of a larger area of damage.*
***Keywords****: FRAGMENTATION WARHEADS, PREFORMED FRAGMENTS*

## *Introduction*

The combat effectiveness of ammunitions is assessed by the degree of damage to the object (target). The effectiveness of firing depends on a number of different factors such as: type, size, mobility and vulnerability of the target, scattering characteristics and striking abilities of the ammunition.

Fragmentation charges are among the most common and advanced classes of ammunition designed to hit virtually all types of targets except for underground, underwater and heavily armored targets.

In today's interpretation, fragmentation ammunition means ammunition hitting the target with a high-speed flow of large quantities of the same type of inert striking elements, having a sufficiently high kinetic energy from the action of detonation products of the burst charge of brisant explosive. [1, 2] The striking elements can be obtained either from the natural destruction of the casing of the fragmentation warhead, or from a preset destruction, or in the form of preformed fragments. [3, 4]

Destruction of a projectile or warhead in fragments is a complex fast-running process of converting the energy from the explosive detonation products into energy for deforming and destroying the ammunition casing and transmitting the energy to the formed fragments. [5, 6]

Remote-action ammunition is capable of hitting the target with a fragments flow at the required distance from the blasting site. They are characterized by a large variety of designs capable to perform numerous combat tasks. [3]

The main advantage of fragmentation ammunition with preformed fragments is their high efficiency, which is ensured by the stable characteristics of the fragmentation field.

In modern designs, preformed fragments are typically compact bodies (cubes, spheres, cylinders) that are made of steel or heavy alloys based on wolfram. [7, 8]

## *Experimental units design and testing*

To study the process of formation and operation of the fragmentation field, various specimens of fragmentation warheads were developed and experimental tests were conducted.

An exemplary embodiment of a fragmented warhead design with preformed cylindrical striking elements is shown in Fig.1.

The casing (pos.15) of the grenade is made of an aluminum alloy, and a steel base (pos.22) is installed between the bursting charge (pos.19) and the preformed cylindrical fragments (pos.22) intended to prevent deformation and destruction of the preformed fragments by the products of the bursting charge detonation, and on the other hand to give them initial speed and sufficient kinetic energy to hit the target.

The groove cylinder (pos.23) serves, on the one hand, for placing in its interior space the preformed fragments in bulk, and on the other - for reducing the losses from the friction forces between the preformed fragments and the casing when they are pushed out of the steel plate (pos.22) under the action of the detonation products. The main purpose of the groove cylinder (pos.23) is, after its displacement from the metal support (pos.22), together with the preformed striking elements, to form the character of a concentrated fragments flow (fragmentation field).

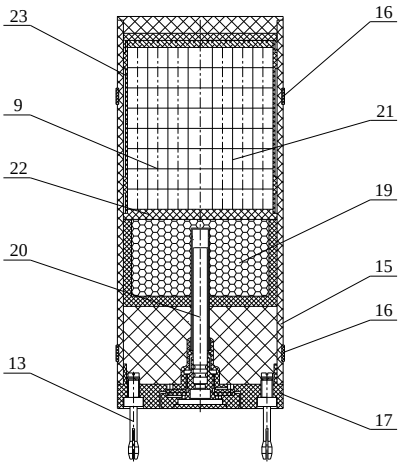



***Fig.1.*** *Fragmentation warhead with preformed fragments: 13 – sockets; 15 – casing; 16 - sealing rings; 17 – bed; 19 – bursting charge; 20 – electrical detonator; 21 – preformed striking elements – cylinders; 22 – safety plate; 23 - groove cylinder.*

The differences in the area of damage in the formation of the concentrated axial front are obtained by a different number of sectors of the groove cylinder - the more the sectors, the greater the dispersion and area of damage.

The developed fragmentation warhead (Fig.1) has the following main characteristics:

- Total weight - 2.975 kg;
- Fragments total weight - 1.710 kg;
- Number of fragments - ≈ 500 pcs.;
- Fragments single weight - 0.0035 kg;
- TNT bursting charge weight - 0.400 kg;
- Metal plate weight - 0.170 kg;
- Casing weight - 0.470 kg.

Two variants of fragmentation warhead have been developed, the main structural difference being the geometrical shape and the thickness of the steel base - 2.5 mm and 5 mm; comparative tests have been made under uniform conditions.

Figure 2 shows the scheme under which the tests of the fragmentation warheads were conducted. Each warhead was located at 12 m from a sectoral circular target fixed at a height of 1.5 m from the ground surface. Cardboard sheets with dimensions 1.4x1.4 m were fixed to a vertical wooden wall in two rows of 15 pieces. The total length of the circular sector was 22 m with a height of 2.8 m, the total area for fixing the hits from the fragments - 58.8 $m^2$.

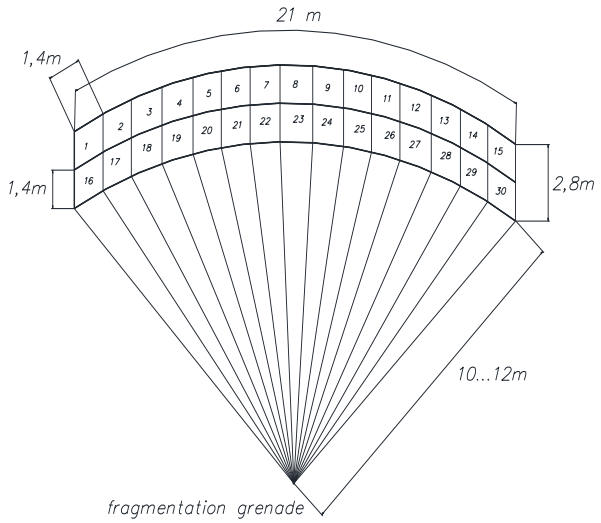



***Fig.2.*** *Scheme for conducting fragmentation warheads tests.*

When a fragmentation warhead explodes, a fragmentation field is formed - a stream of fragments characterized by direction and speed of movement, as well as density, i.e. the number of fragments adjacent to the unit of area they intersect. The density and velocity of the fragmentation flow are important features that determine the possibility of hitting targets. [2, 9, 10] Since the target itself may in general be at a completely different angle with respect to the axis of the fragmentation warhead, when solving the problem of determining the probability of hitting the target, it is necessary, first of all, to know how many fragments fly in a given direction. [11] The answer to this question is given by the so-called fragments dispersal law. It determines the relationship between the relative amount and the velocity of the fragments that scatter in the given direction with respect to the axis of the fragmentation warhead. [12, 13]

Usually this direction is set in a spherical coordinate system with two angles - angle θ in equatorial and angle φ in meridional plane. The angle φ is read from the axis of the fragmentation warhead and can vary from 0 to π. The angle θ varies from 0 to 2π. Thus, the task of finding the fragments dispersal law is reduced to determining the relative amount and velocity of fragments flying in the direction determined by the angles φ and θ. The solution to this problem can be accomplished both theoretically and experimentally. [12, 14]

Experimentally, the angular distribution of the fragments f(φ) and the velocity $V_0=g(\varphi)$ are determined by blasting the fragmentation warhead into a shield target by taking account of the holes in each sector.

When conducting the test, the fragmentation warheads were directed at the center of the sectoral circular target. After each shot the hits in each quadrant were fixed and the results of the tests were recorded in Table 1.

Four pieces of warheads were tested with steel striking elements in the form of cylinders, the casing being made of aluminum alloy, with a steel plate of different thickness and geometric shape placed between the bursting charge and the preformed fragments (experiments No. 1 and 2 – 5 mm; experiments No. 3 and 4 - 2.5 mm).

## *Experimental results and discussion*

The test results obtained are presented in the form of graphs illustrating the fragmentation action of the warheads in various quadrants of the sectoral circular target. Graph 1 shows the hits in the top row of the quadrants, i.e. quadrants 1÷15, chart 2 - hits in the bottom row of quadrants, i.e. 16÷30, and graph 3 - the average results from the hits in the two adjacent vertical quadrants.

***Table 1.*** *Hits of fragments on the target sectors*

| Trial No. / Quadrant | Number of hits in the circular target sectors | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1/16 | 2/17 | 3/18 | 4/19 | 5/20 | 6/21 | 7/22 | 8/23 | 9/24 | 10/25 | 11/26 | 12/27 | 13/28 | 14/29 | 15/30 |
| 1 | 1 | 5 | 4 | 4 | 10 | 12 | 12 | 13 | 13 | 10 | 4 | 3 | 5 | 3 | 1 |
| | 2 | 4 | 5 | 3 | 6 | 20 | 23 | 26 | 17 | 8 | 6 | 5 | 4 | 4 | 3 |
| 2 | 1 | 2 | 4 | 3 | 4 | 7 | 6 | 7 | 5 | 7 | 1 | 3 | 2 | 2 | 3 |
| | 2 | 2 | 2 | 4 | 4 | 7 | 13 | 12 | 10 | 7 | 4 | 2 | 4 | 4 | 1 |
| 3 | 4 | 2 | 4 | 6 | 1 | 6 | 4 | 11 | 6 | 5 | 4 | 3 | 3 | 2 | 2 |
| | 4 | 2 | 3 | 5 | 8 | 7 | 4 | 5 | 5 | 3 | 4 | 4 | 9 | 3 | 4 |
| 4 | 2 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 8 | 5 | 5 | 3 | 3 | 4 | 2 |

Figures 3÷6 show the distribution of fragments in the target from the four trials.

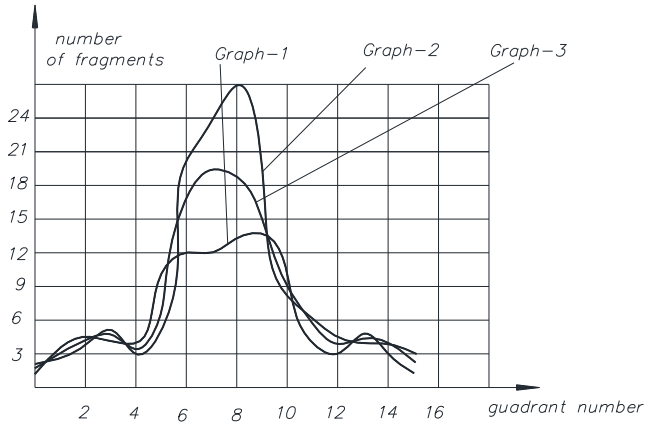



***Fig.3.*** *Fragments distribution scheme - trial 1.*

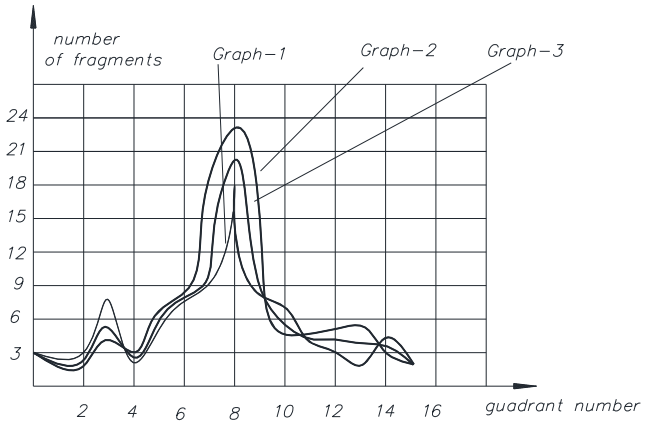



***Fig.4.*** *Fragments distribution scheme - trial 2.*

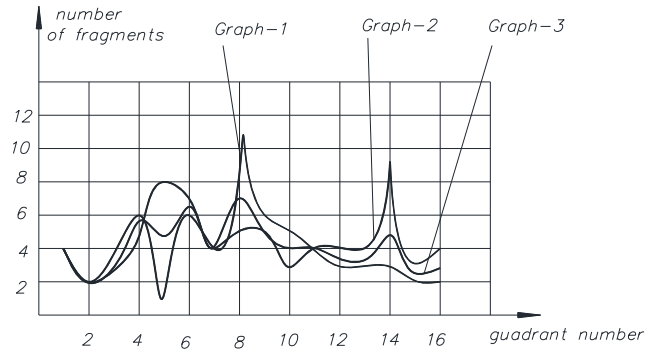



***Fig.5.*** *Fragments distribution scheme - trial 3.*

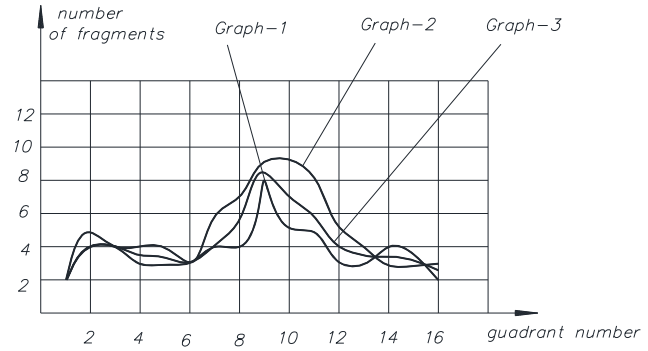



***Fig.6.*** *Fragments distribution scheme - trial 4.*

The analysis of the test results shows that the changes made in the fragmentation warhead design, namely producing the casing of aluminum alloy and the placement of a 5 mm thick steel plate between the bursting charge and the striking steel elements, leads to significant increase of the fragmentation effect. The number of fragments in the area of effect at trials No.1 and 2 is considerably larger, approximately by 20-40 %, compared to trials No.3 and 4, as can be seen from the results in the table and graphs in Fig. 3 and 4, compared to those in Fig. 5 and 6.

It should be noted that the use of thin-walled screens between the bursting charge and the preformed bulk fragments or the absence of a bearing casing leads to deformation of the plate and the fragments, on the one hand, and, on the other - to leakage of detonation products into the gaps formed between the fragments and as a consequence a sharp decrease in their velocity and kinetic energy. In this case, it is appropriate to use an intermediate screen with a mechanical strength commensurate with that of the fragments, located between the bursting charge and the fragments. [15, 16] The use of such a plate, despite the reduction of the filling factor of the explosive, results in a significant increase in the speed of the preformed fragments.

For ammunition with a relatively low starting overload ratio (n<100), the most commonly used are fragmented warhead units with preformed striking elements of various shapes (cube, sphere, cylinder) made of steel or various heavy alloys on the base of tungsten with a density of 16-18 g/cm3. [12, 17] The fill factor (the ratio of the mass of the explosive to the mass of the warhead), when designing warheads, is generally in the range of 0.4 to 0.6, with the fragmentation velocity ranging from 1800 to 2500 m/s. [12, 13]

The designed fragmentation warheads, whose detonation takes place at the optimum distance from the target, significantly increase the effectiveness of fragmentation action on ground-based targets, compared to fragmentation warheads that explode upon contact with the ground. [18]

## *Conclusions*

The following conclusions can be drawn from the tests carried out:

1. The structural changes made to the fragmentation warhead (the producing of warhead casing of aluminum alloy and the placement of a 5 mm thick steel screen between the bursting charge and the preformed fragments) increase the grenade fragmentation effect by approximately 35-40%, covering and effective area of destruction greater than 60 m2. The number of effective fragments in the area of action exceeds 250.

2. The results obtained in the different quadrants after each trial indicate that there is no area which is not affected, moreover, there are fixed hits outside the designated circular sector with a length of 21 m. Hits with a sufficient damage density are fixed bilaterally at least 5 m outside the defined area, indicating that the dispersal angle of the fragments covers a range of approximately 30 m.

3. The analysis of the graphs shows that there is a repeatability of the results, which in turn confirms the correctness of the structural changes made. An increased fragmentation is observed in the area of the lower row of quadrants, i.e. quadrants 16-30.

4. The density of the fragments in and around the middle zone is considerable, which in turn ensures hitting the target in the area of action.

5. In result of the structural changes made, the grenade fragments receive sufficient kinetic energy for damaging the living force.

6. The optimum distance of the grenade detonation from the target is found to be 12 m, resulting in an area with sufficient fragmentation to guarantee the target hitting.

The results obtained may find practical application in the development of specific equipment as part of critical infrastructure protection systems, for example under the „Quasar“ project funded by the European Union within the Intelligent Growth Operational Program.

## *References*

[1] Odintsov, V.A. Modelling the fragmentation processes using unified models. Methodological Instructions. M., “MGTU”, 1991, 58 p.

[2] Baranov, V.L., S.P. Petkov. Modelling the process of forming the initial kinematic parameters of the fragmentation field. News of the Tula State University, Series “Special Machine Building Problems”, issue 4, No 1, 2002, pp 173-177.

[3] Balagansky I.A., L.A. Merzhievsky. Effect of weapons and ammunition. Textbook. Novosibirsk, Publishing house of NSTU, 408 p.

[4] Zecevic, B., J. Terzic, F. Razic, S. Serdarevic-Kadic. Lethal Influence Factors of Natural and Preformed Fragmentation Projectiles. DAAAM International Scientific Book, Chapter 20, 2015, pp. 219-234.

[5] Taylor, G.I. Fragmentation of tubular bombs. Scientific Papers of G.I. Tailor, Vol. III, No 44, Cambridge University, 1963, pp 387-390.

[6] Odintsov, V.A. Mechanics of the impulse fracture of cylinders. Questions of explosion and shock physics. Collection of Articles, MVTU, Vol. 1, pp 22-70.

[7] Rainchard, J., J. Pirson. Deformation and fracture of thick-walled steel cylinders under blast loading. Mechanics, 1958, No 19.

[8] Nadai, A. Plasticity and fracture of solids. M., “Nauka”, 1984. 163 p.

[9] Baranov, V.L., S.P. Petkov. A variant of the straight task for optimizing the parameters of the fragmentation field. Journal of the Technical University - Plovdiv, No 8, 2006, ISSN: 1310-8271, pp 67-74.

[10] Baranov, V.L., S.P. Petkov. Optimization of the fragmentation field parameters. News of the Tula State University, Series “Special Machine Building Problems”, issue 2, No 2, 2001, pp 172-174.

[11] Petkov, S.P. Model for the formation of high-speed elongated striking elements. Engineering Sciences, issue XLV, No 3, 2009. ISSN: 1312-5703, pp 50-57.

[12] Odintsov, V.A. Statistical distributions in fragmentation: Textbook. M., Pu2lishing house of MSTU, 1990. 56 p.

[13] Explosion Physics. Editor L.P. Orlenko. Third edition, revised. Vol. 2, M., FIZMATLIT, ISBN 5-9221-0220-6, 2002, 656 p.

[14] Kalobanova A.E., V.V. Selinova. Fundamentals of the dynamics of the destruction of shells. M., Publishing House of MSTU “N.E. Bauman”, 1996. 98 p.

[15] Kachanov, L.M. Fundamentals of the theory of plasticity, M., “Nauka”, 1979.

[16] Petkov, S.P., V. Nikolova. Modeling of the dynamic properties of the cumulative lining material and casing in a cumulative assembly. Vth International Scientific and Technical Conference "Engineering. Techologies. Education. Security”, Volume 1, 2017, ISSN: 2535-0315, pp 94-98.

[17] Christov, C.I., S.P. Petkov. Comparative analysis of the energy performance of high-speed compact impact elements of cumulative liners with different forming lining profiles. Scientific conference of the Naval University “N.Y.Vaptsarov” – Varna, Section Naval Sciences, 1994.

[18] Georgiev N. L., K. Stoichev, Thu Quang Wu. Modern challenges in military and military technology field. Proc. Conf. with Int. Part. “Metal Science, Hydro- and Aerodynamics, National Security”, 2014, ISSN: 1313-8303, pp 122-128.

# MODIFIED PETRURGICAL MATERIALS BASED ON SEDIMENTARY ROCKS USED FOR BALLISTIC PURPOSES

Prof. L. Lakov PhD, Senior Assist. Prof. Kr. Toncheva PhD, Assist. Prof. Marieta Gacheva,
Institute of Metal Science, Equipment and Technology "Acad. A. Balevski" with Hydro- and Aerodynamics Center – BAS, 67 Shipchenski Prohod Blvd., 1574 Sofia, Bulgaria,
e-mail: krasiton4@abv.bg

***Summary:*** *Bulgaria has a variety of deposits (mainly in northeastern Bulgaria) of sedimentary rocks (marls) suitable for the development of compounding formulations and technology for the production of stone products. On the basis of some of these sedimentary rocks (marls), experimental technologies for innovative formulations with modifiers for usable petrurgical materials are developed and tested. The first prototypes of ballistic protection products are obtained, with physic-mechanical properties better than those when only natural sedimentary rock is used, and lighter and cheaper than in the case of corundum and silicon carbide.*

*The properties of these materials allow for certain alternative applications such as the ballistic protection of ground-based mobile and stationary objects. They also make possible the production of quality articles with protective properties against high-speed kinetic effects, but at significantly lower cost than when traditional materials are used.*

***KEYWORDS:*** *PETRURGICAL MATERIAL, PROTECTION, HIGH-SPEED KINETIC EFFECTS, CORUNDUM, SILICON CARBIDE, SEDIMENTARY ROCKS.*

## *1. Introduction*

**Advanced ceramics for ballistic protection**

Two types of hard ceramics are used: monolithic and composite or two-element $B_4C$-TiB2 ceramics, marl-corundum.

Monolithic ceramics include: oxides (mainly $Al_2O_3$), non-oxide ceramics (silicon carbide, boron carbide, silicon nitride, aluminum nitride, titanium diboride). The basic properties of ceramics for ballistic protection are described in [1-3].

Oxide ceramics, in particular the corundum one, possess physical properties that make them suitable for ballistic protection. Corundum ceramic is cheaper than other ballistic ceramics and can be produced by different methods. Despite its high density (3.95g / $cm^3$), it is suitable for ballistic protection.

In general, non-oxide ceramics have high physic-mechanical properties and relatively low density (except $TiB_2$). This makes them more cost-effective than corundum ceramic, but they are produced by hot pressing, which is expensive and not sufficiently productive. Nevertheless, hot pressing guarantees high mechanical properties. The mechanical properties of hot-pressed corundum are comparable to those of non-oxide ceramics.

Ceramic matrix composites perform very well as ballistic material because of their mechanical properties, especially their fracture resistance. They offer better integrity after ballistic impact than monolithic ceramics.

There is no information in the literature on materials obtained from natural sedimentary rocks modified with materials with high physic-mechanical properties to produce a ballistic product.

Proposed here are combined compositions for new ceramics and corundum or silicon carbide of 30 to 20% Wt% over 100% sedimentary marl rock, fraction from 150 to 250 microns. The aim is to improve the mechanical strength and to maintain low density and low cost.

The mechanical properties of the various new ballistic protection ceramics are given in [4].

The following parameters are determined for the ceramics which will be tested by firing:

- overall shrinkage and change in shape and size;
- density and open pores;
- physical properties (Vickers hardness, fracture strength, sound speed, Jung modulus, flexural strength);
- conformity of the product with the parameters set in the test methodology.

Several factors need to be considered when examining ballistic protection systems: the type of ballistic threat; the manufacturer's capabilities; the properties of the individual armour components. These factors also include the level of threat, the resistance to multiple hits, environmental conditions, spatial constraints, the challenges facing manufacturers, price and weight constraints, the physical properties of the front and the back support material, and the overall ballistic performance of the armour system.

**Design requirements for ceramic armours.**

As with all armoured systems, numerous production factors and solutions affect the performance of ceramic armour.

**Type of ceramics**

The available technical ceramics suitable for ballistic protection are numerous, but are generally divided into cheaper sintered and more expensive hot pressed ones. The higher price is justified when the lower weight of the armoured system is the main requirement. In this case boron carbide is used for individual protection and for aircraft armour elements, as well as silicon carbide for ground equipment. High-density tungsten carbide based ceramics find specific applications where space constraints are limiting. Cheaper ceramics made of sintered 99.5% corundum and silicon carbide or reaction-sintered ceramics, as well as the modified petrurgical materials discussed in this paper, are used when weight restrictions are not the leading ones. However, for many armour systems, more competitive performance and engineering advantages can be provided by high strength steels, titanium, or laminates made of these materials, with an aluminum/composite backing.

**Methods of characterizing ceramic specimens and important ballistic properties**

The material to be tested must be placed in advance under the conditions of the testing environment.

The recommended environmental conditions should be: temperature $200 \pm 2^0$C and relative humidity $65 \pm 5\%$. If conditions other than those are used, they must be recorded.

A minimum of 6 bullets must be fired at the sample and their velocity must be measured.

A hit is recognized only when the sample has been struck at a random angle of incidence smaller than $5^0$. The locations of hits on curvilinear surfaces must be determined and marked in advance.

Full piercing occurs when the bullet passes through the ceramic specimen and pierces the witness plate. All other hits are defined as partial piercing.

The ballistic limit is the velocity for which the puncture probability is exactly 0.5.

Using the Braceton test method, the first cartridge must have a charge which ensures a velocity equivalent to the calculated ballistic limit of the ceramic specimen.

If the first bullet pierces the target, the second cartridge must be loaded with a charge providing a velocity about 30 m/s lower than that of the first one.

***Table 1*** *Ballistic protection ceramics and their mechanical properties*

| Ceramics | Mechanical properties | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Density ($g/cm^3$)** | **Vickers hardness (GPa)** | **Breaking strength three-point bending ($MPa.m^{1/2}$)** | **Young's module (GPa)** | **Speed of sound (km/s)** | **Bending strength (MPA)** | **Micro hardness ($kg/m^2$)** |
| Corundum, sintered | 3.60-3.95 | 12-18 | 3.0-4.5 | 300-450 | 9.5-11.6 | 200-400 | 1,000 |
| Corundum-Zirconium, sintered | 4.05-4.40 | 15-20 | 3.8-4.5 | 300-340 | 9.8-10.2 | 350-550 | 1,200 |
| Silicon carbide, sintered | 3.10-3.20 | 22-23 | 3.0-4.0 | 400-420 | 11.0-11.4 | 300-340 | 1,100 |
| Boron carbide, hot-pressed | 2.45-2.52 | 29-35 | 2.0-4.7 | 440-460 | 13.0-13.7 | 200-300 | 1,400 |
| Titanium diboride, sintered | 4.55 | 21-23 | 8.0 | 550 | | 350 | 1,100 |
| Titanium diboride, hot-pressed | 4.48-4.51 | 22-25 | 6.7-6.95 | 550 | 11.0-11.3 | 270-400 | 1,050 |
| Pure petrurgical material | 2.65 | 10-13 | 2.6-2.7 | 280-300 | 8.0-8.5 | 250-300 | 800 |
| Composite ceramic material - 75% marl and 25% corundum | 2.95 | 11-16 | 2.8-2.9 | 290-360 | 9.0-9.8 | 290-320 | 980 |
| Composite ceramic material - 75% marl and 25% silicon carbide | 2.75 | 12-17 | 3.0-3.5 | 300-390 | 9.8-10.3 | 300-340 | 1,000 |

The use of ceramics for ballistic protection raises the following problems:

- low resistance to repeated hits;
- complex design solutions in its application as an element of armour protection;
- unsatisfactory reparability;
- high price.

According to the data given in [5] for the value of 1 $m^2$ of different protective structures, when compared to steel, a hybrid structure providing equivalent protection from 7.62 mm armour piercing cartridges is from 6 times (for$Al_2O_3$) to 15 times (for SiC) more expensive. For protection against 12.7mm armour piercing cartridges the corresponding figures are 4 times for $Al_2O_3$ and 12 times for SiC.

In this respect, it is of practical interest to explore the possibility of developing new ceramic-based materials which possess satisfactory protective performance properties but are more cost effective. The purpose of the present study is to determine the applicability of newly developed petrurgical material as an element of ballistic protection structures.

## *2. Experiments*

The subject of the present study is a ceramic material reinforced with corundum or silicon carbide components up to 30% and developed for use in building construction or as street pavement. The production technology and product properties are described in [6, 7]. The following recipe composition was chosen for preparing the samples: chamotte, fraction below 200μm – 50%, marl rocks – 40%, washed kaolin – 5%, glass frit – 5%, corundum or silicon carbide ingredients – up to 30% over 100%.

Corundum plays the role of a framework in the structure of the total mass. In the high temperature liquid phase synthesis of the basic matrix and the formation of the petrurgical phases, the high-strength modifying additives remain unchanged and form the macrostructure of the material.

After homogenization, the material was wetted to a moisture content of 20% and allowed to rest for 24 h. Tiles with dimensions of 55 x 55 x 11mm were pressed on a hydraulic press. After drying, they were subjected to high temperature synthesis at a temperature of 1,100° C and left there for 1 hour, then allowed to cool in the oven. The dimensions of the final specimens are 50 x 50 x 10 mm.

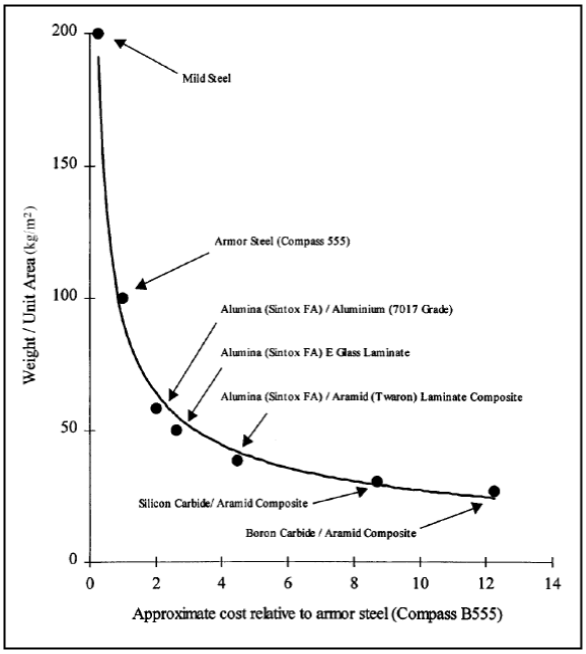



***Figure 1*** *Protective power/price ratio for different materials*

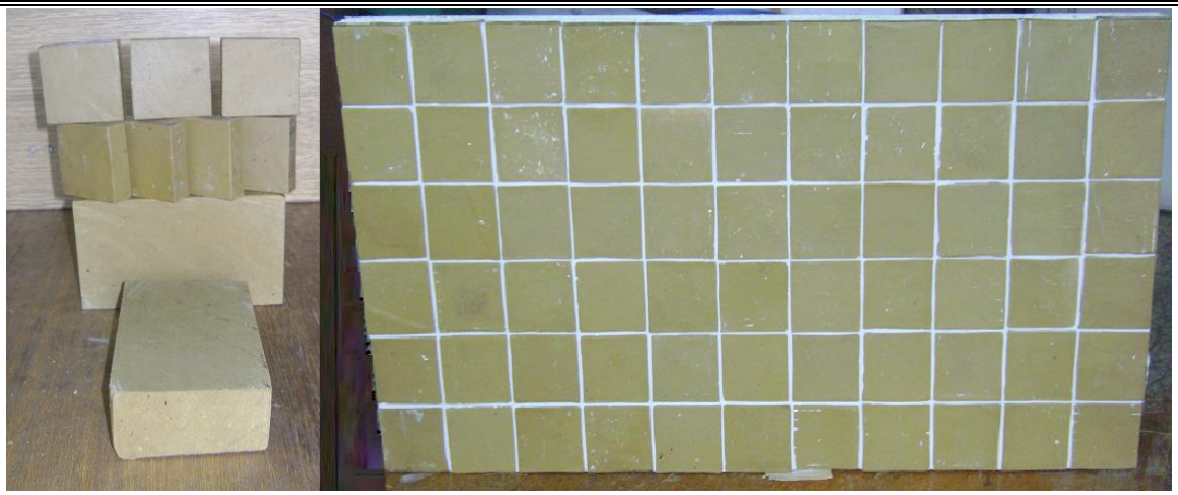


***Figure 2*** *Elements and a protective panel of composite petrurgical material obtained on the basis of corundum-modified sedimentary rocks - 25% over 100% with a grain composition of 150 - 250 microns*

The X-ray phase analysis of the prepared samples revealed the presence of anortite CaAl2Si2O8 -59% and dioxide CaMg (Si2O6) – 39% phases, as well as amorphous phase – 2%. This composition almost fully coincides with the eutectic one for the anorthite-diopside system and this determines the fine crystal structure of the final product. The relative density is 2.60 kg/m$^3$. The micro hardness is 800 kg / mm$^2$.

In the preparation of ballistic test specimens, a 10 mm thick Dyneema HB25 plate was used as a backing layer. The ceramic tiles were glued to the plate using Sikabond AT polyurethane adhesive. On the outside, the specimen was bandaged with a single layer of Kevlar fabric.

The general characteristics of the test specimen are:

- dimensions 325 x 200 x 25 mm;
- weight – 2.370 kg;
- Dyneema plate weight – 0.650 kg;
- ceramics density o – 2.6 g / cm$^3$;
- total weight of the ceramic tiles – 1.400 kg



***Figure 3*** *Front view of a specimen*



***Figure 4*** *Back view of a specimen and witness plate*

### *3. Ballistic tests*

The tests were conducted at the Central Artillery Technical Testing Ground at Zmeevo according to its established methodology under the following conditions:

- weapon type – 7.62mm Modernised Kalashnikov Automatic Rifle;
- initial bullet speed – 720m s;
- ammunition used – 7.62 x 39mm cartridge, model 1943 with steel core;
- shooting distance – 30 m;
- speed sensor – photoelectronic.

A 6-mm-thickwitness plate made of armour steel was placed behind the specimen for recording the piercing effect. The test results are given in Fig. 3 and 4.

### *4. Conclusions*

1. By means of high-temperature liquid-phase synthesis, composite petrurgical materials and articles made of them were synthesized and then used for additionally armouring a protective surface. Their behaviour when subjected to high-speed kinetic effects was investigated. It was found that when struck by the bullet core, the ceramics absorbs the impact energy and is destroyed, while the protected surface behind remains unchanged.

2. It is proved that corundum granulate in the composite material improves the ballistic performance of the petrurgical material.

### *5.References*

[1]. F. Cline and M. L. Wilkins, “The Importance of Material Properties in Ceramic Armor”; pp. 13-18 in DCIC Report 69-1, Part I, Ceramic Armor, 1969.

[2]. S. K. Chung, “Fracture Characterization of Armor Ceramics”, Am. Ceram. Soc. Bull., 69 (3) 358-366 (1990).

[3]. D. J. Viechnicki, M. J. Slavin and M. I. Kliman, “Development and Current Status of Armor Ceramics”, Am. Ceram. Soc. Bull., **70** [6] 1035-39 (1991).

[4]. E. Medvedovski, “Alumina Ceramics for Ballistic Protection”, Am. Ceram. Soc. Bull., 81 (3) 27-32 (2002).

[5] E. Chistyakov, D. Kupryunin, and Gladyshev. "Ultra-short Anti-Brushed Steel",
http://www.niistali.ru/upload/iblock/954/Optional% 20 variant.pdf.

[6]. Lakov L., Encheva St., Tsonev P., Vasilev V., Zhivov B., Toncheva Kr., Technology for production, chemical and phase composition of new "yellow paving stones" obtained on the basis of sedimentary rocks, International Scientific Conference " Design and Construction of Buildings and Structures ”, 15 ÷ 17 September 2016, Varna, Bulgaria, pp. 115-120.

[7]. Lakov L., Stoimenov N., Tsonev P., Vasilev V., Zhivov B., Toncheva Kr., Physicochemical, mechanical properties and tomographic analysis of new "yellow paving stones" from petro-material, Proceedings, International Scientific Conference "Design and construction of buildings and facilities ”, DCB 2016, September 15-17, 2016, Varna, Bulgaria, pp. 121-127.