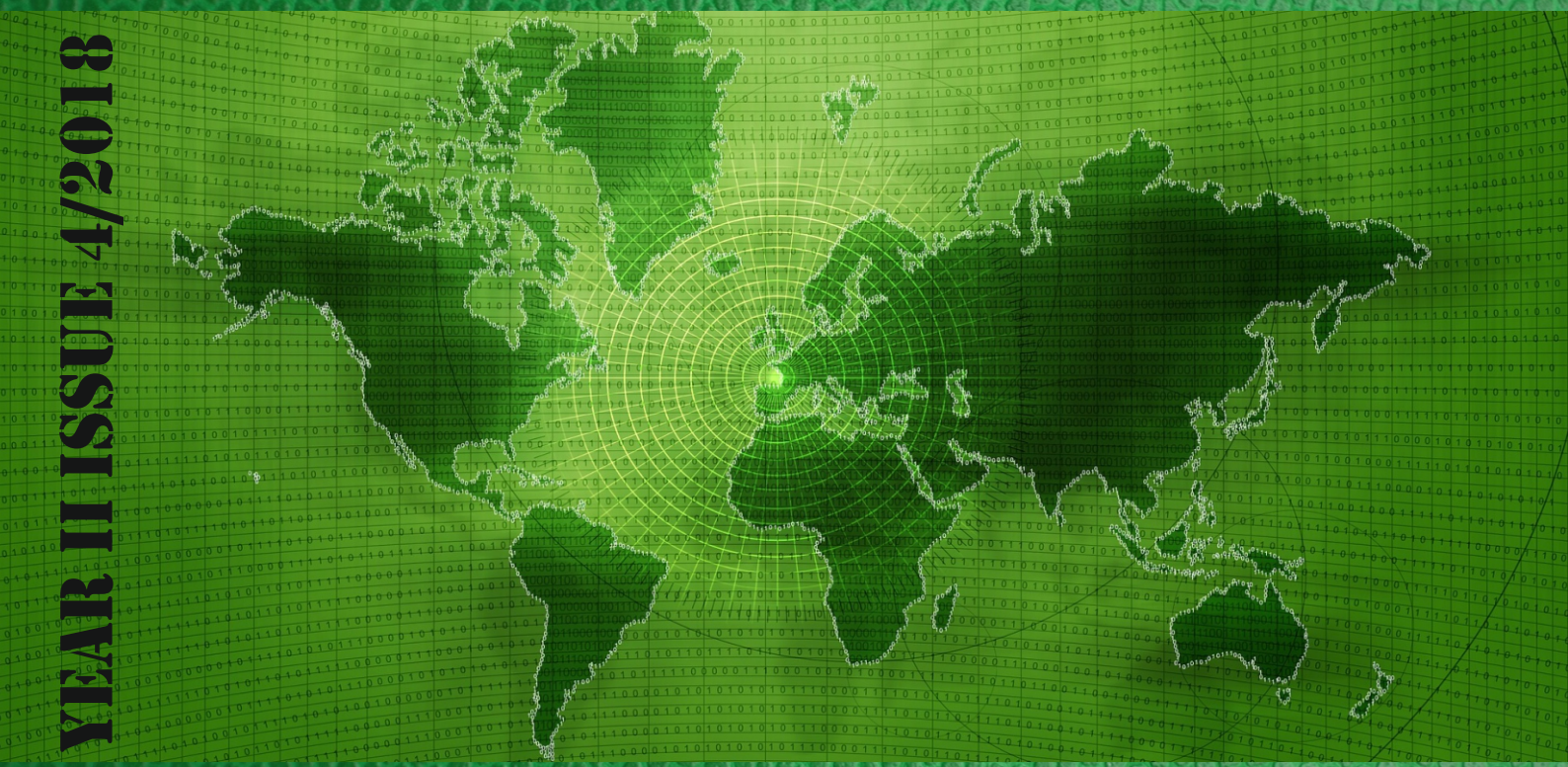
INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

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



YEAR II ISSUE 4/2018

PUBLISHER SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING - INDUSTRY 4.0
BULGARIA

INTERNATIONAL SCIENTIFIC JOURNAL

SECURITY & FUTURE

PUBLISHER:

SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING INDUSTRY-4.0

108, Rakovski Str., 1000 Sofia, Bulgaria

tel. (+359 2) 987 72 90, **tel./fax** (+359 2) 986 22 40**,**

office@stumejournals.com,

www.stumejournals.com

ISSN (PRINT) 2535-0668

ISSN (Online) 2535-082X

YEAR II, ISSUE 4 / 2018

EDITORIAL BOARD

CHIEF EDITOR

Prof. Nikolay Radulov

New Bulgarian University, Sofia, BG

Members:		
Alexander Baranov, Prof.	Higher School of Economics	RU
Alexander Kurbatski, Prof.	Belarusian State University	BY
Alexander Troyanskiy, Assoc. Prof.	Odessa State Polytechnic University	UA
Andrzej Misiuk, Prof.	Warsaw University	PL
Ariana Bejleri, Assoc. Prof.	Polytechnic University of Tirana	AL
Galina Zhavoronkova, Prof.	National Aviation University, Kyiv	UA
Gudrun 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

ON ONE APPROACH TO SOLVING THE PROBLEM OF FORMALIZATION AND MODELING OF THE AIRPORT SECURITY THREATS SPACE
Lev N. Elisov, Nikolay I. Ovchenkov 152

NATIONAL AND INTERNATIONAL SECURITY

SOCIAL SECURITY DETERMINANTS
Dr Wojnarowska-Szpucha S. 158

THE EXAMINATION OF NEW-TYPE SECURITY CHALLANGES CONCERNING THE EUROPEAN UNION WITH REGARD TO COMMUNITY DIRECTIVES OF STRICTER GUN CONTROL
Assistant Lecturer. Dr. Szabó Cs. PhD. 163

ORGANIZATION AND CONDUCT OF MILITARY MANEUVERS "EAST 2018" IN THE RUSSIAN FEDERATION
Chief Assistant Professor PhD eng. Dolchinkov N. T. 167

TYPES OF EXTRAORDINARY SITUATIONS OF TECHNOLOGY AND ACTIVITIES IN EXCEPTIONAL SITUATIONS WITH THE RELEASE OF RADIOACTIVE SUBSTANCES
Chief Assistant Professor PhD eng. Dolchinkov N. T., Acos. Prof. PhD Hvostova M. S., Karaivanova-Dolchinkova B. E. 170

RADIOLOGICAL THREATS TO THE SECURITY ENVIRONMENT
Chief. Assist. Prof. Nikolay I. Padarev PhD 173

THE IMPACT OF TECHNOGENIC ACCIDENTS ON THE SECURITY ENVIRONMENT
Chief. Assist. Prof. Nikolay I. Padarev PhD 176

INFORMATION SECURITY

APPROACH ANALYSIS TO PREVENT STEGANOGRAPHY DATA FLOWS AS A CORPORATE SECURITY BREACHES
Lopit P., Assoc. Prof. PhD. Alieksieiev V. 180

SECURE BIG DATA AND IOT WITH IMPLEMENTATION OF BLOCKCHAIN
Daniela Mechkaroska, Aleksandra Popovska-Mitrovikj and Vesna Dimitrova 183

INVESTIGATION OF AWSCTD DATASET APPLICABILITY FOR MALWARE TYPE CLASSIFICATION
Doc. Nikolaj Goranin PhD., Dainius Čeponis 186

TECHNICAL FACILITIES FOR ENSURING SECURITY

DISTRIBUTED SENSING AS A NEW TOOL FOR FIBRE INFRASTRUCTURE PROTECTION
M.Sc. Munster P. PhD., M.Sc. Horvath T. PhD., M.Sc., M.Sc. Vojtech J. Ph.D. 190

TRIBOLOGICAL PROCESSES EVALUATION DUE TO BULLET-RUBBER CHOPPER WHEEL INTERACTION PHENOMENA
M.Sc. Ing. Dimitrova Ya. 193

EVALUATION METHOD OF THE ARTILLERY'S EFFECTIVENESS AGAINST UNITARY TARGET
M.Sc. Ing. Katsev I., Assistant 196

EXPERIMENTAL DEVELOPMENT OF A SMART ARTILLERY AND MINE ORDNANCE FUZE BASED ON ARDUINO MICROCONTROLLER PLATFORM
Cad. Dimitrov Mir., Assoc. Prof. Ing. Ganev V. PhD.,M.Sc.Ing. Dimitrova Ya. 199

EVALUATION OF HIT'S GROUPING DEVIATION DUE TO TRIBOLOGICAL PROCESSES IN BULLET-RUBBER CHOPPER WHEEL INTERACTION
M.Sc. Ing. Dimitrova Ya. D. 204

INFORMATION TECHNOLOGIES EMPLOYED IN ARMAMENT DESIGN FOR EDUCATION
Delchev L., Beevski A., M.Sc. Ing. Antonov S., Prof. Lilov I. 208

ON ONE APPROACH TO SOLVING THE PROBLEM OF FORMALIZATION AND MODELING OF THE AIRPORT SECURITY THREATS SPACE

Lev N. Elisov [1], Nikolay I. Ovchenkov [2]

[1]Moscow State Technical University of Civil Aviation, Moscow, Russian Federation
[2]P.G. Demidov Yaroslavl State University, Yaroslavl, Russian Federation

Abstract. *The paper examines the issue of formalization and mathematical modeling of potential dangers (hereinafter referred to as threats). Such threats occur in the external environment in relation to the object of transport infrastructure (hereinafter referred to as airport), while ensuring aviation security. The issue of formalization is manifested in the significant uncertainty of physical presentation of security threats and difficulties in choosing a class of functions that describe threats' spread dynamics.*

The authors suggest using the heuristic approach and the format of the boundary value problem of field theory when moving from a linguistic description of the threat space to its formal representation and description. A mathematical model based on partial differential equations describing threat space is proposed. In addition to this, assumptions and limitations associated with its hypothetical representation are formulated. Modeling and results are presented in the form of threat intensity distribution on some topology of the transport infrastructure object. The results are interpreted as the initial information for modeling the airport security system.

1. Introduction

There has been a definite tendency to consider aviation security issues from the point of view of optimal management of its level with a consistent solution of identification, measurement, evaluation and decision-making problems in recent years. Results analysis obtained in this direction shows the urgent need to move to the issue of formalization of the subject area and mathematical modeling. It should be made in order to optimize the process of managing airport's aviation security level.

The authors consider aviation security as a state associated with certain parameters of the investigated object. The quantitative display of such parameters in the dynamics of their changes under the influence of external and internal factors remains in the boundaries acceptable for the operation of the object. The state of the object under protection can be considered as some of its characteristics, associated with an uneven, heterogeneous and unstable environment that provides protection for this object. In this case, we should talk about two issues of formalization and modeling. On the one hand, it is issue of modeling object security threat space. On the other hand it is issue of modeling some space that provides object security. The authors examine the first one in this paper.

The effective functioning of civil aviation as an industry that provides transport services is primarily related to the concept of security. Security is a state of complex system where the action of external and (or) internal factors does not lead to the system deterioration or to inability of its functioning and development. Aviation security (hereinafter referred to as AS) is one of the most important components of this concept. It is defined as the state of aviation protection from illegal interference into aviation activities.

AS is ensured on the basis of organizational and regulatory methods at the present time. Such methods exclude questions of optimizing decisions since optimization involves measuring and evaluating the parameters under study on the basis of some formalization. A few attempts to use the mathematical apparatus in this subject area are connected with economic models [1] and risks [2–4], i.e. with the solution of local problems. The issue of modeling AS as a state of the transport infrastructure object has hardly been discussed in the sources that the authors know. At the same time, it is possible and even necessary to solve the issue of ensuring security on the basis of mathematical modeling in response to ever-increasing demands on civil aviation associated with the increase and complexity of threats to the security of its facilities. In their works [5], the authors showed this and substantiated the fundamental possibility of formalizing and modeling the space of airport security threats based on the theory of boundary value problems [6] and heuristic procedures.

2. Formulation of the problem

The problem of providing AS of the transport infrastructure object is solved within the framework of the complex interaction of the following main elements (Fig. 1):

- The transport infrastructure object (airport), characterized by the presence of a certain structure, including, among other things, critical (most important) elements, interconnected within a certain topology.
- Security system (hereinafter referred to as SS) of the facilities. It includes a set of measures, methods, procedures, technical means, aviation personnel, regulatory framework, etc.
- Subject of illegal activity (hereinafter referred to as SIA) (violator). It is complex concept that includes all possible attributes for the realization of potential threats and the commission of an act of illegal interference.

Thus, the level of AS of the transport infrastructure object is determined as the result of opposition (counteraction) between SIA and SS. Two concepts are introduced and used for this purpose and in accordance with the recommendations of the International Civil Aviation Organization (ICAO) [7]. It is object vulnerability and object security levels. The object vulnerability assessment is implemented in order to determine the degree of its security against potential threats. The object security levels are set depending on the level of potential and immediate threats and define the requirements for the SS. In both cases, the assessment is of high quality and is implemented by expert methods. There are some papers [8] who offer methods for quantifying vulnerability on a qualimetric or probabilistic basis. Such works have not found practical application. Besides, they are of academic interest.

It is necessary to obtain quantitative information on the threats intensity by the topology of object under protection, taking into account critical elements in order to build the structure and configuration of the object security system that meet the vulnerability requirements and the specified security levels (Fig. 1). In a direct formulation, this problem does not have an exact mathematical solution because of formalization problems. In this case, it is proposed not to receive a decision but to take it. For this purpose, the authors have analyzed the structural model of the SIA (violator) [9]. They propose to introduce conditional quantitative estimates of threats level corresponding to the security levels scale. Such the estimates should be obtained by expert methods. It is necessary to obtain the threats' intensity distribution according to the object topology on the basis of these estimates. Such estimates should be considered as boundary and initial conditions if this problem is solved on the basis of the theory of boundary value problems. The proposed heuristic approach is most likely the only possible one since the problem does not have an exact mathematical solution. The second important problem here is to define a class of functions that can describe the expected

distribution. This is even more difficult, because you can only talk about a hypothetical threat space. It is proposed to consider the set of such functions so that, having received a set of distributions of threat intensities, to build the final distribution using heuristic procedures. The resulting distribution of potential threats contains comprehensive information for the formation of an object protection field, whose intensity according to the object topology is aligned with the quality of the SS functioning in quantitative representation. It makes it possible to formulate requirements for a set of aviation security facilities.

The proposed approach was called heuristic modeling. The concept includes a mathematical model and a heuristic formulation of the problem. In this case all the difficulties of formalization go into the permissible inadequacy of the mathematical model with subsequent interpretation of the statistical results of modeling on the basis of decision-making theory.

It is necessary to clarify the difference between two concepts: impact and danger. Impact is any action aimed at an object in order to influence it, cause changes. Danger is the possibility of the occurrence of circumstances in which matter, field, energy, information or a combination of them can thus affect the complex system. In a follow-up it will lead to deterioration or inability to function and develop it. The impact is related to illegal interference act implementation, and the danger is considered as a potential possibility of committing such an act in the context of AS.

The analysis and prediction of undesirable events is carried out on the basis of statistical data on the realized impacts in modern aviation security systems.Considering the fact that the frequency of such events is very small, the statistical sample is significantly limited, with all the expected problems for the forecast. The approach proposed by the authors is based on the examination of potential threats and obtaining the threat intensity distribution by the topology of the protection object in a quantitative matter. The author's approach seems preferable for optimal control of aviation object security level.

3. Heyristic formalization and classes of functions

The structural and logical model of the SIA [9] includes a representative set of threats of different physical nature, significant uncertainty in the description of characteristic and objective functions. As a result, it is characterized by insurmountable difficulties of mathematical formalization. Heuristic formalization here should be understood as the solution of the inverse problem. It means that it is not necessary to give a mathematical interpretation of the threat. It is necessary to provide to a problem setter the right to choose a certain class of equations (equation) for a certain threat, having agreed in advance with the possible incongruity of the real threat and model. The inadequacy of the model is compensated by a set of statistics based on the results of modeling using the chosen equations. It is important that the solution in this case is not obtained as a result of modeling, but is adopted on the basis of certain heuristic rules.

In their works [6, 10] the authors showed the rincipal possibility of using differential equations in partial derivatives for solving this problem. Some classes of such equations are presented below [6, 11–12].

$$\frac{\partial}{\partial x}\left[A_1\,(x,y,z,U,t)\frac{\partial U}{\partial x}\right]+\frac{\partial}{\partial y}\left[A_2\,(x,y,z,U,t)\,\frac{\partial U}{\partial y}\right]+ \frac{\partial}{\partial z}\left[A_3\,(x,y,z,U,t)\,\frac{\partial U}{\partial z}\right]=a\frac{\partial^2 U}{\partial t^2}+b\frac{\partial U}{\partial t}+c\mathrm{U}+\alpha, \quad (1)$$

where

$$a=f_1\,(x,y,z,U,t)\geq 0; \quad c=f_3\,(x,y,z,U,t)\geq 0; \quad (2)$$

$$b=f_2\,(x,y,z,U,t)\geq 0; \quad \alpha=f_4\,(x,y,z)\geq 0.$$

The values of the function U are sought inside a certain domain G bounded by the surface Γ (by the line Γ in two-dimensional case), on which the values of the required function are known, determined by:

$$(\alpha\,U+\beta\frac{\partial u}{\partial n})_\Gamma=F, \quad (3)$$

where α and β – prescribed functions of the point on the boundary Γ;

$F=\varphi\,(x,y,z,U,t)$- some known function in the boundary points;

$\frac{\partial U}{\partial n}$ - the derivative of the required function along the normal to the boundary at the boundary point under consideration.

Depending on the nature of the right-hand side, expression (1) turns into equations of:

elliptic type, when $a=b=0$; $c\geq 0$; $\alpha\geq 0$;

parabolic type, if $a=0$; $b>0$; $c\geq 0$; $\alpha\geq 0$;

hyperbolic type, when $a>0$; $b\geq 0$; $c\geq 0$; $\alpha\geq 0$.

Depending on the values of the functions α and β, the boundary value problem described by equation (1) is called:

Dirichlet problem, when $\alpha=\varphi_1\,(x,y,z)\neq 0$; $\beta=0$.

Neumann problem, if $\alpha=0$; $\beta=\varphi_2\,(x,y,z)\neq 0$,

mixed problem, when $\alpha\neq 0$; $\beta\neq 0$.

Functions A_1, A_2 и A_3 determine parameters of the space substance. Equation (1) is solved in the homogeneous domain G, when

$$A_1=A_2=A_3=const>0.$$

We have for an inhomogeneous volume domain:

$$A_1\neq A_2\neq A_3\neq A_i;\ A_i=\varphi\,(x,y,z)\geq 0$$

Equation (1) is linear when the coefficients A_1, A_2, A_3, a, b, c,d, α and β depend only on the coordinates. It is nonlinear if at least one of them depends on U.

Equations of elliptic type describe processes where function values do not change with time (problems of steady heat conduction, steady filtration flows, stationary magnetic and electric fields, etc.). Equations of parabolic type reflect many nonstationary processes occurring in space (the exploitation of productive oil and gas layers taking into account their elastic capacity, the dynamics of the processes of heating and cooling bodies, etc.).

The necessity of solving hyperbolic equations arises in the study of transient processes in various problems of potential theory. Wave ($a\neq 0$; $b=c=0$; $\alpha\geq 0$) and telegraph ($a\neq 0$; $\epsilon\neq 0$; $c\neq 0$; $\alpha\neq 0$) equations are particular cases of equations of hyperbolic type.

The most common problem is the displacement of the interface of two phases with additional conditions on it with respect to its temperature, heat balance, incoming and outgoing fluxes, latent heat when speaking on the problems of equations of parabolic type. These conditions, as well as the non-linearity of the coefficients for coordinate derivatives, arising from the temperature dependence of the thermal substance conductivity, relate such problems to the category of non-linear boundary-value problems of special complexity.

This problem is described by a system of equations:

$$\begin{aligned}&\frac{\partial}{\partial x}\left[A_1^v\,(x,y,z,T)\frac{\partial T_v}{\partial x}\right]+\frac{\partial}{\partial y}\left[A_2^v\,(x,y,z,T)\frac{\partial T_v}{\partial y}\right]+\\&+\frac{\partial}{\partial z}\left[A_3^v\,(x,y,z,T)\frac{\partial T_v}{\partial z}\right]=C_T^v\,(x,y,z,T)\frac{\partial T_v}{\partial t}\\&\frac{\partial}{\partial x}\left[A_1^w\,(x,y,z,T)\frac{\partial T_w}{\partial x}\right]+\frac{\partial}{\partial y}\left[A_2^w\,(x,y,z,T)\frac{\partial T_w}{\partial y}\right]+\\&+\frac{\partial}{\partial z}\left[A_3^w\,(x,y,z,T)\frac{\partial T_w}{\partial z}\right]=C_T^w\,(x,y,z,T)\frac{\partial T_w}{\partial t}\end{aligned} \quad (4)$$

where indexes V and W characterize the belonging of the functions to the liquid or solid phase of the substance respectively. On the space boundaries S_1 and S_2boundary conditions similar to (3) are defined, in the phase regions V and W, initial conditions $T_v(0)=\varphi_1\,(x,y,z,0)$ and $T_w(0)=\varphi_2\,(x,y,z,0)$, and on the phase interface $\xi(t)$ - additional conditions:

$$T_v/_\xi\,(\mathrm{t})=T_w/_\xi\,(\mathrm{t})=T_0; \quad (5)$$

$$\theta_v-\theta_w=\theta_c, \quad (6)$$

where θ_v and θ_w – heat fluxes flowing to the boundary respectively from the regions of phases *v* and *w*.
θ_c – heat flow absorbed (or released) during the phase substance transformation.

Thus, the issue of formalizing threats to security is solved by choosing an equation and setting it in line with a certain threat.

4. Solution methods

Practical implementation of problems of this type is rather complicated. There are various methods for solving them, some of which are discussed below [13–17].

Analytic solutions of equations of the form (1), (4) can be obtained only for regions of regular configuration with the parameters A_1 = A_2 = A_3 = const ≠ 0 by using the Fourier method, integral or variational methods. The analytic solution of these equations in the general case is practically impossible in the regions of an arbitrary configuration. Therefore, various numerical methods are used to solve them in a general formulation. Besides, only grid method has versatility. This method makes it possible to use it for solving a wide range of boundary-value problems, including non-linear functions of the equations. The grid method provides a finite-difference approximation of all functions of the equation and allows one to reduce its solution to solving systems of equations of the n-th order (n is the number of elements of the space partition) having the form [15, 16, 18]:

$$\begin{cases} \left(\sum_{k=1}^{2m} g_k U_k - U\sum_{k=1}^{2m} g_k\right)_1 = b_1 \dfrac{\partial u_1}{\partial t} \\ \left(\sum_{k=1}^{2m} g_k U_k - U\sum_{k=1}^{2m} g_k\right)_i = b_1 \dfrac{\partial u_i}{\partial t} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \left(\sum_{k=1}^{2m} g_k U_k - U\sum_{k=1}^{2m} g_k\right)_n = b_n \dfrac{\partial u_n}{\partial t} \end{cases} \quad (7)$$

where *k* – number of the point, near to the main point $x_0 y_0$;
m = 1;2;3;….. – number of edges in the point $x_0 y_0$;
g_k – approximate (average) value of the function A on the interval (*o, k*) obtained as a result of finite-difference approximation;
i= 1;2;3;4;…..; n – number of the point.
We will get for the j–th moment of time equation of the following type by performing a similar finite-difference approximation of the right parts of the equations of the system (7):

$$\left(\sum_{k=1}^{2m} g_k\ U_k - U\sum_{k=1}^{2m} g_k\right)_i^{j} = g^{j}_{\tau\,(i)} U_i^{j} - g^{j}_{\tau\,(0)} U_i^{j-1}$$

or after reduction of similar members,

$$U_i^{j}\left(\sum_{k=1}^{2m} g_k + g_\tau\right)_i^{j} - \sum_{k=1}^{2m} g^{j}_{k\,(i)}\, U^{j}_{k\,(i)} = g_{\tau\,(i)} U_i^{j-1}$$

where g_τ – approximate value of the function *b* on an interval Δt = $t_j - t_\tau$
These equations form a system:

$$\begin{cases} \boldsymbol{U_1^j}\left(\sum_{k=1}^{2m} \boldsymbol{g_k} + \boldsymbol{g_\tau}\right)_1^{j} - \sum_{k=1}^{2m} \boldsymbol{g_{k(1)}}\, \boldsymbol{U^{j}_{k\,(i)}} = \boldsymbol{g^j_\tau}\, \boldsymbol{U_1^{j-1}} \\ \boldsymbol{U_1^j}\left(\sum_{k=1}^{2m} \boldsymbol{g_k} + \boldsymbol{g_\tau}\right)_i^{j} - \sum_{k=1}^{2m} \boldsymbol{g_{k(i)}}\, \boldsymbol{U^{j}_{k\,(i)}} = \boldsymbol{g^j_\tau}\, \boldsymbol{U_i^{j-1}} \\ \boldsymbol{U_1^j}\left(\sum_{k=1}^{2m} \boldsymbol{g_k} + \boldsymbol{g_\tau}\right)_n^{j} - \sum_{k=1}^{2m} \boldsymbol{g_{k(n)}}\, \boldsymbol{U^{j}_{k\,(n)}} = \boldsymbol{g^j_\tau}\, \boldsymbol{U_n^{j-1}} \end{cases}$$

The presented methods provide an exhaustive mathematical apparatus for formalizing the hypothetical space of threats to the security of the transport infrastructure object and solving this problem. It should be understood that any formalization assumes a certain degree of approximation to a real object or process, all the more so that in this case the degree of uncertainty in the physical understanding of the object and its formalized description remains and is quite high.

5. Mathematical model and its numerical implementation

We consider the process of spreading the danger to distributed objects, in the first approximation [19–20], as a diffusion process as one of the possible options. Diffusion is the mutual penetration of contiguous substances into one another in the direction of a drop in the substances concentration. It leads to a uniform substance distribution throughout the volume. Diffusion takes place in gases, liquids, solids. With certain reservations, diffusion as a process can be attributed to the process of spreading the danger. Then the mathematical model can be represented by the diffusion equation:

$$\frac{\partial}{\partial x}\left(\sigma(x,y)\frac{\partial u}{\partial y}\right) + \frac{\partial}{\partial y}\left(\sigma(x,y)\frac{\partial u}{\partial y}\right) = f(x,y), (x,y)\epsilon D \quad (8)$$

where u — danger level, $\sigma(x,y)$ — danger permeability, $f(x,y)$ — danger sources density distribution.

We introduce the concepts of "danger permeability", similar to, for example, the heat conductivity in heat distribution problems, and "danger sources density distribution", similar to the density distribution of heat sources by analogy with other diffusion processes. And the positive value of danger sources density distribution characterizes threats to security, and negative - sources of active counteraction to threats. The danger permeability can be different in the domain *D*. It is obvious that permeability should be much less in the protected area than beyond the boundaries of the protected area. At this stage of the study, we consider the permeability of the environment and danger sources density distribution by expertly determined estimates.

Equation (8) is solved in the domain *D* including the protected object and the surrounding area. Boundary conditions must be given on the boundary of the domain We take the zero boundary conditions

$$u_r = 0 \quad (9)$$

Condition (9) means that there is no danger at the domain boundary. A different danger level can be set at the boundary.

Thus, the threat modeling will be considered as a boundary-value problem (8, 9).

The analytical solution of problem (8, 9) is practically impossible. We apply numerical methods for solving boundary value problems. The finite differences method [14–18] has been chosen from various numerical methods [15, 16, 18] for numerical problem solution. It is the simplest one in the implementation for the solution of the problem under consideration. Besides, it provides acceptable accuracy with low computational costs.

We construct a uniform grid on the *XOY* plane to implement the finite differences method. For this we construct two families of equidistant (equidistant) lines

$$x_i = x_0 + ih_x, \quad i = 0, 1, 2, \ldots N_x;$$
$$y_i = y_0 + jh_y, \quad j = 0, 1, 2, \ldots, N_y, \quad (10)$$

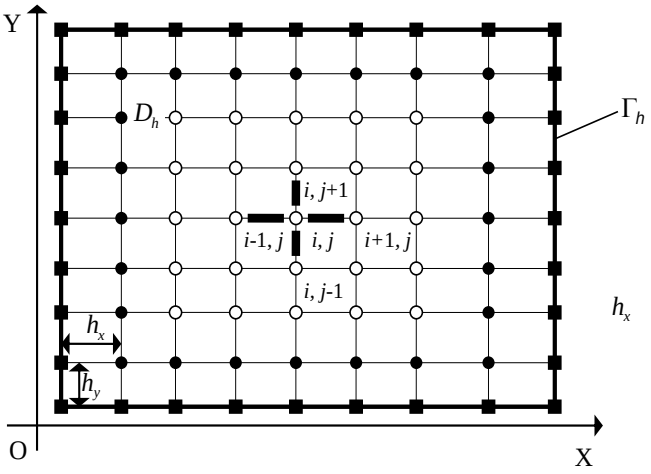
where h_x — grid step, X-direction, h_y — grid step, Y-direction.

In this case we get *grid with nodes* on *XOY* plane $(ih_x, jh_y), \quad i = 0, 1, 2, \ldots, N_x, \quad j = 0, 1, 2, \ldots, N_y$

An example of a grid is shown in Fig. 2.

We consider the nodes that belong to the domain $\bar{D} = D + \Gamma$. Those nodes that are inside the domain *D* are called *internal* (the inner nodes are indicated by o in Fig. 2), and their set is called *grid domain* D_h. The points of intersection of lines (10) with the boundary Γ are called *boundary nodes* (they are indicated ■ in Fig. 2), and their set is called *grid boundary* Γ_h. In the case of a *non-rectangular domain*, the nodes nearest to the boundary are considered as boundary nodes (the distance from the boundary in the directions of the axes X and Y does not exceed the value of the corresponding step). The nodes closest to the grid boundary are called *boundary nodes* (they are indicated • in Fig. 2).

Fig. 2. Grid domain example



We consider *grid functions* of grid nodes $u_h\left(x_i, y_j\right)$ instead of functions $u\left(x, y\right)$ of continuous arguments $x, y \in D$. If a linear differential operator *L* is given, acting on the function *u*, then, replacing the derivatives of the *Lu* with difference relations, we obtain a difference expression $L_h u_h$. It is a linear combination of the values of the grid function u_h on a certain set of grid nodes, called a *template*.

We write the difference approximation of equation (8) for the internal node using the integro-interpolation method [20], a five-point pattern and a constant grid step along the axes *X* and *Y*,

$$-\left[\frac{\sigma(x_i+h/2, y_j)}{h^2}+\frac{\sigma(x_i-h/2, y_j)}{h^2}+\frac{\sigma(x_i, y_j+h/2)}{h^2}++\frac{\sigma(x_i, y_j-h/2)}{h^2}\right]u_{i,j}+$$
$$\frac{\sigma(x_i+h/2, y_j)}{h^2}u_{i+1,j}++\frac{\sigma(x_i-h/2, y_j)}{h^2}u_{i-1,j}+\frac{\sigma(x_i, y_j+h/2)}{h^2}u_{i,j+1}+$$
$$+\frac{\sigma(x_i, y_j-h/2)}{h^2}u_{i,j-1}=f\left(x_i, y_j\right), (x_i, y_i)\in S_h$$

or $a_{i,j}u_{i,j}-a_{i+1,j}u_{i+1,j}-a_{i-1,j}u_{i-1,j}-a_{i,j+1}u_{i,j+1}-$
$-a_{i,j-1}u_{i,j-1}=-f_{i,j}, \quad (11)$

Where $a_{i,j}=\frac{\sigma(x_i+h/2, y_j)}{h^2}+\frac{\sigma(x_i-h/2, y_j)}{h^2}+\frac{\sigma(x_i, y_j+h/2)}{h^2}+$
$+\frac{\sigma(x_i, y_j-h/2)}{h^2}$,

$a_{i+1,j}=\frac{\sigma(x_i+h/2, y_j)}{h^2}$, $a_{i-1,j}=\frac{\sigma(x_i-h/2, y_j)}{h^2}$,

$a_{i,j+1}=\frac{\sigma(x_i, y_j+h/2)}{h^2}$, $a_{i,j-1}=\frac{\sigma(x_i, y_j-h/2)}{h^2}$,

$f_{i,j}=f(x_i, y_i), (x_i y_i)\in D_h$.

The above expressions allow us to approximate an environment with inhomogeneous properties. All the coefficients in the difference formulas will be constant for a domain with homogeneous properties.

The boundary conditions (9) are approximated as follows

$$u_{ij}=0\ , (x_i y_j)\in D_h \quad (12)$$

The approximation proposed has an error order $O\left(h^2\right)$.

We obtain a system of algebraic differential equations with sparse matrices writing the equation (11) for each node where grid function is unknown, numbering nodes sequentially, taking into account boundary conditions and moving all the known members of the right side. Solution is sought only at internal nodes and boundary conditions (12) are taken into account in the right parts of differential equations in the case of the Dirichlet problem.

It is not necessary to apply the general methods of storing sparse matrix when using regular difference template and applying iterative methods for solving systems of differential equations. It is sufficient to store arrays of coefficients of finite-difference approximation for systems of the form (11). We can store two coefficient arrays A_Y A_X connecting the nodes in the template, respectively, of the axes X and Y (Fig. 3)

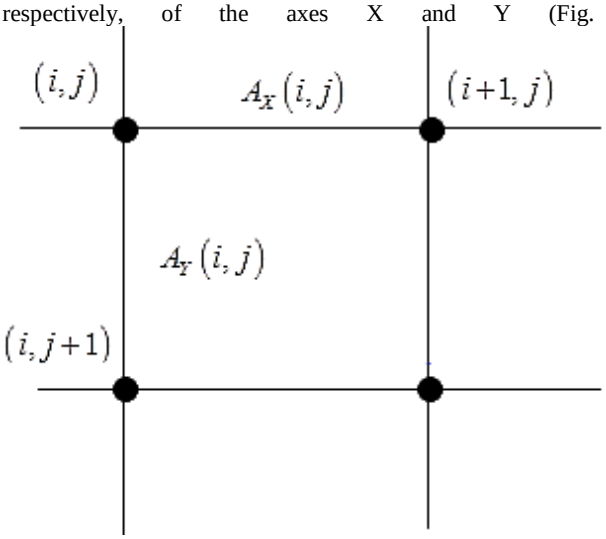


Fig. 3. *The coefficients of a differencing template*

We use the Seidel iterative method [21, 22] for the numerical solution of the system of difference equations. This method provides a sufficiently good rate of convergence and agrees well with the difference representation of the model with relative simplicity of implementation.

In Seidel's method, each element of the grid domain corresponds to an element of a two-dimensional array with indices equal to the node coordinates. In each iteration, the nodes are sequentially bypassed (we take a detour along the horizontal grid lines). For the current node, the refined approximation of the solution is calculated using a formula having the form for the adopted coefficient storage scheme

$$U_{(i,j)}=\frac{1}{Ax(i,j)+Ax(i-1,j)+Ay(i,j)+Ay(i,j-1)}$$
$$[Ax(i,j)\cdot U(i+1,j)+Ax(i-1,j)\cdot U(i-1,j)++Ay(i,j)\cdot$$
$$U(i,j+1)+Ay(i,j-1)\cdot\ U(i,j-1)\ ++f(i,j)] \quad (13)$$

When calculating by (13), we use the approximations already updated in this iteration in neighboring nodes. The approximation obtained is written in place of the old value. The process ends when the norm of the relative change in the solution is sufficiently small

$$\frac{\|U^{(k)}-U^{(k-1)}\|}{\|U^{(k)}\|}\le\varepsilon,$$

where $\mathbf{U}^{(k)}$ и $\mathbf{U}^{(k-1)}$ — solution vectors on the k-th and $\left(k-1\right)$-th iterations, ε — given small positive number.

6. Results of modeling

Single threat modeling results implemented in MATLAB system [23–24] are presented below. Variants of the main program and functions implementing the iterative process are developed.

The problem is solved in a rectangular domain, with the coordinates of the lower-left corner of x1 = 0, y1 = 0 and the upper-right corner of x2 = 1 and y2 = 1. Grid pitch h = 0.01, permeability of the external environment sigma = 1.0, coordinates of danger source xDan = 0.5 and yDan = 0.5, danger magnitude uDan = 1.0. Coordinates of the protected area xProt1 = 0.2, yProt1 = 0.4, xProt2 = 0.4, yProt2 = 0.6, permeability of the protected area sigma1 = 1.0e-12. Danger density within the protected area is zero. The decision was made up to epsilon = 10-6. The three-dimensional graph of the solution surface is shown in Fig. 4.

From the graph in Fig. 4 danger level is sharply reduced, but is not zero in the protected area with almost zero danger permeability

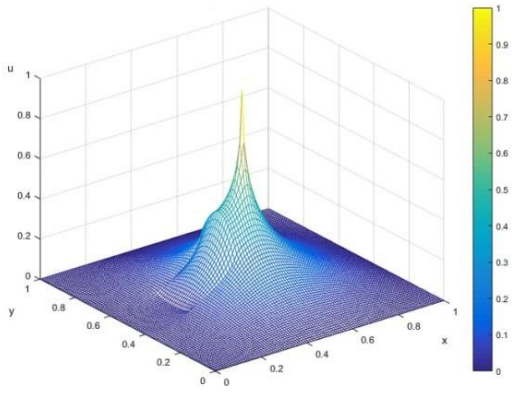


Fig. 4. *Solution surface graph*

.

Danger values can be clearly seen on the graph of the level lines (Fig. 5).

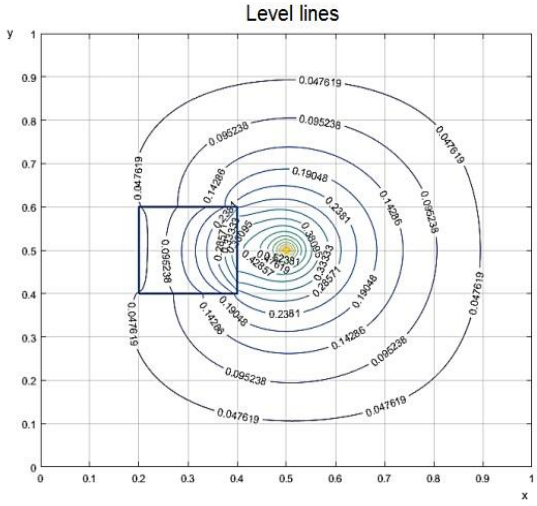


Fig. 5*. Graph of lines for solving the problem with one danger source*

The protected area is highlighted by a rectangle.
The solution is obtained after 1979 iterations (Fig.6).

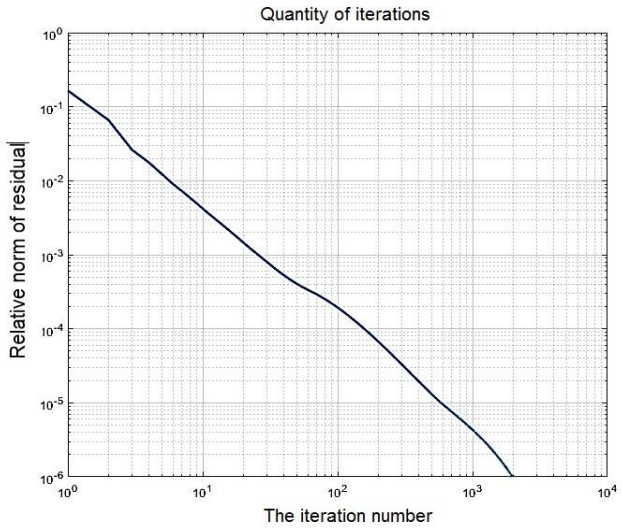


Fig. 6. *The graph of dependence of the relative norm of the correction on the iteration number when solving the problem with one danger source*

The results obtained should be considered as intermediate, more precisely, as initial, taking into account the limitations and assumptions presented above. Next, we must solve the problem of finding statistics for solving similar problems for various initial and boundary conditions and for other classes of functions. The final solution, in this case, should not be obtained, but adopted on the basis of certain heuristic rules. The results prove the principal possibility of applicability of the author's approach, connected with the combination of heuristic formalization and mathematical modeling with the subsequent decision-making on the configuration of the requirements for the object's protection system.

7. Conclusion

The proposed author's approach is the first stage in the solution of the global issue of creating an automated system for managing the level of aviation security of objects with a distributed structure (airports). A heuristic method was developed in combination with heuristic procedures, which excludes all previously uncontrollable difficulties of formalization from the process of mathematical modeling. The adequacy of the mathematical model, the reliability and accuracy of the results obtained is solved within the system of decision-making on the formation of requirements for technical means of protection on the basis of the principle of acceptability of aviation security level. At this stage, the transition from the intensity of the distribution of security threats by the object topology to the performance indicators of the protection system and its elements is carried out. This transition is the prerogative of further scientific development of the authors.

8. References

1. Y. Wang, H. Sun, J. Zhu, B. Zhu. Optimization Model and Algorithm Design for Airline Fleet Planning in a Multiairline Competitive Environment. Mathematical Problems in Engineering. Article ID 783917, 13 (2015).
2. F. L. Edwards, D. C. Goodrich. Introduction to Transportation Security. — CRC Press,388 (2012).
3. J. Price, J. Forrest. Practical Aviation Security: Predicting and Preventing Future Threats. — Butterworth-Heinemann, 598 (2016).
4. G. Tamasi, M. Demichela. Risk assessment techniques for civil aviation security. Reliability Engineering & System Safety, Vol. 96, Issue 8, 892-899, (2011).

5. L. Elisov, N. Ovchenkov, R. Fadeev. Introduction to the theory of aviation security / [ed. L. Elisov]. — Yaroslavl: Filigree, 320 (2016).
6. S. J. Farlow. Partial Differential Equations for Scientists and Engineers. — Wiley, 448 (1982).
7. Safety Management Manual (PMU). DOC 9859. AN / 474. Second edition. — ICAO, Montreal, 240, (2009)
8. V. Volynsky,Yu. Volynsky-Basmanov, Yu Mikhailov. On the issue of the definition and quantification of threats to the implementation of acts of illegal interference into the activities of civil aviation facilities. — Moscow: Transport Safety and Technology, No. 1 (24), 24–29, (2011).
9. L. Elisov, N. Ovchenkov. On the issue of structural modeling of subjects of transport security. Scientific Bulletin of the Moscow State Technical University No. 197. — Moscow: MSTUCA, 58–63, (2013).
10. L. Elisov, N. Ovchenkov. Some issues of grid and neural network modeling of airport security management problems. Scientific Bulletin of MSTUCA, **20**, No. 03. — Moscow: MSTUCA,21-29, (2017)
11. J. R. Buchanan, Z. Shau. A First Course in Partial Differential Equations. — World Scientific Publishing, 624 (2017).
12. J. D. Logan. Applied Partial Differential Equations. — Springer, 289 ()2014).
13. S. Chapra. Numerical Methods for Engineers. — McGraw-Hill Science, 994 (2009).
14. G. F. Pinder. Numerical Methods for Solving Partial Differential Equations. — Wiley, 320 (2018).
15. G. D. Smith. Numerical Solution of Partial Differential Equations: Finite Difference Methods. — Clarendon Press, 350 (1986).
16. S. Mazumder. Numerical Methods for Partial Differential Equations: Finite Difference and Finite Volume Methods. — Academic Press, 484 (2016).
17. S. Rao. The Finite Element Method in Engineering. — Butterworth-Heinemann, 782 (2017).
18. G. E. Forsyte, W. R. Wasow. Finite-Difference Methods for Partial Differential Equations. — Dover Publications, 464 (2004).
19. R. S. Varadhan. Lectures on Diffusion Problems and Partial Differential Equations. — Springer, 315 (1981).
20. A. Samarskii, P. Vabishchevich. Computational heat transfer. — Moscow: Librocom, 784, (2014).
21. C. T. Kelley. Iterative Methods for Linear and Nonlinear Equations. — Society for Industrial and Applied Mathematics, 180 (1987).
22. V. Gorbachenko. Computational linear algebra with examples on MATLAB. — St. Petersburg: BHV Petersburg, 320, (2011).
23. H. Moore. MATLAB for Engineers. — Pearson, 688 (2017).
24. J. Li, Y.-T. Chen. Computational Partial Differential Equations Using MATLAB. — Chapman & Hall, 378 (2008).

SOCIAL SECURITY DETERMINANTS

Dr Wojnarowska-Szpucha S.
Military University of Technology, Poland
Email: sylwia.wojnarowska-szpucha@wat.edu.pl

Abstract: *The article contains a description of the national security system of the Republic of Poland, in accordance with the division written in the National Security Strategy of the Republic of Poland of 2014. Particular attention was focused on the subsystem of support, including social entities. The second part presents the selected determinants of social security*.

Keywords: NATIONAL SECURITY, SOCIAL SECURITY, SOCIAL SECURITY CONDITIONS, UNEMPLOYMENT, MIGRATION, POVERTY.

Introduction

Security is one of the basic values and human needs, [security (survival) and development is the main goal of each entity in the long-term][1]. American psychologist, Abraham Maslow, the author of the hierarchy of needs, identified five human needs: physiological, security, belonging, recognition and self-fulfilment. According to him, security is already placed in the second position just after the psychological needs of humans, such as food, housing, clothing and procreation[2]. Because this is one of the most-awaited needs of a human, citizen, it is also the basis for the proper functioning of the country, therefore the priority of each state is to care for security. Nowadays, this task is particularly difficult due to the variety of security threats, their unpredictability, and therefore security should be perceived as a continuous process.

So what is security, in the literature of the subject one can find many definitions of this concept, the most concise is given by the Dictionary of Polish language, where security is: [a state of non-threat][3], while the Dictionary of terms in the field of national security defines safety as: [a state that gives you confidence and guarantees its maintenance and chances for its improvement. One of the basic human needs is a situation characterized by a lack of risk of losing something that a person particularly values, e.g., health, work, respect, feelings, material goods][4], according to J. Stańczyk [security is the main need of a man and social groups, and at the same time the most important goal][5] the definitions quoted indicate that security is extremely important for a man, social groups, countries, it creates opportunities for development, ensures a peaceful existence, so it is necessary to create opportunities for its effective assurance.

The nature of security manifests itself in various dimensions due to the objects, which is why in the literature on the subject we distinguish military, political, economic, cultural, ecological, information and social security[6]. Individual types of security have an impact on each other, therefore, in order to ensure it, it is necessary to maintain care for the others.

The aim of this article is to illustrate the concepts regarding security, the structure of the national security system of the Republic of Poland with particular emphasis on social security, its conditions and the impact on the security of an individual, a citizen.

1. The location of the social security system in the National Security System of the Republic of Poland

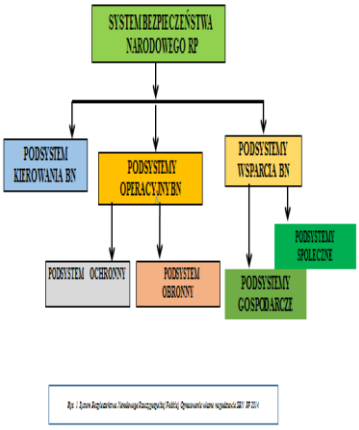
When beginning this chapter, the definitions of national security, state security and social security should be clarified, but before this happens it is advisable to illustrate the differences in the concept of nation and state. According to W. Kitler, the nation is [… a multicultural (multi-ethnic) civil society, inhabiting a territory (always identified with the territory of the state), connected with material and moral values, the implementation of which can be ensured only within the state][7], the state according to the definition of the Dictionary in the scope of national security is: [a political organization of a social group recognized by the international society including a specified territory, in which its authority applies along with the laws it creates][8]. In the same dictionary, we can find definitions of state security, namely: it is a [real state of internal stability and sovereignty of the state, which reflects the lack or occurrence of any threats (in the sense of satisfying basic existential and behavioural needs of society and treating the state as a sovereign entity in international relations] and state security defined as [the state obtained as a result of the properly organized defense and protection against the external and internal threats defined by the relation of the defense potential to the scale of threats][9].

Nowadays, many various internal factors influence security [they are related to what is happening inside the national security, and these are factors of the material-energetic, social and cultural nature][10] and external [they include the same factors, but constituting the property of the national security environment and affecting them both directly and indirectly][11], other security conditions include: variability, unpredictability and surprise[12], as distinguished by researchers, they cause that security is not a permanent, certain phenomenon established on a fixed basis. Due to the impact of all these factors, the conditions of state security are constantly striving to improve their ways, means to provide it, by implementing new strategic documents, operating procedures and organizational structures.

In the Republic of Poland, the National Security Strategy of the Republic of Poland of 2014 is the strategic document covering the issues of national security. It is a document prepared in accordance with the provisions of the Act of November 21, 1967 on the general obligation to defend the

[1] S.Koziej, *National Security Strategy (of a State),* in: *Fundamentals of security of the contemporary state (entity), implications,* : ed. J. Pawłowski, AON, Warsaw 2015, p. 493.
[2] See Maslow A. *Motivation and personality,* PWN, Warsaw 2016, p. 115-119.
[3] www.sjp.pwn.pl/slowniki/bezpiecze%C5%84stwo.html (access 22.10.2018).
[4] Ed. J. Pawłowski, *Dictionary of terms in the field of national security*, AON, Warsaw 2009, p. 13.
[5] J.Stańczyk, *Contemporary understanding of security,* ,ISP PAN, Warsaw 1996, *p*. 18
[6] Cf. ed. M. Leszczyński, *Security in the local dimension,* Difin, Warsaw 2013, p.11; A. Skrabacz, S Sulowski, *Social security. Concepts, conditions, challenges*. Elipsa, Warsaw 2012, p.12.
[7] W.Kitler, *National Security of the Republic of Poland, Basic categories, conditions, system,* AON, Warsaw 2011, p. 21.
[8] Ed. J. Pawłowski, *Dictionary of terms in the field of national security*, AON, Warsaw 2009, p. 95.
[9] Ibidem, p.16.
[10] W.Kitler, *National Security of the Republic of Poland, Basic categories, conditions, system,* AON, Warsaw 2011, p. 101.
[11] Ibidem, pp.101.
[12] See J. Pawłowski, J. Marczak, K. Gąsiorek *The concept, character and determinants of national (state) security*, in: *Fundamentals of security of the contemporary state (entity) implications,* ed. J. Pawłowski, AON Warsaw 2015, p. 20.

Republic of Poland[13], including in its content the general problems related to security and ways of using available entities that are owned by the state. This document systematizes the strategic potential of the national security of the Republic of Poland, defines its objectives[14], defines the national security system as: [strengths, means and resources designated by the state to carry out tasks in this area, properly organized, maintained and prepared][15] and performs the division into subsystems of management and execution, including the operational subsystems, which include the defense and security subsystem and the support subsystems including the economic and social subsystem[16] .



The management subsystem is the overriding link of the national security system, which consists of the public authorities and managers of organizational units that perform tasks aimed at ensuring and maintaining the national security. As part of the management subsystem, a special main role was attributed to the Parliament, the President of the Republic of Poland and the Council of Ministers.

The executive subsystems constitute the forces and means to secure the security through the implementation of various tasks. The structure of executive subsystems is formed by the operational and support subsystems, the tasks of the operational subsystems (defense and protection) include the prevention of threats that may adversely affect the functioning of the state, citizens and the associated national security threat. The entities of the defense subsystem are:

- Polish Armed Forces, whose task is to maintain readiness to act in the event of a threat to state security and implementation of the mission: [guaranteeing defense of the state and opposition to armed aggression, supporting protection subsystems in the field of internal security and assistance to the public, participation in the process of stabilizing the international situation][17];

- diplomacy, which is supposed to create a positive image of our country, to resolve conflicts, disputes through diplomatic actions;

- military special services[18] aimed to collect, process information significant to state security, identification and counteracting the external and internal threats to the defense of the country;

- industrial defense potential, whose overriding goal is to provide equipment for armed forces and other entities taking care of the security of the Republic of Poland.

The structure of the protective subsystem includes: justice, anti-terrorism institutions, law enforcement and public order services, civil protection and rescue services, border services, security services for public authorities and administration, institutions for cyber security, institutions for protection of classified information and other bodies. [The main tasks in protection subsystems include ensuring conditions for maintaining the constitutional order, internal stability of the state and civil security][19], i.e. the broadly understood protection against non-military threats[20], created by human actions or forces of nature.

The support subsystems (social and economic), as the name of "support" indicates, are designed to support, power the remaining subsystems. The tasks that the social subsystem has to face concern the broadly understood social security, they consist of: protection of national heritage, education for security, social security, demography, social potential, media in the social security system. In the second issue of this article, the tasks carried out under this subsystem will be discussed in detail.

The mission of the economic subsystems is to protect the country's economic potential against all activities that accompany the crisis situations or war actions and the support of operational subsystems. As part of the economic subsystem, we distinguish: financial, energy, food, ecological, infrastructural security, and maintaining strategic reserves.[21]

2. Social security structure[22]

Social security in the literature of the subject is defined as: [… the entirety of legal and organizational activities performed by government entities (national and international), non-governmental organizations and citizens themselves, which aim at providing a certain standard of living to individuals, families and social groups, and preventing their marginalization and social exclusion][23]. A. Skrabacz specifies that social security [means the protection of existential foundations of the life of

[13] See the *Act of November 21, 1967 on the general obligation to defend the Republic of Poland*, Journal of Laws of 2018, item 1459, 1669, art. 6, par. 1 and art. 4a, par 1.
[14] [The potential of national security serves the implementation of national interests and the achievement of strategic goals], *National Security Strategy of the Republic of Poland*, Warsaw 2014, p. 13.
[15] Ibidem, p. 13.
[16] See. Ibidem, p. 13.
[17] *National Security Strategy of the Republic of Poland*, Warsaw 2014, p. 31.
[18] See the Act of June 9, 2006 on the Military Counterintelligence Service and the Military Intelligence Service, Journal of Laws of 2017, item 1978, 2405, of 2018, item 650, 1544, 1669.
[19] *The White Book of National Security of the Republic of Poland*, BBN, Warsaw 2014, p.169.
[20] [Non-military threats – a type of threat involving such a combination of events in international relations, in which it is likely that there will be a limitation or loss of conditions for undisturbed existence and development of the state, or its sovereignty as a result of non-armed violence against it], [20] Ed. J. Pawłowski, *Dictionary of terms in the field of national security*, AON, Warsaw 2009, p. 95.
[21] See *The White Book of National Security of the Republic of Poland*, BBN, Warsaw 2014, p.184-190, *National Security Strategy of the Republic of Poland*, Warsaw 2014, p.40-42.
[22] The content of this chapter is based on: the Research Grant of the Institute of Security and Defense Systems of the Faculty of Logistics of WAT no. 997/2018 entitled *The logistics system as the determinant of the defense capabilities of the Republic of Poland*, and in it: *Migration of the population as a threat to social security in Poland* – by S.Wojnarowska-Szpucha.
[23] M. Leszczyński, *Social security and state security*, Pub. Of the Jan Kochanowski University of Humanities and Natural Sciences, Kielce 2009, p. 37.

people, ensuring the possibility of satisfying individual needs (material and spiritual) and the implementation of life aspirations through the creation of conditions for work and study, health protection and pension guarantees][24]. J. Gierszewski defined the essence of social security as: [counteracting social threats and ensuring the possibility of survival and free development of individuals and social groups under specific conditions with the use of available means][25]. In fact, all this means that social security should constitute the subject of interest for all entities: citizens, non-governmental and other institutions and the state, because only with the involvement and cooperation of all of them it is probable to entirely guarantee it.

The components of the social security subsystem based on the National Security Strategy of the Republic of Poland and the White Book of National Security of the Republic of Poland constitute (see fig. 2): the management of social security development, social potential of Poland, counteracting demographic threats, social security, education for security, protection of national heritage and the role of media in guaranteeing social security.

Social security management includes state bodies and various self-government institutions (social welfare centres, support centres, social welfare homes, counselling centres and other) public service organizations[26], whose activities are socially useful.

The social potential of the state is formed by the human capital, the development of which increases the possibilities of an active social life of an individual, which is an important determinant of the activity of the civil society, as well as the improvement of the quality of life of citizens. With the development of human capital, it is possible to increase employment, prolong professional activity, improve the quality of life, the situation of older people and people at risk of social exclusion, improve health and improve the qualifications of citizens[27].

The contemporary education system aims to educate an active and mobile society, aware of the importance of security. The aim of education of social security subsystems is to prepare them for functioning in the event of threat and war, and to implement social support tasks for operational subsystems.

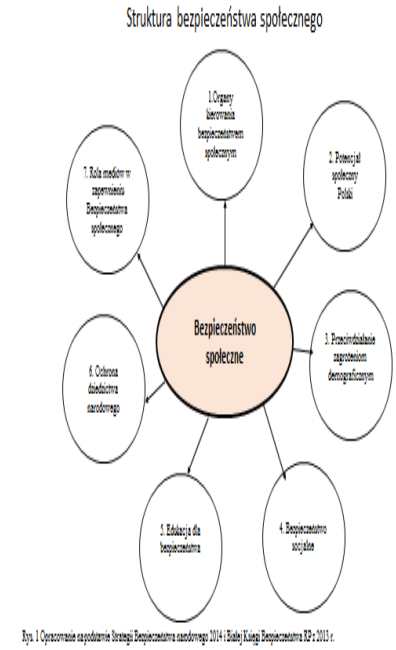
Counteracting demographic threats is an important task for the Polish state, it is necessary to counteract unfavourable demographic changes. The implementation of this objective includes: an appropriate family-friendly policy (encouraging the possession of offspring, supporting families with children), proper migration policy (motivating to return to Poland, offering support after returning, improvement of offers on the labour market) and immigration policy adequate to our country (satisfying the needs of immigrants in the field of work and care).

Social security requires many activities aimed at increasing the sense of social security, including preventing social exclusion and reducing poverty. These activities will be implemented through: creating an effective system of benefits and social benefits, access of citizens to all goods (equal access to education, health care), activization of the excluded people, building good relations between the state and the citizen, and cooperation of all social assistance institutions.

Education for security due to changing threats, their unpredictability, it is necessary to educate the society, raising its knowledge, awareness concerning the contemporary security threats and the possibilities of reacting to them. Education for security should include teaching in the general education system, higher education, improving the qualifications and skills of services responsible for maintaining security as well as employees of government and self-government administration.

The system of protection of national heritage is an important element of Polish identity, therefore its protection and security is one of the tasks of the state, which will be implemented by: [ensuring universal and equal access to culture, activization of social capital, and strengthening patriotic attitude, as well as active and conscious citizenship][28]. The promotion of area related to our tradition and heritage is also of particular importance.

The role of the media in the national security system – mass media were and will be the basic tool for transmitting information, both daily and of importance to the security of the state and citizens. In the situation of threats to national security or the outbreak of war, media cooperation with state institutions is extremely important. As part of this cooperation, the media are obliged to provide information about: the scale of threats, behaviour of the society in emergency situations, the possibility of obtaining assistance, and raising public awareness of the identification of threats and effective response to them.



Rys. 1 Opracowanie na podstawie Strategii Bezpieczeństwa narodowego 2014 i Białej Księgi Bezpieczeństwa RP z 2013 r.

All entities forming a social security subsystem fulfil a very important role in its creation, cooperation between them is extremely crucial since they often complement each other, without the assistance, the other entity is unable to fulfil its mission in creating social security. The maintenance and development of social security has an impact on the overall functioning of national security, because it is its element, which is why its provision is one of the elements of state policy.

[24] A.Skrabacz, *Social security, Theoretical and practical basics,* Publishing house Elipsa, Warsaw 2012 , p.38.
[25] J.Gierszewski, *Organization of the national security system,* Pub. Difin, Warsaw 2013, p. 77.
[26] See the Act of April 24, 2003 on public benefit and voluntary work, Journal of Laws of 2018, item 450, 650, 723, 1365.

[27] See the Resolution no. 104 of the Council of Ministers of June 18, 2013 regarding the adoption of the Human Capital Development Strategy 2020, M.P. 2013 item 640.

[28] *National Security Strategy of the Republic of Poland,* Warsaw 2014, p.38.

3. Conditions of social security

In the current situation of our country, many factors affect the social security, the main being: unemployment and related labour migration, poverty, as well as social exclusion causing them. The task of the state is to ensure social security, because its low level may lead to the development of pathology, lack of trust in the state and its institutions.

In order to approximate the phenomenon of unemployment, it is necessary to determine who the unemployed is, it is more reasonable to use the definition contained in the Act of April 20, 2004 on the promotion of employment and labour market institutions, where: [the unemployed is a person that is not employed and does not perform other gainful employment, able and willing to take full-time employment in a given profession or in a given service or other paid work][29], from this definition it can be inferred what unemployment itself is, it is a situation in which the state cannot provide work for people with the ability to take it.

Unemployment constitutes a negative determinant of social security because its effects have an impact on the individual, his family, society, as well as the state economy. The authors: J. Auleytner, K. Głąbicka divide them into[30]:

- individual effects of unemployment;
- social effects of unemployment;
- economic and financial effects.

Individual effects of unemployment are felt directly by the unemployed and indirectly its consequences also affect his family. The symptoms of unemployment depend on its duration, the longer it lasts the deeper its effects are. At first, the unemployed person may lose faith in own abilities, have a problem with too much free time, and assess himself worse and worse. Over time, the situation deteriorates, it is related to financial difficulties causing a reduction in the standard of living, the lack of ability to meet own basic needs and those of his family, uncertainty about the future, consequently all this leads to states of depression, withdrawal of the citizen from public and cultural life of the country, which is followed by social isolation.

Social consequences of unemployment are related to the costs which apply to the increased social benefits, public dissatisfaction, fear of losing one's own job, an increase in the phenomena of social pathology, crime.

The economic and financial consequences concern the state, which incurs costs related to:

-expenditure on benefits and training for the unemployed;
-counteracting unemployment;
-employment of officials in labour offices.

In addition to the costs, state revenues are reduced due to the lack of tax and social insurance contributions.

In the case of young, educated people who know foreign languages, wanting to ensure a good start in life, or wanting to improve the material situation of the family, unemployment often affects the decision of labour migration. Due to the closeness, easier procedures of taking up work, the European Union member states have been the main direction of labour migration of the Poles for years. According to data of the Central Statistical Office, since 2009, the phenomenon of growth of persons emigrating abroad in order to make a living is visible[31]. The intensification of this phenomenon on a larger scale causes the intellectual and economic impoverishment of the nation.

When analysing the unemployment rates in Poland from 2014 to 2017, its decline can be observed[32], however despite the improvement, this phenomenon should not be underestimated, because, as mentioned above, it affects the citizen, society and the state.

Poverty is closely related to the unemployment discussed above, it is its inevitable consequence. In literature, one can find different definitions of poverty, generally defining it as a lack of necessary resources, insufficient for human life, it is a state of scarcity, lack of possibility to satisfy basic needs of a person and his family. A more detailed definition is given by J.Gierszewski [poverty is a state of various kinds of lack of needs in such dimensions that a man cannot overcome them himself. The poor are characterized by cumulative deprivation, which causes their distinct separation and marginal position in relation to the reference groups through the level of material position][33].

The scale and importance of the phenomenon is emphasized by A. Skrabacz stating: [… poverty is considered today as one of the most important and most dangerous social phenomena, affecting both poor and rich states. Poverty results in significant social consequences, ranging from the lack of demand for goods, through difficulties in obtaining education, maintaining good health, to worsening of pathological phenomena, such as: crime, drug abuse, homelessness][34], this is undoubtedly a phenomenon which, like unemployment, will affect the citizen, his relatives and the state.

It seems quite difficult to determine the determinants of poverty, in the opinion of the Poles surveyed by the Centre for Public Opinion Survey, the main criterion includes income and more precisely its amount[35], the Central Statistical Office CSO measures poverty using data from household budgets taking into account three boundaries: extreme poverty (minimum of the existence, threat for biological human development), relative poverty (the level of consumption is lower than the level of the majority of people in Poland) and statutory poverty (people who, according to the regulations, are granted cash benefits from social assistance).

In the case of extreme poverty, since 2015 an annual decline was recorded, relative poverty is also a declining level and statutory poverty, which has been falling since 2013[36]. In the

[29] The Act of April 20, 2004 on the promotion of employment and labour market institutions, Journal of Laws of 2018, item 1265, art. 2, point 1.

[30] See J. Auleytner, K. Głąbicka, *Social policy – between protection and subsidiarity*, Higher Pedagogical School in Warsaw, Warsaw 2000, p. 17-18.

[31] See www.stat.gov.pl/cps/rde/xbcr/gus/LU_infor_o_rozm_i_kierunk_emigra_z_polski_w_latach_2004_2011.pdf (access 27.10.2018) and www.stat.gov.pl/obszary-tematyczne/ludnosc/migracje-zagraniczne-ludnosci/informacja-o-rozmiarach-i-kierunkach-emigracji-z-polski-w-latach-20042016,2,10.html?pdf=1 (access 27.10.2018).

[32] At the end of December 2013, unemployment in Poland amounted to 13.4 %, in December 2014 to 11.4 % and in December 2017 to 6.6 %, source: https://stat.gov.pl/obszary-tematyczne/rynek-pracy/bezrobocie-rejestrowane/stopa-bezrobocia-rejestrowanego-w-latach-1990-2018,4,1.html (access 27.10..2018).

[33] J. Gierszewski, *Organization of the social security system*, Pub. Difin, Warsaw 2013, p. 148.

[34] A.Skrabacz, *Social security, Theoretical and practical basics*, Publishing house Elipsa, Warsaw 2012 , p.128.

[35] The largest number of respondents (24 %) determined that the income of PLN 1000 net per person in the family means poverty, 14% found that it is PLN 500, 9% claimed that PLN 800, 7% listed the amount of PLN 1500, while others provided different amounts. Source: Announcement from the CBOS research, *Social perception of the poverty problem*, no. 83/2017, Warsaw 2017; https://cbos.pl/SPISKOM.POL/2017/K_083_17.PDF (access 27.10.2018)

[36] Extreme poverty: 2008-2014 is an increase (from 5.6 to 7.4%), from 2015 the decrease in 2016 reaching 4.9%, and in 2017 – 4.3 %; Relative poverty: 2008 – 17.6% drop, decrease to 13.9 in 2016 and 13.4% in 2017; Statutory poverty: 2008 is 10.6 % and a decrease to 2011, in 2012-2013 an increase to 12.8 % in 2013, the next years a decrease to 10.7 % in 2017. Source: www.stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5487/

literature on the problem of poverty, two types of poverty are mentioned most often: absolute, which means [the state of living conditions that prevent or significantly impede the implementation of basic life functions][37] and relative [determined by reference to a specific life situation of the individual and family in comparison with the level available to others][38], so it depends on who we compare with whom.

In order to prevent the phenomenon of poverty and improve the situation regarding this issue in Poland, it is necessary to:

-increase the education opportunities for the poorest families;

-support the activity of people affected by poverty through their participation in social life;

-implement tasks within the social assistance system through cash benefits (permanent, periodic, purposeful, special benefits, loans and others), other benefits (e.g. social work, material assistance, specialist counselling and others).

Social exclusion is often the result of the above-mentioned unemployment and poverty, but it can also be caused by other factors, old age, place of residence (rural areas), lack of education or addition to alcohol, drugs, exclusions cause lack of full participation in social life, activities of a given community. The authors J. Czapiński and T. Panek distinguish three categories of exclusion[39]:

- structural (defined by the place of residence – village, low education and income per person below the poverty line);

- physical (related to the old age or disability);

- normative (created through alcohol abuse, drug use, conflicts with the law, being a victim of discrimination on the grounds of nationality, appearance, beliefs or other reasons).

In Poland, the main cause of social exclusion include[40]: poverty, drug addiction, mental illness, alcohol addiction, unemployment as well as homosexuality, bisexuality or transsexuality.

Summary

The problem of human security is a current and important issue, and a sense of security is one of the basic human rights, it is a state consistent with the life of a human being as a man. The Convention for the Protection of Human Rights and Fundamental Freedoms and the Constitution of the Republic of Poland guarantee them to the citizens. The security of individuals and social groups is one of the essential and fundamental values of every society and state structures. It is the satisfaction of one of the fundamental human needs, i.e. a sense of security that occurs immediately after basic needs, such as: satisfying hunger, housing, procreation, but at the same time is more important than the need for love or the desire to belong to a group. Social security can be guaranteed by friendly interpersonal relations, a sense of value and satisfaction with achieving goals and life plans of a person. The sense of security occupies a special rank in the life of every man, family, local community, as well as entire nations, because it concerns such basic values as life, health, individual development and national heritage.

The goal of the activities of the state should be to ensure social security, which is an integral part of national security. In the process of caring for social and national security, cooperation and collaboration of all entities and their resources is extremely important, because only a joint effort of the state, organization, citizens can bring the desired effect which is a guarantee of security. However, it should be kept in mind to treat security as a process that is subject to constant changes under the influence of variable factors of the surrounding reality.

Bibliography

Auleytner J., Głąbicka K., *Social policy – between protection and subsidiarity*, Higher Pedagogical School in Warsaw, Warsaw 2000

Czapiński J., Panek T., (ed), *Social diagnosis. The conditions and quality of life of the Poles*, Social Monitoring Council, Warsaw 2007

Gierszewski J., *Organization of the social security system*, Pub. Difin, Warsaw 2013

Kitler W., *National security of the Republic of Poland, Basic categories, conditions, system*, AON, Warsaw 2011

Koziej S., *National Security Strategy (of the State)*, in: *Fundamentals of security of the contemporary state (entity), implications*: ed. J. Pawłowski, AON, Warsaw 2015

Leszczyński M., *Security in the local dimension*, Difin, Warsaw 2013

Maslow A. *Motivation and personality*, PWN, Warsaw 2016

Pawłowski J., (ed), *Dictionary of terms in the field of national security*, AON, Warsaw 2009

Pawłowski J., Marczak J., Gąsiorek K., *The concept, character and determinants of national security (state)*, in: *Fundamentals of security of the contemporary state (entity), implications*, ed. J. Pawłowski, AON Warsaw 2015

Skrabacz A., *Social security, Theoretical and practical basics*, Publishing House Elipsa, Warsaw 2012

Skrabacz A., S Sulowski, *Social security. Concepts, conditions, challenges*. Elipsa, Warsaw 2012

Stańczyk J., *Contemporary understanding of security*, ,ISP PAN, Warsaw 1996

The white book of national security of the Republic of Poland, BBN, Warsaw 2014

National Security Strategy of the Republic of Poland, Warsaw 2014

The Act of June 9, 2006 on the Military Counterintelligence Service and the Military Intelligence Service, Journal of Laws of 2017, item 1978, 2405, of 2018, item 650, 1544, 1669.

The Act of April 20, 2004 on the promotion of employment and labour market institutions, Journal of Laws of 2018, item 1265, art. 2, point 1.

The Act of November 21, 1967 on the general obligation to defend the Republic of Poland, Journal of Laws of 2018, item 1459, 1669, art. 6, par. 1 and art. 4a, par. 1.

Resolution no. 104 of the Council of Ministers of June 18, 2013 regarding the adoption of the Human Capital Development Strategy 2020, M.P. 2013 item 640.

www.stat.gov.pl/cps/rde/xbcr/gus/LU_infor_o_rozm_i_kierunk_emigra_z_polski_w_latach_2004_2011.pdf
www.stat.gov.pl/obszary-tematyczne/ludnosc/migracje-zagraniczne-ludnosci/informacja-o-rozmiarach-i-kierunkach-emigracji-z-polski-w-latach-20042016,2,10.html?pdf=1
www.stat.gov.pl/obszary-tematyczne/rynek-pracy/bezrobocie-rejestrowane/stopa-bezrobocia-rejestrowanego-w-latach-1990-2018,4,1.html
www.sjp.pwn.pl/slowniki/bezpiecze%C5%84stwo.html
www.cbos.pl/SPISKOM.POL/2017/K_083_17.PDF
www.stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5487/14/5/1/zasieg_ubostwa_ekonomicznego_w_polsce_w_2017.pdf
www.diagnoza.com/pliki/raporty/Diagnoza_raport_2007.pdf
www.stat.gov.pl/...zycia/...zycia.../jakosc-zycia-w-polsce-w-2015-roku-wyniki-badan

14/5/1/zasieg_ubostwa_ekonomicznego_w_polsce_w_2017.pdf (access 28.10.2018)

[37] A.Skrabacz, *Social security, Theoretical and practical basics*, Publishing house Elipsa, Warsaw 2012 , p.127.

[38] J. Gierszewski, *Organization of the social security system*, Pub. Difin, Warsaw 2013, p. 151.

[39] See J. Czapiński, T. Panek (ed.), *Social diagnosis. Conditions and quality of life of the Poles*, The Social Monitoring Council, Warsaw 2007, p. 316, http://www.diagnoza.com/pliki/raporty/Diagnoza_raport_2007.pdf (access 27.10.2018).

[40] See CSO, *Quality of life in Poland in 2015. Results of the social cohesion survey*, Warsaw 2017; www.stat.gov.pl/...zycia/...zycia.../jakosc-zycia-w-polsce-w-2015-roku-wyniki-badan (access 27.10.2018)

THE EXAMINATION OF NEW-TYPE SECURITY CHALLANGES CONCERNING THE EUROPEAN UNION WITH REGARD TO COMMUNITY DIRECTIVES OF STRICTER GUN CONTROL

Assistant Lecturer. Dr. Szabó Cs. PhD.[1]
National University Of Public Service, Faculty of Law Enforcement. Department of Private Security and Municipal Policing [1]
szabo.csaba@uni-nke.hu

Abstract: *The degree of need for security and the means of creating it change from era to era. Genera-tions of different eras formulate their security aspiration from different perspectives, but the protection of human life has always been brought to the forefront. This aspiration finds its expression at the individual and social levels. The individual, during the process of his so-cialisation, expresses clear expectations that the state shall satisfy his need for security as a basic demand. This is a common social objective, established between the citizen of the state and the state to make sure that security, order, and liberty be fulfilled. In recent years, the need for both individual and society security has undergone radical changes. In the EU member states and in its decision-making organisations, the strengthening of citizens' security is a key objective. New security challenges such as international terrorism, proliferation of arms of mass destruction, unstable states, global environmental problems, the emergence and intensification of international irregular migration, have resulted in the extension of the concept of security. Following sudden and unexpected changes in the security components affecting the entire territory of the European Union concerns have arisen on the part of both individuals and societies. Increasing security challenges and risks today require more and more intensive state intervention and effort to maintain public safety and public order. Terrorist and criminal acts committed in the European Union over the past period enhanced the need for such a law enforcement system, which so far has been practically un-known, existing mostly in theoretical models. The decision-making bodies of governments facing new security challenges have applied the introduction of available legal, economic and law enforcement regulations to address emerging emergency situations. Several Mem-ber States of the European Union have adopted a number of measures and legal regulations that have not even been brought to the attention of decision-makers in recent years. These changes, which have been supported by a number of research projects, can also be seen as reform efforts that should have already been enforced by lawmakers in an earlier period, as relevant available data were available on the strengthening of the European terrorist threat and the transformation of its development dynamics. The research described in this paper, through reviewing issues of the weapons policy domain of the European Union, analyses the questions formulated by the European Council in relation to such new security challenges as the suppression of illegal acquisition of fire-arms, the increasing of security risks relating to the transport, import and export of civilian firearms in the European Union, the improvement of traceability of legally held firearms (hunting, sports, self-defense) and ensuring that deactivated firearms are rendered inopera-ble. Giving the professional analysis of the background of the directive on stricter firearms possession foreseen by the European Commission in 2015, the study seeks to highlight the need for EU action to tackle the new security challenges in the weapons possession policy*.

Keywords: WEAPONS POLICY, ARMS CONTROL, SECURITY POLICY, WEAPONS ACT, NEW SECURITY CHALLENGES, POLICE.

1. Introduction

On 13 November 2015, terrorist acts were carried out at several locations in Paris, where in several waves around two hundred people were killed by concerted attacks. In order to ad-dress the new security challenges (with focus on the illicit acquisition and trade of firearms) affecting the European Union, the European Commission has launched the negotiating phase on the preliminary control of legal norms of the draft envisaging stricter firearms regulation. Following terrorist acts, the Member States of the European Union have decided to intro-duce minimum rules to prevent the illegal acquisition of firearms. The purpose of the measure was to tighten up the legal framework for restricting the acquisition of firearms used in terrorist acts. Subsequently, the European Commission presented its professional concepts and guidelines for tightening the existing Firearms Directive (in force since 1991) to be the basis of a security protocol that shall be elaborated in future (where armament interests will be a secondary priority). According to the document, the European Commission, in the whole spectrum of its planning and decision-making system, has revised the existing weapons categories and reclassified them according to its own concepts. The result of this re-structuring was that civilian semi-automatic firearms similar in their operation system to fully automatic military weapons were intended to be reclassified from the 'B' weapons category (subject to authorisation) into the 'A' weapons category (banned). The changes in-tended to be introduced gave rise to a great indignation in the European Union's Member States having traditions with some civilian firearms. Many criticisms have been made in respect of the creation of rules for the introduction of measures to re-regulate civilian pos-session of firearms. The European Commission reasoned the need for stricter firearms regulation to address the new types of security challenges. The firearms concepts formulated in the draft directive deal with more stringent controls on hunting clubs and shooting clubs, the reclassification of firearms categories, the ban on semi-automatic weapons, the development of a technical standard system for deactivated weapons, and the transformation of the systems of rules on museum weapons.

The paper intends to carry out a background analysis (and also a legal analysis) in the context of the stricter firearms control strategy of the European Commission, seeking the answer to whether the recent arms control proposals provide for the European Union appropriate responding measures to the new security challenges posed by terrorist acts.

In the course of my investigations, I sought answers for three issues:

- Is it justified on the part of the European Commission to tighten up the existing firearms control principles in order to address the new security challenges facing the European Un-ion?

- To what extent does stricter firearms regulation affecting the Member States of the Euro-pean Union influences the development of professional areas of sport hunting and shooting sports and the market situation of the European firearms manufacturers and distributors sector?

- Are the future revision of the European Commission's Firearms Directive and the formula-tion of proposals for its amending justified and necessary?

To answer the questions I used the method of literature research and analysis of legal regulations.

2. Presentation of the background

The European Union's Member States are primarily themselves responsible for maintaining and effectively securing the internal order and public security of the Member States, but the new cross-border security challenges require coordination of independent capacities to act of individual Member States and the efficient use of the EU funds to build trust and cooperation, and to facilitate information exchange and joint action. In order to strengthen cooperation on security issues in the European Union, Jean-Claude Juncker, the president of the European Commission, in his statement explained that according to the policy guidelines the European Union's security program should be addressed as a matter of priority, in connection with which the European Commission (in line with the 2015 Commission work programme) is committed to restrictions relating to safe transportation of firearms in order to enhance the implementation of the European Union's security policy concept. On 28 April 2015, the European Commission set out a European Agenda on Security for the period 2015-2020 to support cooperation between Member States and to identify and address security threats. In the Agenda on Security, the European Commission has defined tackling of security challenges such as fight against terrorism, organised crime and cybercrime. The Europe-an Commission has laid down the concrete tools and measures that can be taken by the Member States in their mutual work to improve public order and public security in order to address the three most serious threats more effectively. In the 2016 schedule and work programme, the European Commission envisaged to revise existing firearms legislation in 2016 in order to improve information sharing, strengthen traceability, standardise firearms mark-ing and establish common standards for the firearms deactivation. In order to prevent terrorist attacks and persistent threats affecting the Member States of the European Union, the European Commission has taken the decision to significantly speed up work processes in connection with civilian firearms. The European Commission has taken significant steps to implement the elements of the Agenda. Measures and initiatives taken to strengthen security complement ongoing work to combat the illegal trafficking of firearms, including, including in particular the operational action plan between the European Union and Western Balkans, and the joint investigations and the police cooperation, which have been in place since 2013.

3. Amendments to the rules on firearms possession adopted by the European Commission

The European Commission has set up a package of proposals to amend a firearms directive to tighten the acquisition and possession of firearms by private individuals and the transfer of firearms to another European Union Member State.

The planned revision includes the following:

- Adopting stricter (national) legal regulations prohibiting civilian possession of semi-automatic firearms. The measure states that semi-automatic firearms may not be in the possession of private persons under any circumstances, even if the deactivation of those firearms has previously been implemented in practice (in officially regulated way);

- Creation of stricter rules on the online sale of firearms to prevent the purchase of firearms, firearm pieces and ammunition on the Internet;

- Uniform regulation at Community level for the designation of firearms and the more effective traceability of weapons;

- More effective coordination and exchange of information between Member States. This productive contact and information system may provide assistance in cases when an authorisation issued by a national authority for the possession of a firearm is not recognised by another Member State's authority as a valid authorisation. Problems arising from such situations can be eliminated by compulsorily linking Member States' official databases of weapons;

- Establishing common minimum criteria for specific weapons (e.g. signalling and starter pistols) so that they cannot be converted into fully functional firearms;

- Determination of stricter requirements for the dissemination and sale of deactivated firearms;

- Determination of stricter requirements for weapon collectors in order to reduce the risks of selling to potential offenders.

During the review, the European Commission has envisaged additional further restrictions on the use and circulation of deactivated firearms. The amendment (taking into account the methods of perpetration of terrorist acts committed in the past) is primarily aimed to additionally restrict the civilian possession of firearms no longer authorising to possess, as is currently allowed, any of the most dangerous firearms falling under category 'A' – even if they have been deactivated. The European Commission delegates the implementation of the regulation to the national authority and also obliges the Member States to implement the destruction of illegally held weapons using all available forces and tools. The European Commission has identified collectors of weapons as a possible source of traffic of firearms, as persons ensuring the acquisition of firearms. According to the draft, firearms collectors should still have the possibility to acquire firearms, but under the same authorisation and declaration requirements as private persons.

In order to improve the effective traceability of firearms, the European Commission has envisaged introducing stricter rules on the marking of firearms to avoid markings from being easily erased or changed (e.g., as opposed to the markings on the label), and therefore extending the obligations in relation to imported firearms and clarifying on which elements new markings shall be placed. A new regulatory element has been included in the draft saying that Member States will have to keep records of firearms for an indefinite period un-til the destruction of the firearm and not only for 20 years as is currently the case. In terms of tracing firearms, the European Economic and Social Committee has been seeking to sub-mit a proposal for a directive of the European Parliament and of the Council amending the Council Directive 91/477/EEC on control of the acquisition and possession of weapons. In its working document on the single market, production and consumption, the Committee has formulated the objective of the Directive to ensure the security of citizens and to promote the functioning of the internal market by laying down rules for all stages of the life cycle of the firearm, ranging from production to destruction.

4. Revision of the European Commission's Firearms Directive

The first part of the study presents and analyses the background of Directive 91/477 adopted by the European Commission on 18 November 2015, which contains proposed amendments to the control of the acquisition and possession of firearms. In this chapter, the solution structures are outlined in connection with the new security dilemmas justifying the tightening of the rules on firearms by the European Commission and affecting the European Union, which we are seeking to determine using a cooperative security model that operates with a complex toolbox.

- normativism: the norms adopted by the European Commission regarding the tighten-ing of the rules on firearms (taking into account the value content) should be subjected to a critical examination of their compatibility with the interests of Member States, market actors (arms manufacturers, distributors, professional interest organisations) and arms holders;

- suitability: the legislative mechanism of the European Commission should take into account both the security policy

challenges affecting the Member States of the European Union and the expectations and needs formulated in connection with the strengthening of people's confidence. In this context, the European Union's security policy concept needs to outline such solution structures in connection with new security challenges and risks, as mass irregular migration, terrorist acts committed using asymmetrical methods and special tools in developed countries, issues of necessity of militarisation of law enforcement agencies, the enhancement of self-defenses in specific areas of the private security sector, the protection of infrastructures of high priority for supplying the population, issues of the security of places of public entertainment, or the addressing of challenges connected with firearms;

- complexity and comprehensive approach: new security challenges affecting the European Union require the use of complex systems of tools, including public, civilian and law enforcement solutions;

- multi-level approach: the complex system of secure stability of the European Union is shaped by state and non-state actors. Following the identification of new complex security challenges, it becomes indispensable and inevitable (following the logic of the multi-level approach model) that the strategy to be followed takes into account the interests of state and non-state actors associated with the identified security risk. Looking at this issue from another perspective: In order to address the new security challenges, the European Commission as a decision-making body defines in a coherent decision-making framework the interests along which a multi-level approach can be developed for efficiency, thereby reducing the injury to the interests of non-state (professional) actors;

- multilateralism: against the new security challenges facing the European Union, it is only possible to act effectively through the ongoing, intensive and effective multilateral cooperation between state and non-state actors.

The Firearms Directive 91/477 of the European Commission has highlighted the legislative issue caused by the absolute absence of professional coordination, as well as impact assessments. Making the necessary impact assessments, those environmental, social, governmental, security and economic impacts may become identifiable that can provide a strategic overview of who may be involved in the legislative process. After having analysed the security problems identified based on the impact assessment results, the European Com-mission provides for the policy objectives and the decision-making system and then, through examining the possible effects of the solution structures, defines a complex strategic action plan to address the security challenges effectively and quickly.

4. Conclusion and Findings

The European Commission's package of measures to tighten firearms control also includes an implementing regulation laying down common minimum standards for the deactivation of firearms, which make re-activation much more difficult in case of deactivated firearms. The Firearms Directive stipulates that properly converted deactivated firearms are no longer considered firearms but pieces of metal that can freely move within the European Union's internal market without a firearm license. However, the experiences and conclusions of recent terrorist acts show that deactivated firearms may be illegally re-activated, either by using home-made firearm pieces or by using firearm pieces available through the Internet. These factors cover complex issues that require complex responses to identify and solve the problems. It is a fact that there is no single legal source with regard to the deactivation of firearms in the European Union, and this deficiency significantly increases the level of security risks. In order to address this problem, the European Commission has prepared a proposal package that sets out rigorous and harmonised criteria how Member States shall include in their National Firearms Acts the deactivation criteria for firearms to become unfit for use as a firearm. The outlined measure is complemented by the prohibition of the pos-session of firearms of category 'A', which also imposes obligations on firearms holders in cases where firearms of category 'A' were deactivated. The European Commission's Implementing Regulation is based on the criteria for firearms deactivation developed by the Permanent International Commission for the Proof of Small Arms (the CIP)

The European Commission has examined the role of the Internet in the illicit arms trafficking. The analysis of the Firearms Directive and preparatory studies investigating the policy field has shown that the firearms manufacturers and distributors are increasingly using the Internet as a firearm sales channel. This information was backed up by police reports analysing recent terrorist attacks in the European Union. In some cases, firearms used to commit terrorist offenses were assembled from firearm parts legally purchased via the Internet. The European Commission proposes to prohibit the sale of firearms, firearm components and ammunition via teleshopping (especially via the Internet), and the proposal pro-vides a possibility to facilitate this for licensed traders, distributors and brokers.

The overall finding and conclusion of the research is that illicit trafficking in fire-arms is a serious problem in itself and poses a security risk that significantly contributes to social insecurity caused by the perpetration of violent or compulsive offenses and other crimes (such as drug smuggling, trafficking in human beings, as well as terrorist attacks). These security risks pose a significant threat to the security of the EU Member States and their citizens. In the European Union, the nature and scale of illicit firearm trafficking are difficult to assess due to the hidden nature of the problem. Within the framework of cross-border cooperation, the Member States and law enforcement agencies of the European Union take joint actions in combating illicit firearm trafficking in a number of cases. We can also identify significant issues in dealing with cross-border illicit trade in illegal firearms.

Currently there are significant differences in the legal frameworks of the EU Member States in relation to the fight against illicit trade in firearms. This concerns the definition of offenses, the type and extent of sanctions to be applied to legal and natural persons, the aggravating or mitigating circumstances and the degree of neglect and intent. The international and EU legal frameworks affecting the illicit trafficking in firearms are widely defined and give the signatories considerable discretion as regards the implementation of key provisions. The adoption, at the European Union level, of minimum rules against illicit firearm trafficking would be beneficial for the police and the investigative authorities of the Member States allowing to reduce the legal uncertainty generated by differences in national legal systems, which would facilitate prosecution and greatly reduce the possibilities of criminals to use loopholes.

Researches show that the differences have an impact on the effectiveness of cross-border police and judicial cooperation. The fight against illicit firearms trafficking requires the Member States to adopt a uniform and effective EU-wide legislation. Nevertheless, it is essential for the European Union, the Member States and the competent authorities to initiate cooperation and dialogue, at the national level and the EU level on policy issues, with financial and economic analysts, firearms manufacturers and traders, further with hunting clubs, sporting associations and professional chambers to reduce illicit firearm trade and to combat illicit online weapons trafficking.

A number of stakeholders (and Members of the European Parliament) reacted negatively to the ban on some semi-automatic firearms proposed in the package of measures by the European Commission, which measures are deemed to be an unnecessary and burden-some limitation by hunter and sports shooter societies objecting the lack of data from preliminary impact studies that could support expected legal, economic and professional implications. The conclusion can be drawn that the amendment to

the Firearms Directive is necessary to address terrorist acts committed with firearms and the new security challenge affecting the European Union. It should be noted that the regulation may adversely affect the conditions of competition both within the internal market and the international market in a number of professional and economic fields closely linked to the legal possession of fire-arms (pushing back the online trade; weapons-related cultural heritage; historical weapon collections; research in connection with firearms; paid hunting).

Literature

[1] EIGEL, C.: Internal Security in an Open Market: The European Union Addresses the Need for Community Gun Control. In: *Boston College International and Comparative Law Review*. 1995, No. 18. p. 25-36.

[2] OZANNE J.-SMITH, K. A, NEWSTEAD J. STATHAKIS, V.Z., CLAPPERTON, A: Firearm related deaths: the impact of regulatory reform. In: *Injury Prevention.* 2004, No. 10. p. 15-33.

[3] P. J. COOK, W. CUKIER, K. KRAUSE: The illicit firearms trade in North America. In: *Criminology and Criminal Justice.* 2009, No. 9. p. 75-77.

[4] L. TRÓCSÁNYI, B. SCHANDA: Introduction to constitutional law; The Fundamental Law and Hungary's constitutional institutions. Methods of constitutional law. *HVG-ORAC Lap- és Könyvkiadó Kft.* Budapest, 2014. p. 25-29.

[5] SPAPENS, A.C.M.: Trafficking in Illicit Firearms for Criminal Purposes within the European Union, European Journal of Crime. In: *Criminal Law and Criminal Justice*. 2007, No. 15. p. 33-35.

[6] The Fundamental Law of Hungary. In: *Magyar Közlöny (Hungarian Official Gazette).* 2011, No. 43.

[7] WINTEMUTE G.: Broadening denial criteria for the purchase and possession of firearms: need, feasibility, and eff ectiveness. In: *Webster D, Vernick J. (editors): Reducing gun violence in America. Johns Hopkins University Press, Baltimore*. 2013. p. 5-7.

[8] Cs. SZABÓ: Examination About the Law Enforcement Strategies which are Influence the Criminal Behaviour. In: *Academic And Applied Research In Military And Public Management Science.* (3) 2016. p. 263-269.

ORGANIZATION AND CONDUCT OF MILITARY MANEUVERS "EAST 2018" IN THE RUSSIAN FEDERATION

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

Abstract: *From 11 to 17 September, the military maneuvers "East 2018" took place on the territory of the Central and Far East Military Districts of the Russian Federation with more than 300,000 participants, more than 10,000 combat units and 1,000 airplanes. Representatives of the Armed Forces of China and Mongolia took part in the maneuvers. In this exercise, there was a military controversy between two contingent opponents in order to play out different options for defense forces' behavior.*

KEYWORDS: *MILITARY MANEUVERS, RUSSIAN FEDERATION, PARTICIPANTS, DIFFERENT OPTIONS, COMBAT, AIRPLANE*

1. Introduction

In Russia, from 11 to 17 September 2018, the largest military maneuvers "East-2018" took place in the last 40 years. They continued one week until September 17 and took place in two stages. The armies of the Central and Eastern Military Counties of the Russian Federation worked in five Combat Training and Combat Training Centers, four Air Force bases and mixed naval and air training and covered the waters of the North Sea Ocean, adjacent to the Asian part of Russia, Beringovo, Ohoto and Japanese seas with Avacha and Cronoshkin bays.

The Department of Defense of the Russian Federation has timely published information on the start of the maneuvers and invited military observers from 59 countries, including NATO members, even though the maneuvers took place in the Asian part of Russia and were thousands of kilometers from Europe [1].

As provided by the established plans, the troops of the Central Military District Army and 3 Armies of the Far East Military District were some sort of enemy on the battlefield with the so-called "Center" and "East". In the scenarios besides the Land Forces, participation took different types of ships and submarines from the North and Pacific fleets, parts of all types of Air Force and Air Force troops and Airborne troops and military aviation. The maneuvers gained international status, as at some stages of the event took part also military from the People's Liberation Army of China (NEAK) and the Mongolian Armed Forces (BCM).

It is bold to say that the maneuvers were one of the largest in this century in the world - more than 300,000 soldiers, sergeants and officers, more than 1,000 airplanes and other flying equipment, about 80 warships based in various military bases from Asia and Europe and approximately 36,000 armored vehicles: tanks, BTR, MTPL and BMP [2].

Russian Defense Minister Army General Sergei Shoigu confirmed to the media that East-2018 was the largest preparation and conduct event on the territory of the Russian Federation since the time of the West-81 teachings. This exercise was conducted on the territory of the then Soviet Union with the participation of troops from the former Warsaw Pact countries.

2.1. Main tasks of the maneuvers

"East 2018" has no analogue in territorial scope - polygons and bases located from the Arctic Ocean coast to the Pacific coast and the adjacent islands have been activated. Participating parties have carried out more than 7,000 km of ground-based transits on their disembarkation and vessels sailed more than 4,000 nautical miles. The main thing in this exercise is that maneuvers are carried out on entire armies and other large divisions. According to the General Staff of the Armed Forces of the Russian Federation Army General Valeriy Gerasimov these maneuvers are held in several strategic directions with the participation of 2 military districts and under the direct guidance of the Minister of Defense. While the exercise is conducted with one military district in one strategic direction under the direction of the Chief of Staff. On September 13, one of the most important parts of the maneuvers was also observed by the president and chief commander of the Russian Federation Vladimir Putin at the Zukul Gulf in Zabaykallieto.

One of the main tasks of the maneuvers is the rapid transfer of tens of thousands of combat units and hundreds of thousands of Central Russian soldiers into the Far East and the Pacific Coast. But the main task, according to the Head of the General Staff of the Air Force, is to check the actual state of the combat preparation of the parts, the fighting skills of the different types of troops.

The maneuvers took place in 2 stages. During the first stage for 2 days, the staff of the contingent adversaries carried out personnel planning and preparation, realization and expulsion of the relations between the participants, coordination of the actions of the participants and logistic security of the troops. Over the next 5 days troops performed different types of maneuvers: dealing with massive air strikes, countering wing missiles, defensive, offensive, and crawling actions.

The Pacific Navy ships on the high seas reflected air strikes, destroyed the fleets of the contingent enemy, and countered an opposing landing on the Pacific coast. Different types of airplanes and helicopters from the FF Military and Space Forces carried out missile and bomb attacks on ground and air targets. The Chinese Air Forces also participated in the maneuvers to carry out their own and joint tasks.

The most interesting school battles took place at the Zukol district and, as I mentioned, were monitored by Russian President Vladimir Putin and 87 military observers from 59 countries. There were the defense ministers of the three participating countries - Russia, Mongolia and China - who participated in the maneuvering process. The Joint Military Formations of 3 Armies of the East Military District, China and Mongolia, reflected the attack of 2 armies from the Central Military District. After the completion of the substantial part, ten Sergeants and officers from the three countries were awarded by the President of Russia for maneuvering skills and a large-scale military review and a parade of the Zukol polygon [3].

In addition, they used robots, unmanned airplanes, drones, parachute deserts, forced water barriers, and all in a rapidly changing environment. Real-time automated control systems, which have a combat experience on Syrian territory, were actually shown and used.

Since 1990, there have been no such large-scale military exercises on the territory of the Far East. In 1994, 1996 and 1998 years, joint Russian-American exercises "Maritime Cooperation" were held in the Primor Sea - then Pacific Pacific Navy ships, 7th US Navy and parts of the Marines of both countries were activated.

Since 1994, joint Russian-Japanese teachings have been held on several occasions to help those in distress in marine casualties or disasters. But the number of participants did not exceed 2,000 people.

For the first time in the history of the Russian Federation in August 2003, great strategic exercises were held in the Far East, known as East-03. More than 70,000 military and civilian specialists were involved. Then the teachings were held irregularly, and from 2010 onwards every four years.

Strategic command exercises have been held in recent years once a year, but this year a different form of planned martial training was chosen - maneuvers. Therefore, during the maneuvers, in the opinion of the chief of the General Staff of the Armed Forces of the Russian Federation, there is no sense of futility, but action in an environment close to the real.

2.2. Purpose of military maneuvers

"What is the difference: Strategic exercises are, as a rule, conducted with one military district in a strategic direction under the direction of the Chief of Staff, and maneuvers - on several strategic areas, where several military areas were present, in this case, troops from The Central Military District and the Eastern Military District, the Pacific Navy and the North Navy.

The centerpiece of the action was near the Zukol district and the maneuvers were carried out under the supervision of the Minister of Defense of the Russian Federation , - said Army General Chief of Staff of the Russian Armed Forces General Valery Gerasimov at a briefing for foreign attachés, noting that in such Big teachings are mutually beneficial for staff and troops.

He also said that during the Soviet era in the territory of the Kievan, Belorussian and Baltic military districts and the Baltic Sea, the number of participating soldiers, weapons and military maneuvers "West-81" was similar. But with regard to the spatial scope, the depth of regrouping and the armament involved, the current maneuvers are at a much higher level of organization and conduct.

It is remarkable that not only troops from two military districts, two navy troops, troopers and various troops took part in the current maneuvers, but also the governing bodies and subdivisions of the People's Liberation Army of China and the Mongolian Armed Forces. "On the one hand, it is close to the West-81 maneuvers, as there were international partners from the Warsaw Pact countries, but it has greatly expanded geography, routes and horizons of maneuvers," notes TASS military analyst Viktor Litokwyn. He also noted that in 1981 participation took countries that had signed a mutual assistance treaty in an attack on one of them. And there is no such contractual relationship between Russia, China and Mongolia. they are not allies under the current international treaties [4].

According to the press service of Russian President Dmitry Peskov, China's participation in Russian strategic maneuvers talks about the expansion of the two countries' interaction in different spheres. It is not by accident that the Eastern Economic Forum in Vladivostok, on 10 September, negotiated an increase in economic cooperation between Russia, China, Japan, the DPRK and South Korea and signed billions of dollars. "All of this will lead to an increase in Russian-Chinese military co-operation, better interaction of different dangers, as well as peacekeeping, stability and security in the region," a Chinese Ministry of Defense press release said. "Enhancing the capabilities of the Chinese Armed Forces, as well as gaining invaluable experience of joint actions with Russian armed forces, will help maintain peace, stability and security in the region," said Kuwa Yanwei, the military attache of China at the Moscow Embassy. He emphasizes that maneuvers are not targeted against any particular third party. He also mentions in East-2018 that more than 3,200 soldiers, 900 ground-handling vehicles, 30 aircrafts, and Chinese-backed turrets were involved.

Like any major event, these maneuvers have begun with a series of preparatory events - more than 20 specialized exercises of generic troops that are accompanied by unannounced inspections and command and staff training. This stiffness in joint actions, where more than 36,000 combat units are moving at the same time, is achieved with a lot of work, and through training sessions a good agreement between the different participants is achieved. At the end of the maneuvers, the Minister of Defense thanked all direct participants and their accompanying people and equipment for good actions under conditions close to actual military action.

For about 10 days, Russia managed to transfer and redeploy more than 160,000 troops to the east, along with the necessary equipment, with the transfer of technology beginning as late as August. 21 formations have been thoroughly overhauled, several thousand civilian population from the maneuvering area mobilized. In the Southern and Central Military Areas, subdivisions of territorial troops were formed, which were transferred from military transport aircraft to the Eastern Military District to perform combat training tasks [6].

All this has been done in coordination with the other ministries in order not to interfere with the usual transport corridors and the functioning of all civilian structures.

By way of comparison, I could say that in the East-2014 teachings that took place between Baikal Lake and the Pacific Ocean in the east and the southern border of Russia with China and Mongolia to Chukotka and the Arctic Ocean islands involving about 155,000 people.

Viktor Litokin, a military observer and TASS analyst, believes that "everything is related to the professional training, operative art and skills of commanders and staff, and the ability to quickly transfer large forces and assets over long distances" [5].

More than 80 warehouses for fuel and ammunition and 100 points for food were created for the material provision of maneuvers in the eastern parts of Russia. Deputy Army General Army General Dmitry Bulgakov told journalists that "in the interest of the troops of the Cogol (Buryatia) polygons, additional fuel filling stations were built using modern means of fueling and supplying fuel. more than 100 field cuisines operate in the organization of the servicing of the servicemen". According to his words, about 36,000 military servicemen from the Sub-divisions for Material & Technical Service (MTO) took part in the maneuvers. More than 2,000 specialists in military equipment and industrial workers at the military-industrial complex have taken care of the state of the art.

The very high level of relocation and reconciliation of NACS troops was marked by the military attache of the PRC in Russia, Kuy Yanwei. "I want to sincerely thank the Russian side for the wonderful organization and location of the Zugol polygon in Buryatia, where conditions for exercises and rest were created," he told the media after the maneuvers ended.

The army of the Central Military District is involved in the teaching with all its personnel. "These are unprecedented large-scale maneuvers in which we engage with great pride and where new forms and means of action will be applied, some of which have been tested in a real Syrian setting," said the Commander of the District Lieutenant General Alexander Lapin. These maneuvers are not a mass regrouping and transfer of troops, and they consist of various combat episodes that will be played on different polygons in eastern Siberia.

According to the Chief of Staff of the General Staff of the RF, "the main objective of the" East 2018 "maneuvers is to verify the actual level of training of the military formations, which can be assessed only by the scientists of the respective scale, the maneuvers performed on a bilateral basis a superior form of verification of combat mastery, ground, air and maritime capabilities of troops and armies from both military districts. " According to General Gerasimov, maneuvering features are the two-way format of both action and management at all levels.

During the conduct of the tactical episodes, robotics, unmanned aircraft, parachute air landing, the activities of a specialized mobile brigade and other tactical tasks were widely used.

For the participants, a complex and rapidly changing environment was developed, requiring quick, operational and sometimes non-standard solutions.

The troops carried out tasks of conducting dynamic maneuvering, keeping escorting artillery fire accompanied by air strikes from the military-space troops. Also a counter-attack with forced water partitioning in complicated conditions is also carried out. All of this was united in a general scenario involving action on land, air and water. And one more thing - the solution to these tasks fell on three armies: Russian, Chinese, and Mongolian, who together had to solve the assigned tasks.

After the major part of the maneuvers was completed before the President of Russia, the defense ministers of the three countries and the observers held a parade of the participants in the Tsugol polygon, involving more than 25,000 Russian soldiers, more than

7,000 military and special equipment around 250 planes and helicopters, Chinese and Mongolian soldiers.

Here I have to mention some of the technology that is involved in East 2018 - modernized Iskander missile complexes, upgraded T-72s with improved features, modernized T-80s and new T-90s. In Military Space Force, these are the new Su-34 and Su-35 aircraft, the Mi-28 and Mi-35 thrusters. The Pacific Fleet and the North Navy are ships with modern Calibre rocket systems and others. And also ships of a perfectly new class, which logistically provide the forces in marine and ocean waterways.

Already on August 23, the CBO press service reported that the Su-24 bombers, MiG-31BM interceptors, and Su-25 assault rifles from the Chelyabinsk Oblast, the Perm and Krasnoyarsk regions, were transported to the Eastern Military Operational Airports. A total of 30 aeronautical units. The crews have gone through more than 4,000 km, making several refueling at Novosibirsk and Krasnoyarsk airports.

At the NATO headquarters, maneuvers were considered to prepare Russian military for large-scale global conflicts. On August 28 in Brussels, Dylan White, as a representative of the North Atlantic pact, commented on the conduct of the maneuvers. East-2018 demonstrates focusing on preparing Russia's armed forces for large-scale conflicts, which complements the picture we see from earlier - more decisive Russia, which has significantly increased its military budget and its military presence, "he said. your statement. Here I can mention that the military budget of the Russian Federation is less than 10% of the US military budget, which according to the latest data is more than 15 billion dollars.

The NATO official also stressed that Russia is not obliged to observe the rules of the Organization for Security and Cooperation in Europe (OSCE) in conducting maneuvers regarding information on maneuvers and invitations of foreign observers because the venue is outside the sphere of dissemination of the OSCE , whose boundary is Ural.

On September 6, the Ministry of Defense of the Russian Federation informed the military attachés about the content of the international maneuvers "East 2018". "Despite the fact that maneuvers are taking place several thousand kilometers from Russia's western borders, speculative comments appeared in some media in Western Europe, in which Russian maneuvers are attributed to aggressive focus on NATO and the EU", - finds a deputy Minister of Defense of the Russian Federation General Colonel Alexander Fomin. He drew attention to the military attachés "to the complete and obvious absence both in the preceding and in those maneuvers of the Russian Federation's Armed Forces, though small signs of anti-Nato direction."

3.Conclusions:

1. The "East 2018" maneuvers are the most extensive exercises conducted in Russia in Soviet times, involving more than 300,000 troops, more than 36,000 military units and 1,000 airplanes, all of them generations of troops from the aircraft of the Russian Federation;

2. Maneuvers have gained international status with the involvement of military from China and Mongolia; they have been watched by Russia, China and Mongolia Defense Ministers and 91 military observer from 59 countries;

3. Through these teachings, a Russia emerged, which regained its strength and sought to regulate the conflict points around the world with its diplomacy and determination. It has shown that it should take into account the claimants of world powers;

4. A summit between the leaders of Russia, China, Japan, DPRK, South Korea and others was held immediately before the maneuvers in Vladivostok. the Eastern Economic Forum signed many contracts between the participants and which is also a prerequisite for enhancing economic and military cooperation between the countries of the region.

4.Literature:

1. Долчинков Н. Т. Провеждане на маневрите „Изток 2018“, Ньучна конференция «Актуални проблеми на сигурността» НВУ «Васил Левски» Велико Търново, 2018.

2. Изявление на Министъра на отбраната на Русия, септември 2018;

3. Изявления на Началника на Генералния щаб на ВС на РФ, септември 2018;

4. Изявление на Заместник министъра на отбраната на Русия, септември 2018 ;

5. Информация от пресслужбата на Министерството на отбраната на Русия, септември 2018;

6. Изявления на пресслужбата на Централния военен окръг на Русия, август 2018;

7. Лилов И. Н. , Банабакова В. К. Стоянов С., Роля на интегрираните логистични комуникации за подобряване на логистичното обслужване, 14-та международна конференция "Силата на знанието", Гърция, Солун,2017

TYPES OF EXTRAORDINARY SITUATIONS OF TECHNOLOGY AND ACTIVITIES IN EXCEPTIONAL SITUATIONS WITH THE RELEASE OF RADIOACTIVE SUBSTANCES

Chief Assistant Professor PhD eng. Dolchinkov N. T.[1,2], Acos. Prof. PhD Hvostova M. S.[2], Karaivanova-Dolchinkova B. E.[3]
[1] National Military University „Vasil Levski“, Veliko Tarnovo, Bulgaria,
[2] National Research University "Moscow Power Engineering Institute", Moscow, Russia,
[3]ROU-Veliko Tarnovo
n_dolchinkov@abv.bg

Abstract: *There is an analysis of the major emergencies that occur in our daily lives. Technogenic emergency situations with the release of radioactive substances, separation of dangerous chemical substances and distribution of biological substances are briefly identified. Their impact on humans and the environment is shown and what action is needed to take in the event of an emergency with the release of radioactive substances and radiation.*

KEYWORDS: *EMERGENCIES, RADIOACTIVE SUBSTANCES, DANGEROUS CHEMICAL SUBSTANCES, BIOLOGICAL SUBSTANCES, ACTION, POLLUTION*

1. Introduction

It is accepted that emergency situations (IS) are called conditions that occur as a result of the action of natural disasters (natural IS), accidents and disasters in industrial production or in transport (technogenic IS), ecological catastrophes, diversions or actions of social , political or military nature, characterized by a large or abrupt deviation from the normal course of processes and phenomena in society and resulting in a significant impact on the viability of people, living nature, the economy, society the sphere and the surrounding objects and facilities [6].

Emergency situations of a technogenic nature that are related to man's production can be associated with environmental contamination or without such contamination. Environmental pollution can occur in accidents in industrial plants with the disposal of radioactive, chemical and biologically hazardous substances.

2.1. Types of emergencies of a technogenic nature

Emergencies with the discharge or risk of discharges of radioactive substances may occur in the operation of nuclear power stations, research nuclear reactors, nuclear fuel manufacturing or processing plants, nuclear craft and in the event of the accident of vehicles transporting nuclear reactor components. Such an accident is also possible for enterprises operating for military nuclear programs or for units containing nuclear weapons or their components associated with the nuclear chain reaction. As a result of such accidents and depending on the meteorological phenomena occurring in the area, pollution of the environment or adjacent water areas may be different in degree and scope [4]. The consequences of such accidents are long-term and examples are the Chernobyl disasters (USSR, Ukraine), Fukushima (Japan) and others.

Nuclear weapons pose a huge threat to man and our environment. With its striking factors, it is one of the most deadly weapons ever created by man. Any one of the striking factors, even on their own, could kill thousands of people, break an ecological system or destroy an infrastructure [1].

Other failures of a technogenic character are those related to the discharge or the risk of discharges of hazardous chemical substances. This can happen in chemical plants, enterprises handling dangerous chemical substances or in places where they are stored. Most often this is accompanied by environmental pollution with chemical substances outside the sanitary area of the site, collective poisoning of the population and consequent undesirable environmental pollution, which may lead to the need to carry out degassing of the site and sanitation of the infrastructure and the population.

The main actions for the elimination of the consequences of the use of combatant toxic chemicals are as follows:

- meteorological monitoring (vertical atmospheric stability, atmospheric pressure, wind direction and speed, air temperature and rainfall);

- conducting a chemical reconnaissance to establish the type and concentration of BTWB and the determination of chemical contamination zones;

- evacuation of the population in the opposite direction of the distribution of aerosols from BTWV;

- Separation of sites for special and sanitary treatment in non-contaminated areas [11].

The latter type of accidents of this type are the accidents associated with the disposal or the risk of discarding biologically active substances. These are accidents in which environmental pollution has occurred with hazardous biological substances when discharged from research centers or industries in which bacterial materials are investigated, developed, prepared, processed or transported.

Towards IP without environmental pollution we can account for accidents that are accompanied by blasts, fires, demolition of buildings, destruction of hydrotechnical devices, disturbance of transport system integrity and communications, etc. Due to the fact that this kind of accidents do not emit radioactive, chemically dangerous and biologically dangerous substances, we will not stop at them [7].

2.2. Emergencies with release of radioactive substances

In the current dynamic time, different sources of ionizing radiation and radioactive substances are increasingly being used in every branch of the economy.

On our planet, everything is about the perturbation of various natural and anthropogenic, terrestrial and cosmic sources of ionizing radiation, ie. in particular in the natural and manufac- tured environment. Ionization beams accompany the life of the planet in various areas of concern at all stages of the world. They are an integral part of our existence because, as we all know, the largest source of light and heat in our universe is the sun, and there is a continuous thermonuclear process and we reach the gamma rays that determine the natural radioactive background in the Earth's atmosphere [9].

Science of the construction of the atom has enormous opportunities for development, but also a serious danger to mankind and the environment, as evidenced by the consequences of nuclear experiments and accidents in the United States, England, France, the USSR, Japan and a number of Pacific islands.

The first serious environmental and soil pollution caused by human activity is that in Japan, dated August 6-9, 1945. Above the Japanese cities of Hiroshima and Nagasaki, with no special military necessity, the Americans throw the first atomic bombs in the history of mankind. Previously, a nuclear experience has been made in the Nevada desert, for which there is hardly any information in the public domain. The era of the atomic race began, including the former USSR, France, Britain, etc., and the number of nuclear states today is over 20.

Of course, the pollution of the environment and the soil with radioactive substances is also increasing with the emergence of the

nuclear industry. This was not known at first, and there was a lack of reliable information on the negative impact of radiation on the environment and humans due to insufficient theoretical and field studies and the secrecy of production, was not an opportunity to accurately assess the amount of this pollution, environmental and social damages caused by it.

For a long time, due to lack of information, it was considered to be relatively limited, local and not very dangerous. Later it was found that the various stages of production of uranium fuel (open or closed mines, hydrometallurgical production and uranium concentration, purification, enrichment, etc.) is possible to "enrich" the environment with uranium radionuclides and especially with radon (radon-222). The waste from the major hydrometallurgical plants was first discharged without purification and sufficient additional treatment in the nearest water bodies and, when irrigated, polluted the agricultural areas and the plants grown on them. Only about 50 years ago it is recommended that uranium-contaminated and other radioactive products lead to the cultivation of special crops that can extract and concentrate uranium and purify water, and indirectly protect the soil from radioactive contamination [10].

Of course, the most radioactive contamination of the environment and the soil after the crash in Chernobyl, Ukraine (former Soviet Union) on 26.04.1986, Trimail Island - USA - 1976; Fukushima, Japan - March 2011 and other minor nuclear accidents and accidents.

Local pollution of the environment and soil was also described in Spain in 1966, as a result of a collision in the air of a nuclear-carrying aircraft with a tanker. Radioactive substances from the unexploded nuclear device were scattered over an area of several thousand hectares. 990 tonnes of soil was buried and buried in tombs for radioactive substances in South Carolina, USA. These and a number of other known and unknown cases indicate that in the current armament, despite the high degree of certainty, the risk of nuclear pollution in vast territories actually exists, even in relatively peaceful times and quiet regions.

In the aftermath of the major accidents in Chernobyl and later in Fukushima, more attention has been paid to the need to train specialists whose main task is preventive action to prevent radiation accidents and mitigate the consequences of their eventual occurrence. Increasing influence is being given to the prevention of work with sources of ionizing radiation in more and more sectors of the economy, healthcare and related activities. A special place is also devoted to possible terrorist acts in which sources of ionizing radiation and various radioactive isotopes can also be used. This would affect all inhabitants of a region, continent or larger territory of our planet without being interested in nationality, religion, gender, race or other distinctive features of people.

Nowadays, modern biotechnologies have been developed in a number of countries where, with the help of special algae, uranium is extracted and concentrated in their biomass and thus water is cleansed [12].

Nuclear materials must be transported, stored and processed. Each of these activities leads to an increase in the risk of radioactive contamination of the environment, damage and, respectively, disease to humans, animals and the animal world. Every radiation accident is associated with an accident that leads to the disposal of radioactive products and ionizing radiation in larger dimensions than the predetermined and accepted safety standards.

As a rule, the main causes of the failures in the operation of the nuclear power plant are events related to the passage of safety thresholds across the various components of the reactor core. The cause of an accident may be the formation of critical mass when loading, transporting and storing fuel elements.

In the event of disturbing the controlled neutron reproduction, the reactor core reactor may cause thermal or nuclear explosions. As a result, uncontrolled chain reaction will occur, which in turn will cause an increase in energy released and destruction of the reactor core, accompanied by explosion and release of radioactive substances and an overdose of γ-rays.

The radioactive impact on the staff of the damaged facility and the people who work and live in the infected area may be characterized by a dose of internal and external contamination. Here we have to note that under external influence we understand the direct irradiation of the person from the sources of ionizing radiation, which are outside his body, most often these are sources of neutrons and γ-rays. When the source is in the human body, we have internal irradiation and such sources are concentrated in the most sensitive organs - the thyroid gland, arteries, and so on. It should be noted that radioactive substances can not penetrate the human skin, and they reach the inside of the human body through the absorbed food and beverages and particles of the inhaled air. The radionuclides that accumulate in the body accumulate in one or more bodies called "critical", the accumulation being predetermined by the physical and chemical properties of each radionuclide. The essence of treatment is the use of agents that accelerate the release of radionuclides from the body. There are specific treatments for each radionuclide [8]. Urgent action is needed against two groups of radionuclides (isotopes of iodine and strontium), since early treatment after their entry into the body is most effective.

Radiation is dangerous to humans because ionizing radiation causes the formation of a huge amount of free radicals that the body is unable to neutralize in a timely manner. Free radicals are chemically extremely aggressive, they attack cell membranes and vital molecules (nucleic acids, enzymes, etc.). As a result, both the function and structure of cell membranes and biomolecules are impaired. This initiates the atypical processes at the cellular and molecular level for the healthy organism, which subsequently manifest themselves as different diseases.

2.3. Radiation protection activities

Radiation protection activities can be divided into three stages:
- preparatory (prior to the terrorist attack, with radioactive contamination); The preparatory stage includes selection, testing and, if necessary, calibration of available dosimetry equipment; providing the necessary equipment and individual protective means; establishing a link between the team entering the radioactive contamination area and the relevant command center;

- operational (during radioactive contamination);

- final (measures to eliminate the consequences).

When issuing the hazard alert, the instructions given on the radio, television, special means of communication or in any other pre-established manner (sirens, bells, megaphones, etc.) are observed. It is working to change the legislation and to include in the announcement the mobile operators operating in the country, because through them the information will reach for maximum time to maximum number of users.

It is especially important for people to be pre-prepared by the media not to panic and to trust the reported official information.

The most effective protection is provided by pre-prepared hiding places. With hermetic closure and filtration facilities, hideouts are completely isolated from radioactive contamination. It is a problem at the given stage of development that in Bulgaria, unlike Russia, these hiding places are practically unusable for the most part.

The main precaution is to restrict the access of radioactive materials to the premises. Therefore, in the case of a shortage of hiding places, any massive (panel, brick) building and each dwelling can be used to protect the premises if the premises are sealed (before or after the danger signal). The least that can be done right away is to close the doors and windows, towels, scarves, better moistened. In the open, the body is protected with thicker clothing, hats, shoes, gloves, polyethylene cladding.

The underground premises (basements, garages) provide a higher level of protection than the building's floors. Where possible, use such premises or rooms on low floors without external access

It is important to control the dose of radiation exposure of the rescue workers by dosimetry [5].

The basic principle is that surgical emergency always takes precedence over radiological emergency.

Clothes contaminated with radioactive material are not discarded, shaken or brushed or washed, but folded gently with the lining outside and harvested in polyethylene bags. The envelopes are tied firmly and, where possible, subjected to dosimetric control that will decide the fate of the clothing. If the radioactive contamination is massive, the clothes should be destroyed by burying them deep in the ground. The burning of clothes is unacceptable because the fire and the smoke transmitted by the wind will disperse the radioactive material on a wide perimeter around.

Consumption of water and food after radioactive contamination

1. Water and beverages in closed containers are unavailable for radioactive contamination, so they can be used without restrictions. It is a good idea to keep the bottled mineral water safe for children.

2. The risk of using water from springs and wells is minimal. Water can be used for hygiene and drinking (if there is no bacteriological risk).

3.Water water from the urban water supply network can be used without limitation as long as the treatment facilities (chlorination) are working properly and the pipelines are not interrupted (in case of damage to the pipes the risk is bacteriological).

There is virtually no risk of internal contamination with radioactive materials: even if they fall on large open waters (dams), they are quickly settled on the bottom and kept from the mud.

4. Exclude rainwater tanks detected if rainfall coincides with radioactive contamination. Such water can not be used without dosimetric control.

5. The use of water for hygienic purposes (washing, bathing, cleaning with a wet cloth, etc.) is possible in all cases mentioned above in the section. 1, 2 and 3. Cleaning is by no means a vacuum cleaner; the radioactive material gathered there will turn it into a small dirty bomb.

6.Any "unprotected" food (from a container, a jar, a container, a suitable package) should be considered contaminated, whereas with dosimetric control it can not be proven otherwise, only in case of extreme necessity, such products as fresh fruit , vegetables, meat - provided that mandatory precautions are taken: thorough washing with water, scraping, peeling, cutting (ie all possible ways to remove the surface layer).

7. Milk, especially if given to children, should be used very cautiously and in reduced quantities. It is possible for the animals to be pastilles of grass polluted with radioactive material. Then the radionuclides pass and even concentrate in the milk. Under no circumstances should milk be purchased from private producers but only packaged in large milk-based compartments where, in the event of an accident, dosimetric control will be organized.

8. Decontaminating bulk products (flour, sugar, salt) are "left aside" until their radioactivity is reduced or used by mixing them with appropriate uncontaminated batches to reduce their specific radioactivity to acceptable levels & Quot; dilution effect & quot;).

9. In general, all canned products (in metal or glass packaging), as well as products stored in refrigerators or ordinary cabinets, are not contaminated. The only necessary precaution is to wash the wrapping or wiping with a damp cloth on the fridge before opening them.

10. Domestic animals and birds that have been outdoors in a contaminated area (after the radioactive material has settled) may be slaughtered and consumed. Additional measures are added to the usual procedures to avoid contamination of the meat (abundant washing). The skin and intestines must be disposed of (buried).

11. Eggs can be consumed without restrictions after washing with water and soap (the radioactivity accumulates in the shell) [3].

Where there is evidence of the use of radiological weapons and contamination in a particular territory with radioactive materials, the task of predetermined and specialized training groups (Civil Protection Teams, Medical Teams) is to identify the boundaries of the infected area with dosimetric equipment, entering and leaving the area, the number of those affected, who need medical assistance, the type of radionuclide used. Hospital evacuees struck by external contamination are subject to complete sanitation.

All teams working in the area contaminated with radioactive materials and the receiving departments of the respective hospitals targeted by the affected persons must have dosimetric equipment and a complete set of individual means of protection for each person of the staff.

Impacted by internal contamination (depending on the amount and type of radionuclide entering the organism), after complete sanitary treatment, are subjected to adequate treatment. The medical teams have ready-made Instructions for the Treatment of Damaged with External or Internal Pollution, where detailed approaches and treatment principles are described [2]. There are different approaches to different groups of radionuclides, different drugs are used and this is also reflected in the Instructions. There are also Instructions for the treatment of combined injuries (radiation in combination with chemical or biological weapons).

3. Conclusions:

1. Emergency training is necessary in view of the current international environment. After passing, learners acquire basic knowledge, skills and habits for action when an emergency occurs due to an incident, accident, terrorist act or otherwise.;

2. Specialized bodies at the Ministry of the Interior and Fire Protection and Population Protection Directorate in Bulgaria, the Ministry of Emergency Situations in Russia or the relevant structures in other countries should be prepared to take appropriate action in the event of an Emergency;

3. Greater attention should also be paid to international cooperation and joint action in the event of an emergency involving more than one country.

4. Literature:

1. Гърдев Е, Н. И. Пъдарев. Реални заплахи от ядрено оръжие за мирното население , Сборник доклади от научна конференция на НВУ “В. Левски” „Радиационната безопасност в съвременния свят“, В. Т. 2017.

2. Долчинков Н. Т., Хвостова М. С. Обучението по радиационна защита в контекста на актуалната международна обстановка, Годишна научна конференция НВУ, Велико Търново, 2018;

3. Долчинков Н. Т., Мерки за радиационна защита при аварии с възможни радиационни последствия за населението, Научна конференция „Актуални проблеми на сигурността“, НВУ, Велико Търново, 2017;

4. Долчинков Н. Т., Радиационната безопасност в България конференция „Радиационната безопасност в съвременния свят“, НВУ, Велико Търново, 2016 г. ;

5. Долчинков Н. Т., Развитие на националната автоматизирана система за непрекъснат контрол на радиационния гама-фон, Годишна научна конференция на НВУ, В.Търново, 2016 г.

6. Долчинков Н. Т., Хвостова М. С., Караиванова-Долчинкова Бонка Енчева, Действия при извънредни ситуации от техногенен характер, Научна конференция „Актуални проблеми на сигурността“, НВУ, Велико Търново, 2018;

7. Долчинков Н. Т., Хвостова М. С., Караиванова-Долчинкова Бонка Енчева, Действия при извънредни ситуации от техногенен характер с отделяне на радиоактивни вещества, Научна конференция „Радиоационната обстановка в съвременния свят“, НВУ, Велико Търново, 2018;

8. Зайцев А. П. Защита населения в чрезвычайных ситуациях, Москва, 1999;

9, Лилов И. Н., Миновски И. Н., Христов Й. Л. Evacuation algorithm of armoured vehicles, The 23rd international scientific conference Knowledge-Based Organization -Sibiu 15-17.06.2017

10. Маринченко А. В. Безопасность жизнедеятельности, Дашков и Ко, Москва, 2015 г;

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

12. Тарасов В. В. Основы защиты населения и территории в чрезвычайных ситуациях, Москва, МГУ, 1998.

RADIOLOGICAL THREATS TO THE SECURITY ENVIRONMENT

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

Abstract: *The threats to the modern security environment from radiological materials are explored. The possible scenarios for radiological impact from open and / or closed radioactive sources and nuclear weapons and the degree of potential danger are analyzed. The psychological effects of the population are examined. The role of state policy in radiological threats is stated*.

Keywords: RADIOLOGICAL, RADIOACTIVE SOURCES, THREATS

1. Introduction

In the new geostrategic situation in Europe and in the context of profound transformations in the domestic political situation in individual countries, there are serious changes in the nature of the security threats. The spectrum of new specific security challenges and threats is expanding. Some of them are hard to foresee. Such are the proliferation of weapons and technologies, including weapons of mass destruction, terrorism; refugee problems and illegal immigration; the manifestations of Islamic fundamentalism; environmental problems, industrial accidents and disasters, etc. Some of these threats have an international dimension and are of a global nature. Therefore, broad international co-operation is needed to neutralize them. They have a lasting character and therefore influence national and international security for a long time. The proliferation of nuclear weapons and other weapons of mass destruction is a threat to international security. It is a threat to our country as well. The number of countries that develop their own programs and produce dual-purpose materials, technologies and equipment has grown a lot. Attempts have been made to procure or develop and trade in nuclear technologies and materials from criminal groups and individuals using drug trafficking and arms trafficking channels or creating new ones. Countries such as Iraq, India, Pakistan and others are striving to acquire nuclear weapons and more.

The terrorism is the most serious threat to Bulgaria. This is a clear from the annual report on the state of our National Security in 2016. An in-depth analysis of the external environment for security and the dynamics of the processes in the world has been made, which determines the strengthening of the existing and emergence of new risks and threats to security of the Republic of Bulgaria. International terrorism and the proliferation of weapons of mass destruction, regional conflicts, migration processes, cross-border organized crime in the Balkans, terrorist threats from religiously motivated groups, hybrid actions against NATO and the EU, particularly against our country, as well as many other listed risks , which requires adequate management of the resulting hazards. [2]

The external environments, as well as the listed risks in the internal environment for our national security, require a set of interrelated priorities and sectorial policies integrated with EU, NATO, UN and OSCE security policies.

2. The Possible Scenarios for Radiological Impact to National Security

It is impossible to predict all potentially possible scenarios of radiological terrorism, which may differ in terms of objectives, ways and means that can be used. Objects may be individuals of the population, communities, the entire population of a country, and even predetermined purposes or persons may be predetermined. The use of radioactive sources or materials is one of the most likely scenarios for terrorist action plans. These are unprotected closed sources that can be placed in a variety of locations inside or outside buildings, vehicles, industrial sites, and other one. Radioactive substances in the form of hermetically sealed sources are used for various purposes in industry, medicine and more. These sources have a variety of activities, but the greatest danger is the unprotected sources of high activity. The consequences can be serious.

Radioactive material can either be dispersed in the environment (Radiological Dispersal Device (RDD)– dirty bomb) or directly irradiate people (Radiation Emission Device) resulting in individuals being exposed to alpha, beta or gamma rays. Polonium poisoning has been already employed in different occasions; orphan sources could easily be attached to explosive devices to spread ionizing radiations that can be inhaled, ingested or leading to people's skin or clothes being exposed). Of course, the most dangerous incidents should be theorized against nuclear power plants, with the risk of leaks or (worse) explosions resulting in a wider contaminated area with longer lasting effects not only on people, but also on the environment.

An RDD is a conventional bomb not a yield-producing nuclear device. RDD is designed to disperse radioactive material to cause destruction, contamination, and injury from the radiation produced by the material. An dirty bomb can be almost any size, defined only by the amount of radioactive material and explosives. A passive dirty bomb is a system in which unshielded radioactive material is dispersed or placed manually at the target. An explosive RDD—often called a "dirty bomb"—is any system that uses the explosive force of detonation to disperse radioactive material. A simple explosive RDD consisting of a lead-shielded container—commonly called a "pig"—and a kilogram of explosive attached could easily fit into a backpack. An atmospheric RDD is any system in which radioactive material is converted into a form that is easily transported by air currents. A variety of radioactive materials are commonly available and could be used in an RDD, including Cesium-137, Strontium-90, and Cobalt-60. Hospitals, universities, factories, construction companies, and laboratories are possible sources for these radioactive materials. [1]

Improvised Nuclear Device (IND) is intended to cause a yield-producing nuclear explosion. An IND could consist of diverted nuclear weapon components, a modified nuclear weapon, or indigenous-designed device. INDs can be categorized into two types: implosion and gun assembled. Unlike RDDs that can be made with almost any radioactive material, INDs require fissile material—highly enriched uranium or plutonium—to produce nuclear yield. [1]

Although the exact impact from a RN attack is hard to estimate, there are some simulations made on the damage that a detonation containing radioactive materials would cause to a city.

As part of the US Department of Homeland Security's Improvised Nuclear Device (IND) preparedness program Mr. Brooke Buddemeier from the Lawrence Livermore National Laboratory have calculated that a 10KT ground explosion within 1.6 miles of the U.S Capitol would lead to 1 million people exposed to 1Gy or more in the first 4 days. His simulation suggests that such a scenario would lead to more than 50,000 deaths due to blast, burn or radiation. Another simulation made by Dr. Cham Dallas from the Institute of Disaster Management and presented to the US Senate

Homeland Security Committee concludes that 180,000 people would be injured and in need of treatment (10KT detonation). [1, 6]

Another effect in radiological incidents is psychological. After terrorist incident, terror is instilled in the population, especially if the attack is against a soft target. Way afterward, statements of radiological use for the attack will heighten this fear, leading to psychosis and possible alienation of suspected ill/contaminated victims. Such substances are usually not perceptible by human senses, thus creating a fear determined by the absence of recognizable threats. [3]

Under affected area there is a sociological and will directly influence our collective behavior; in the wake of terrorist attacks against music venues, stadiums or restaurants, many people will decide to avoid such places. Long term effects however, can lead to behavior and routine changes, adapting one's lifestyle to new threats and fears. [6]

There are also logistic and operational problems to consider. Radiological substances released in an urban area will lead to prolonged emergency situations in time and space; metropolitan areas contaminated with biological, chemical or radiological agents will be forbidden for long periods, complicating the victim's rescue operations and influencing institutional, economic and normal activities resumption. Table 1 suggests possible radioactive materials as means of use.

Table 1: *Source or material, which can use for nuclear terrorism [9]*

Source or material	Source dimensions	Danger and Mode of Action
Small radioactive sources (nuclear medicine, brachytherapy)	$1nm^3 \div 100\ cm^3$	External exposure
Large radioactive sources (^{192}Ir ^{60}Co)	$1\ cm^3 \div$ some m^3	External exposure
Radioactive material containing a large source	$500\ cm^3 \div 1\ m^3$	Spray with or without explosive. External and internal irradiation.
Spent nuclear fuel	above $1\ m^3$	Spray with or without explosive. External and internal irradiation.
Attack against NPP or reactor failure	Fuel elements - length 5m	
Reactor failure	Destroyed active area or elements on first contour	External and internal irradiation.
Traffic incident with radioactive material	100÷200 l	External and internal irradiation.
Nuclear charge	A suitcase bomb	Shock wave, външно облъчване
Nuclear blast	A suitcase bomb	Shock wave, thermal radiation. External and internal irradiation.

Apart from the use of various devices by terrorists, it is not possible to exclude the attack of Kozloduy NPP or of nuclear power plants near our country. History has known cases of terrorist attack, which has led to many implications for the security environment. This report [10] presents the results of an independent analysis of the health and economic impacts of a terrorist attack at Indian Point that results in a core meltdown and a large radiological release to the environment. We find that, depending on the weather conditions, an attack could result in as many as 44,000 near-term deaths from acute radiation syndrome or as many as 518,000 long-term deaths from cancer among individuals within fifty miles of the plant. These findings confirm that Indian Point poses a severe threat to the entire New York metropolitan area. The authors of [11] give examples of technogenic emergencies with the disposal of radioactive particles from recent decades and present the existing potential sources of ionizing radiation near Bulgaria. In [12] is an analysis of their possible influence on the radiation situation in Bulgaria.

3. Role of the country to prevent the proliferation of radiological weapon

The fight against organized crime, and in particular with terrorism, is a long process, accompanied by expense of many human and material resources.

A major element of this struggle is the construction of anti-terrorist specialists. Of course, the problem of material provision of these specialists, as well as improvement of their knowledge and skills, is no importance, given rapid development of means and means used by terrorists to carry out their criminal acts.

Therefore, in parallel with practical work to prevent the criminal acts of individuals or terrorist groups, countries such as Bulgaria, which have no significant resources in organizational and financial terms, should use experience, financial and material assistance that can and should be in this critical period. The type of aid should primarily consist of providing know-how, specialized software and cooperation on information exchange, experience and training of specialists on the use of a technical tool for detecting banned and especially dangerous materials, as well as in the field of exchange of experience on the implementation of the Law on Measures against Money Laundering.

Of particular importance for the internal infrastructure in this plan is also the possible assistance for additional equipment with video equipment and equipment for observing passengers and freight in the area of the main railway stations; the purchase and additional equipment of equipment for carrying out radioactive control of goods at the border stations and the interior of the country; the preparation and further training of employees who will be involved in the management and handling of special equipment; providing the necessary protective equipment, in the event of extraordinary and crisis situations. [13]

The Government of the Republic of Bulgaria support adoption of Resolution 1373 (2001) by the UN Security Council, has undertaken and takes practical measures for its implementation. Through various legislative and administrative measures, the Bulgarian country has effective control over use of its territory by natural and legal persons who plan, assist, finance or commit terrorist acts against other states or their citizens. The Bulgarian Government is and will continue to make efforts, on a bilateral and multilateral basis, for the signature, ratification and implementation by the UN Member States of all universal and regional conventions relating to the fight against terrorism, and in particular the 1999 Convention on fight against terrorist financing. The Republic of Bulgaria will actively and constructively support all international fora for the adoption and enforcement of an effective international law system against terrorism, including a UN General Convention against Terrorism, which will be the universal reference framework for the multiplicity of international law instruments against terrorism.

The author B. Dimitrov [8] is concerned with the automated information systems for radiation monitoring in the Republic of Bulgaria and their capabilities for assessing the nuclear environment and warning to population. The emphasis is placed on the Unified Radiation Monitoring Information System, and the other existing

systems at national and institutional level. The purpose is to determine the capabilities of these systems to provide information on gamma levels that support the process of forecasting, warning and disclosing the population in nuclear, hazard cases.

4. Conclusion

Although the initial radiation and nuclear crisis response plans exist in all EU countries. In an average or large-scale incident, an affected country may not have the strength to deal with the situation for several reasons:

• Lack of capability and decontamination capacity,

• Limited stock of decontamination solutions,

• Limited specialized medical abilities and capacity,

• Lack of capacity and capacity for waste management (including disposal of contaminated water),

• Limited capacity and capacity to respond to crises (CR) and counteraction.

Only a few countries in EU have deployed military capabilities to decontaminate early staff. This creates a requirement for a minimum level of interoperability between countries and synchronized their Plans. Some cross-border bilateral or multilateral radiological and nuclear exercises are already in place, but in most cases they are related to incidents involving nuclear power plants and are concentrated on CR alone.

Prevention and CBRN protection and recovery are complex in nature and expensive questions. Efforts should focus on prevention measures; However, these failures, an international system, ready to deal with CBR (N) incidents, must be established to mitigate the effects.

5. Bibliography

1. https://www.cia.gov/library/reports/general-reports-1/cbr_handbook/cbrbook.htm#0

2. Доклад за състоянието на националната сигурност на Република България през 2016 г. МС на РБ. София. 2017

3. B. Immenkamp, "ISIL/Da'esh and non-conventional weapons of terror", European Parliamentary Research Service. 2015, p.4

4. https://www.interpol.int/Crime-areas/CBRNE/Radiological-and-nuclear-terrorism/Project-Stone

5. Council conclusions on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union – an EU CBRN Action Plan – Adoption http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015505%202009%20REV%201

6. Rogan, A., Chemical, Biological, Radiological, and Nuclear Threats. Atlantic Treaty Association. 2017.

7. Димитров, Б. К., Аспекти на ЯХБЗ при защитата на критичната инфраструктура. Сборник „Доклади от годишна научна конференция на НВУ „В. Левски". Том 11. 2015. стр. 155 – 162.

8. Димитров, Б. К., Анализ на автоматизираните информационни системи за непрекъснат контрол на гама фона в Република България. Сборник доклади от годишна научна конференция в НВУ „Васил Левски". том 4. 2017. стр.126 -133

9. IAEA. Generic procedures for assessment and response during a radiological emergency. TECDOC-1162. International Atomic Energy Agency. Vienna. 2000.

10. Lyman, Edwin S., The health and economic impacts of a terrorist attack at the Indian point nuclear plant. Union of Concerned Scientists. 2004.

11. Долчинков Н., Н., М. Хвостова, Б. Караиванова-Долчинкова, Действия при извънредни ситуации от техногенен характер. НВУ. В.Т. 2017.

12 Долчинков Н., М. Харалампиев, Анализ на действащите и проектирани ядрени мощности в региона и евентуалното им въздействие на гама-фона на територията на България. НВУ. В.Т. 2017.

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

THE IMPACT OF TECHNOGENIC ACCIDENTS ON THE SECURITY ENVIRONMENT

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

Abstract: *The situation changes in territory of our country lead to change in nature and importance of security factors and threats. Threats of technogenic nature for national security were analyzed. The factors for risk assessment of the impact of anthropogenic accidents on the security environment are presented.*

Keywords: TECHNOGENIC, ACCIDENTS

1. Introduction

In the beginning of 21st century the system of international relations was bound up with periodic and often contradictory tendencies. There are technological, environmental and demographic changes that have a huge impact on the public processes in the every countries.

The dynamics of international relations shows that in recently years of armed clashes between armed groups of ethnic, religious, financial, territorial-community and other controversies has decreased. Changes that occurred in last decade of the twentieth century and in the beginning of 21st century form a new strategic environment of security and proportion of military political forces on a global and regional scale. Along with the positive trends, there are a number of risks and threats, mostly of asymmetric nature.

In the context of new geopolitical realities, the Republic of Bulgaria and the other countries from Alliance and European union, must be deal with risks of a difficult nature, such as acts of terrorism, proliferation of nuclear and conventional weapons, technological and cyber-attacks targeting modern communication and information systems, government infrastructure, with many environmental threats and the lives and health of citizens. The new threats are mostly asymmetrical and non-traditional in nature. These new realities make it a matter of studying the various threats - traditional and non-traditional, particularly topical.

The topic is up to date and has a bearing on whole of the society, the state, and survival of mankind. There is no country capable of counteracting itself on new, invisible, unpredictable, and diverse threats to security. The aim of the report is to trace and analyze the leading traditional and new challenges, risks and threats to security in the first decades of the 21st century. The subject of development is the security environment at the beginning of the 21st century, and the subject of security threats and their impact on national security.

2. Relationship between National Security and Anthropogenic Accidents

The term "national security" first appears in American politics. For the first time, US President Roosevelt used the definition of "national security" in his speech to Congress in 1904. The accession justify of the Panama Canal Area to interests of national security. This term is used again by US President Franklin Roosevelt after the attack of Japan against the American military base at Pearl Harbor in December 1941.

According to Walter Lipman, "The state is in a state of certainty when it does not have to sacrifice its legitimate interests in order to avoid war, and when it is able to defend its interests if necessary by conducting war". [7]

In 1998, The National Assembly of the Republic of Bulgaria adopts the Concept of National Security, according to which "National security has the protection of the fundamental rights and freedoms of Bulgarian citizens, state borders, territorial integrity and state independence, where there is no danger of an armed attack, violent change of the constitutional order , political dictates or economic coercion for the state, and the democratic functioning of state and civic institutions is ensured, as a result of which society and the nation keeps and increases their welfare and evolves. Security is guaranteed when the country successfully realizes its national interests, goals and priorities and, if necessary, is able to effectively protect them from external and internal threats.". [8]

In a nation-wide sense, the threat is defined as a presumption of an incident, a crisis situation, or of damage to basic values, interests and objectives of society, life, health and property of citizens, destruction of existing material and natural resources and the functioning of the economy as a result of the manifestation of these events. [9] The threats are detrimental to all systems of public life, from individual to state. The threat to individual is an intention or desire to damage dignity and integrity of another person.

"The risk" is defined as an act of uncertainty, probability of consequences, dangerous condition, damage and loss, benefit and profit, behavior. The risk is an indefinite threat. There is no definite time for it to happen. Even if it is established early enough, in principle it is impossible to neutralize. The risk resembles threat but differs from fact that there is no other condition between threat and crisis, whereas between emergence of the risk and the crisis that time has not been established. The threat is a specific risk with the possibility of immediate realization.

According to the National Strategy of the Republic of Bulgaria "The strategic environment of security is complex, dynamic and difficult predictable dimensions. Impact on its formation has been: globalization, crisis in financial and economic sphere, proliferation of weapons of mass destruction and means of delivery, climate and health problems, demographic, environmental and energy problems, asymmetric risks and threats, threats to information security , countries with weak statehood, internal and regional conflicts, European and Euro-Atlantic integration, efforts of the international democratic community to maintain stability and stability ". [8]

Protecting the population from disasters, accidents and catastrophes is a priority activity in civilized countries. In Europe and in our country there are natural and industrial risk factors that affect the security of people, production and property. They lead to the need for reliable protection of the population, the implementation of preventive activities to prevent or reduce the losses and the consequences of disasters, accidents and catastrophes.

As a consequence of the technological activity of a human, major industrial accidents can arise with separation of strong toxic substances from the pharmaceutical, metallurgical, chemical, textile industry, accidents in the nuclear power industry, etc. The main flow of vehicles transporting dangerous goods passes through the territory of the country, which, in the event of a catastrophe, creates conditions for pollution of the environment. The state of the road and rail infrastructure, as well as the organization of the controls, do

not meet the safety requirements and are prerequisites for catastrophes and severe consequences. In the case of transport accidents or oil spills, oil products or natural gas, conditions are created for pollution and danger to humans health.

There are sites in the country that deal with radioactive sources. They can lead to the creation of radiation accidents and incidents. Insufficient control by the competent authorities of different owners of radioactive isotopes and sources of ionizing radiation and incompetence of citizens creates conditions for uncontrolled radioactive exposure.

In part of the settlements sanitary and hygienic conditions are deteriorated, which is a prerequisite for epidemics and diseases of a significant part of the population. The existing production and economic conditions in our country, worsened international situation, insufficient control of the trade in animals and products from them create conditions for occurrence of biological outbreaks.

The lack of systematic technological treatment and fertilization of soils, the free use of plant protection products and climatic conditions lead to a reduction in part of permanent crops. The state of environment in a number of areas is approaching an environmental catastrophe that poses a direct life and health threat of the population.

In recent years the number of terrorist acts, the spread of narcotic drugs and human trafficking have increased, leading to a deterioration of the socio-economic conditions of life in the Republic of Bulgaria. [1]

3. Industrial Accidents affecting the Security Environment

There are many sites in the country's energy, chemical, metallurgical, petroleum and pharmaceutical industries. They work with explosive, highly flammable, combustible and highly toxic substances. They can cause industrial accidents and fires. Under adverse weather conditions, the pollutants released may cause environmental pollution of a cross-border nature.

Any mistakes in the operation of the Kozloduy NPP may lead to accidents involving the disposal of radioactive products in the environment. This may complicate the radiation situation, whereby a portion of the population can be irradiated above the admissible norms. In unfavorable weather conditions, if radioactive discharge is not controlled, radioactive contamination of the environment, including transboundary pollution, is possible.

In the operation of nuclear power plants there is a likelihood of an accident with possible radiation consequences for the population. The potential danger of such an accident shall be analyzed and evaluated beforehand in the design of the NPP, considering all possible emergency situations (realistic and hypothetical scenarios) and on that basis the necessary measures to prevent accidents and mitigate the consequences to an acceptable level according to regulatory requirements.[12]

According to the "Safe Use of Nuclear Energy Act", persons who carry out nuclear energy and ionizing radiation and radioactive waste and spent fuel management activities are obliged to take measures to prevent accidents and to limit and eliminate the consequences from them. The competent state authorities shall define and implement emergency planning and emergency preparedness measures in the case of a possible accident with possible radiological consequences. These measures are based on an analysis of the possible scenarios for the occurrence and development of various accidents and the assessment of the radiation risk to the population.

Despite stringent safety measures for the operation of different types of nuclear reactors and the availability of automated management, control and protection systems, operational practice indicates that emergency situations may arise which are accompanied by uncontrolled releases of radioactive substances into the environment . Analysis of emergency situations shows that most often they are due to errors by the service staff, ie mostly subjective factors. [2, 3, 4]

Radioactive contamination could occur when:

- Emergency situation at Kozloduy NPP, accompanied by uncontrolled releases of gaseous radionuclides into the environment;

- transboundary radioactive contamination;

- in the case of a car accident carrying a radioactive material.

There are companies working with sources of ionizing radiation in the country. In the event of accidents, local outbreaks may occur, dangerous to the operating staff. They can become subject to intrusion, criminal trafficking and radiation terrorism.

On the territory of the country there are unplanned aviation, artillery, naval and ammunition in the quantity and location. Some have retained their combat capabilities and pose a risk of improper handling. Industrial failures are possible when they fall into the technological process of metallurgical firms.

There may be biological outbreaks as a result of insufficient control of trade and export of animals and products.

Large quantities of chemical substances are used and stored in the industry, which under certain circumstances - accidents or natural disasters - can become a threat to people's health and lives. To prevent accidents, strict preventive measures are taken, but if they arise, there must be an immediate response to the specialized bodies to address the situation and to eliminate the consequences.

All sites are practically chemically hazardous, using chemical technology. These are primarily chemical, petrochemical and similar plants and plants, repositories of hazardous chemicals and oil products warehouses. Chemical objects can also include a significant part of the non-chemical industries, in the process of which hazardous substances are applied and have chemical transformations. It is true that objects with chemical technologies are potential sources of hazardous substances and environmental pollution and they can be called chemical-risk sites. By Valery Legasov's definition, in the event of an accident at any industrial site, the process of destructive release of its own energy source, where raw materials, intermediate products, and plant production are involved in an emergency process, create disruptive factors for the population and the environment, the level of chemical risk is significantly high. [10]

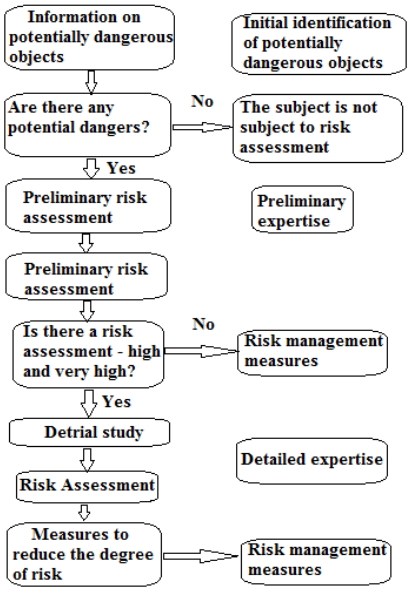


Fig. 1 *Risk Analysis for Anthropogenic Accidents*

Risk analysis for industrial accidents can generally be performed based on the scheme of Fig. 1.

4. Transport accidents affecting the security environment

Despite the rapid technological changes, the Balkans retain their important geostrategic position. With the enlargement of the EU and NATO, the importance of the region as a transport, infrastructure and energy junction is growing. The importance of the region is also growing, as a link with the European markets to the Caucasus and Central Asia.

Types of transport accidents can generally be divided by the center of the event, namely land, sea and air. The favorable geostrategic position of the Republic of Bulgaria is an important prerequisite for busy road, rail, air and water transport. The international routes to Central Europe, the Middle East, the Baltic States and Russia pass through the country. This creates conditions for transport accidents related to the transport of dangerous goods, causing environmental pollution and endangering human life and health.

On the territory of the country there is a process of development and distribution of the oil and gas transmission networks, telecommunications, the international traffic of commercial and industrial goods is enhanced. They represent an object of control.

The Danube and the Black Sea connect us with the countries of Central Europe and the Black Sea Basin. They are natural waterways for the transport of large quantities of petroleum products and severe accidents can have serious environmental consequences.

Under the conditions of a complex criminogenic situation, it is possible to cause accidents due to diversions of oil pipelines, gas pipelines, electricity transmission networks, theft and traffic of radioactive sources. Possible damage to infrastructure and production facilities. These potential dangers can lead to escalation of tensions that will turn into crisis. Transport plays a key role in the development of any modern society as a means of economic development and a prerequisite for achieving social and regional cohesion. Bulgaria's transport sector is of utmost importance for enhancing the competitiveness of the national economy and servicing the population. This is evidenced by the fact that as of 2008 the Bulgarian transport system provided on average daily 2.54 million passenger trips and 274 thousand tons of freight.

In our country, it was agreed on November 17 to honor the memory of those killed in crashes. The highest share of transport accidents in Bulgaria is related to road transport. Of course, there is no need to underestimate the railroad on which a significant amount of dangerous goods is carried, and the air in which the number of victims is numerous.

The assessment of traffic safety situation on the roads, in the light of tasks and objectives set out in the National Road Safety Improvement Strategy of the Republic of Bulgaria for the period 2011-2020, makes it possible to set certain priorities for work with a view to creating the conditions for continuing the trend of permanent reduction of victims of traffic accidents.

Table 1: *Traffic accident statistics on the territory of Bulgaria. [11]*

period	In 2017	In 2016	In 2015
traffic accident, num.	6 888	7404	7226
died, num.	682	708	708
injured, num.	8 680	9374	8973

5. Global Anthropogenic Risks affecting the Security Environment

Energy and resource security are an element of the national security. Water resource problems, environmental pollution, limiting access to strategic raw materials can lead to tensions and crises at national and in the ternational level. The modern economic and the technological development and use of resources, environmental pollution and urbanization bring environmental issues as a specific risk and a threat to national security.

In the modern world, political threats - terrorism, extremism, separatism, and so on - are becoming increasingly important.

A serious strategic threat to Europe is terrorism, especially since the Madrid attacks of 11 March 2004. In the past, the actions of terrorists are primarily directed at specific political leaders, and contemporary attacks are global in nature, cause many sacrifices and are mostly related to religious extremism. European countries are both targets of terrorism and its base. Al Qaeda bases are found in the UK, Italy, Germany, Spain and Belgium. That is why European counter-terrorism policy is paramount.

In the new international environment, terrorism gains greater comprehensiveness. Terrorists are rapidly developing ways and means of achieving their criminal objectives, involving more people, overcoming geographical barriers, and creating clusters between groups in one or more countries.

The proliferation of weapons of mass destruction is the greatest potential threat to European and world security. New technologies and research increase the potential danger of attacks with biological, chemical weapons and radioactive materials. The risk to Europe's security is rising with the proliferation of missile technology. Regional conflicts have an impact on European interests and regional stability. Whether in the immediate vicinity of EU borders (Balkans) or in different parts of the world, they cause numerous casualties, destroy social and material infrastructure, threaten minorities and fundamental human rights and freedoms. Conflicts are growing into extremism, terrorism and state instability. They lead to an increase in crime, stopping investment and disrupting the normal functioning of political and economic processes. [1, 8]

Existence of the conflict zones unresolved issues in inter-state relations, socio-economic problems, political instability and internal conflicts and inefficient cross-border control complicate the regional environment. A challenge for the national security is infiltration of refugee flows and illegal immigrants into the country. The social threats, including corruption, crime, drugs, illness, hunger, poverty and others, seriously threaten security in our country. Incorrect governance, corruption, abuse of power and weak institutions, lack of accountability and civil protests lead to a weakening of government and state institutions. The organized crime is an internal threat to the EU, but it has an external dimension. Trafficking in drugs, women, illegal immigrants is the criminal activity of organized criminal networks, often linked to terrorist groups.

The environmental threats including disasters, accidents, catastrophes, pollution and others have little impact on security. The origin of threats to security and the existence of man are increasingly associated with the unfavorable state of the environment. There is no doubt that environmental pollution can cause a number of ecologically-based diseases, resulting in a reduction in the life expectancy of people affected by adverse factors.

Environmental security threats include likelihood of occurrences of phenomena and processes whose implementation may lead to negative impacts on the environment and health of the population. These phenomena and processes are expressed in intentional or unintended environmental impacts of human activity or as a result of the occurrence of natural and natural disasters and catastrophes. [6]

The global risks resulting from human activity on the security environment - environmental catastrophes and socio-economic manifestations are detailed in [1].

6. Conclusion

Prognosis and analysis of potential dangers and threats indicates that they can lead to serious difficulties in the normal rhythm of the crisis areas. The vital management systems, normal functioning of the national economy and threatening the lives and health of the population can be impaired. The environment of security is characterized by high dynamism and increasing unpredictability. Changes in it depend primarily on the impact of non-military (asymmetric) risks and threats. Dynamic changes in the security environment have shown that conflicts and crisis situations that are complex and difficult to predict and manage can occur in the present and in the future with a high probability. This poses risks and threats to the national security.

In order to reduce the losses and to eliminate the consequences, it is necessary to plan and coordinate measures for the protection of the population and the national economy in advance with the state authorities, the local authorities and the national economy. Contemporary actions in carrying out emergency and emergency rescue work require the establishment of an organization, the preparation of authorities for leadership, forces and resources and their keeping in constant readiness. To ensure the implementation of the emergency and emergency rescue works and the provision of living conditions in distressed areas it is necessary to plan and allocate stocks of material and technical means and regulate the order and the ways of their use.

7. Bibliography

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

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

3. Димитров, Б. К., Аспекти на ЯХБЗ при защитата на критичната инфраструктура. Сборник „Доклади от годишна научна конференция на НВУ „В. Левски”. Том 11. 2015. стр. 155 – 162.

4. Димитров, Б. К., Анализ на автоматизираните информационни системи за непрекъснат контрол на гама фона в Република България. Сборник доклади от годишна научна конференция в НВУ „Васил Левски”. том 4. 2017. стр.126 -133

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

6. Padarev, N., Analysis of the Relation Between Climate Changes and Security Area, International Conference Knowledge-Based Organization, Vol. XXIV. ISSN 1843-682X. Sibiu. Rom. 2018. (pp 169-173)

7. Стратегия за национална сигурност на САЩ. 2006.

8. Стратегия за национална сигурност на България. 2011.

9. Среда за сигурност - рискове и заплахи за националната сигурност (2010) – Годишният доклад на Държавна агенция „ Национална сигурност " за състоянието на националната сигурност за 2010г.

10. Владимиров В. А., В. И. Измалков, А.В. Измалков, Радиационная и химическая безопасность населения. Москва. Деловой Экспресс. 2005.

11. https://www.mvr.bg

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

APPROACH ANALYSIS TO PREVENT STEGANOGRAPHY DATA FLOWS AS A CORPORATE SECURITY BREACHES

Lopit P.[1,2], Assoc. Prof. PhD. Alieksieiev V.[1,3]

[1] Lviv Polytechnic National University, Lviv, Ukraine

[2] polina.velebnik.pm.2015@lpnu.ua
[3] vladyslav.i.alieksieiev@lpnu.ua, https://orcid.org/0000-0003-0712-0120

Abstract: *Once the steganography was invented, it still remains one of the most effective ways to hide information in publicly accessed data sources. Many applications of different steganography techniques were known since WWII, but there are no yet any good approach to detect whether there is a hidden message in some data source (image etc.) while it is not expected to be found. This may also cause a fundamental security breach in corporate security systems. In the era of Facebook, Instagram and many other social networks with a huge amount of images and photos it seems obvious to use steganography applications for the purpose of security breach. A saboteur or a spy can use any image from social networks to disclose corporate sensitive data or to exchange hidden messages. That is why steganography detection should be considered as a necessary tool to prevent security breaches and sensitive data leaks. This research is focused on analysis of current approaches in problem of steganography detection. Mainly the approaches to detect steganography in images were discussed.*

Keywords: STEGANOGRAPY, STEGANOGRAPHY DETECTION, CORPORATE SECURITY, DATA FLOWS, SECURITY LEAKS, WEB BROWSER EXTENIONS

1. Introduction

Steganography is a well-known method of cryptography [1]. There is a number of implementations to hide some information within some carriers (i.e. in an image). Common cryptography techniques usually assume the possibility of secret message interception. This guaranties any necessary security level. Unlike to that the steganography relies on the principle, that the hidden or secrete information should be hidden within a public visible carriers and no one should guess there is something hidden.

As many reviewers mention the steganography approaches are in use since ancient ages [2]. Obviously, people are very inventive in their passion to hide secretes they have. First steganography approaches used texts and paintings to hide secret messages. Due to a technologies development there are many new carriers appeared in steganography [3–7]. Since a widespread use of computers and computer networks, the steganography came into all media carriers, including texts, images, audio, video and IP datagrams.

There are many known useful techniques of copyright and theft protection via steganography watermarking to protect media data in the Internet. On the other hand, some modern printers use steganography techniques to watermark each printed page and make an invisible signature allowing printer identification. Digital content protection is the area where steganography was successfully used. Most Internet users do not even think they are forced to see steganography processed media (images, photos etc.) at many websites trying to protect their authorship. All these steganography applications prove the fact the steganography became an integral part of our modern life.

2. Prerequisites and means for solving the problem

Nevertheless, there is a number of reports revealing facts about illegal use of steganography for the villain's purposes, including intelligent services' spies [8] and terrorists [9]. These facts turn us to thoughts of security breaches, corporate data protection and preventing sensitive data leaks. Each company is interested in analysis of possible channels of data flows to be able to identify the breach.

In the era of mobile devices, social networks and mobile internet, allowing any common person to become a "spy", it is of a great importance for cybersecurity purposes to unveil possible channels of leaks, to identify menacing data flows and not to break civil rights simultaneously. Each corporate worker uses to download and looks through tons of text and image information every day. Evidently, this could be the easiest way for hostile informer to use hidden messages in an invisible manner within a publicly visible carrier.

For example, a hidden message transfer scenario may include taking and sharing selfies with some custom encoding/decoding application for a mobile device. However, from the spy point of view, this scenario is vulnerable to disclosure with physical evidences of malicious activity (the device with software installed in it). Another scenario may involve visiting some website performing all the necessary steganography processing. This scenario can envisage some "independent" steganography processing service with anonymous access with just encoding secrete message into user's image and displaying the hidden message after decoding a steganographic image (the image can be given by URL). Combining such service with some "incognito" browser mode and "anonymizer" web service may allow eliminating any digital evidences at spy's device.

The idea of transferring steganography-processed images over public networks is not a new one. Moreover, there is a number of researches with its implementations [5–7]. Some authors (like [5, 6]) are using their custom approaches of LSB algorithm. There are suggestions on how to hide information in a publicly available billboard display [5] and suggestions on how to detect presence of steganographic information in publicly available content (jpeg-images) from Internet [7].

Of course, using social networks, which are performing their own image processing with compression, makes it difficult to guarantee lossless data transfers over these networks. Nevertheless, these networks can be used to share links to some "funny" images at third-party websites. The best candidates for being used as a channel for steganography data flows could be websites providing original (not changed) media content to its visitors.

Applying any of depicted scenarios leads us to a conclusion, that there should be some way either to check all corporate incoming and outgoing Internet traffic (check for steganographic data on a firewall, proxy etc.) or to check Internet traffic directly at workplaces in a web browsers. The ideal solution could be a corporate web browser to prevent steganographic leaks with embedded content inspection. Unfortunately, this solution is very expensive and requires many resources to support such custom web browser. However, all modern web browsers support extensions or plugins. This is a convenient way to extend a browser functionality without intruding the browser itself.

3. Solution of the examined problem

Our approach to solve the problem of preventing steganography data flows will exploit the opportunity to use web browsers plugins. Such plugin should match the following requirements:

- Plugin should analyze content of a web page, the user (company employee) visits.
- Plugin should extract images from the HTML-code and perform detection of hidden steganographic information. Statistics analysis methods should be used to analyze this information.
- Plugin should have a modular structure to allow further improvement, refactoring and support, including ability to add new methods of hidden information detection.
- Plugin should block suspicious data transfers and send a notification to security department with detailed description of possible malicious activity.

As an initial approach, we will use a good known LSB algorithm. Building the described above plugin should allow first a simple detection of LSB encoded steganography for bitmap images (BMP image format), and the most popular in the Internet image formats: JPEG-images and PNG-images. Next, we will develop and add methods for steganographic data detection in other popular graphic formats. Our current target is to develop the plugin as a platform for its further improvement via embedding new methods.

4. Results and discussion

Our plugin parses the HTML code, and extracts the list of images from of a web page. Then it performs a test of each image for possible hidden content in the image. Fig. 1 presents the example of parsing and image extraction from HTML.

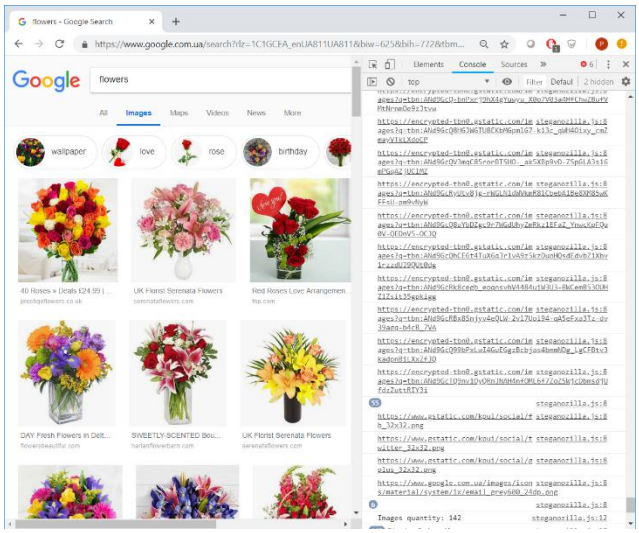


Fig. 1 *Parsing and extracting list of images from HTML*

We prepared an image to perform a test of our plugin working on detection of possibly hidden data within the image. Then we were adding a hidden data (text file named “cubaan.txt” with text string in it: “alpacas rule the world”) to the image using LSB algorithm.

Fig. 2 shows the original JPEG-image. The steganographic JPEG-image with a hidden data shown at Fig. 3.

Fig. 4 presents the original PNG-image and the steganographic PNG-image with hidden data shown at Fig. 5.

As one can see we have successfully processed with steganographic data insertion most popular image types – JPEG and PNG. Results of steganographic processing for BMP images are good known, so we do not present the examples here in this paper. All images of these three types are detected if a hidden steganographic data appears there. It is a very limited solution yet, because we only used popular LSB steganography algorithm in our plugin as method of encoding. Nevertheless, we had built a good initial platform solution as an approach for the required web browser plugin. This plugin allows easy extension later with new modules to implement detection of more steganography encoding methods.

5. Conclusion

Here in the paper we offer an initial problem analysis and a test implementation of steganography detection plugin for a web browser. The set of requirements for such kind of an online security solution was offered. Following these requirements, we are going to improve the developed plugin and allow a wider set of image types (not only BMP, JPEG and PNG) to be analyzed on-the-fly. Based on the presented ideas a security web-service can be developed. The service may gather and accumulate security alerts from different users and help to identify most typical channels of steganography data flows.

6. Literature

1. Steganography – Wikipedia // Wikipedia.org – 01.10.2018. – https://en.wikipedia.org/wiki/Steganography
2. Steganography: Past, Present, Future / James C. Judge // SANS Institute, 2001. – 29 p. – Retrieved from: https://www.sans.org/reading-room/whitepapers/stenganography/paper/552
3. Review on steganography for hiding data / Sagar S.Pawar, Vinit Kakde // International Journal of Computer Science and Mobile Computing – Vol. 3 Issue 4, Apr. 2014, P. 225-229. – Retrieved from: https://www.ijcsmc.com/docs/papers/April2014/V3I4201468.pdf
4. Steganography and Steganalysis: Different Approaches / Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal // ArXiv.org, 2011 – Retrieved from: https://arxiv.org/ftp/arxiv/papers/1111/1111.3758.pdf
5. Steganography An Art of Hiding Data / Shashikala Channalli, Ajay Jadhav // International Journal on Computer Science and Engineering – Vol. 1(3), 2009. – P.137-141 – Retrieved from: https://arxiv.org/ftp/arxiv/papers/0912/0912.2319.pdf
6. Unseen: An Overview of Steganography and Presentation of Associated Java Application C-Hide / Jessica Codr // Washington University in St. Louis, Apr. 2009. – 21 p. – Retrieved from: https://www.cse.wustl.edu/~jain/cse571-09/ftp/stegano.pdf
7. Detecting Steganographic Content on the Internet / Niels Provos, Peter Honeyman // CITI Technical Report 01-11, Center for Information Technology Integration, University of Michigan, Aug. 2001. – 14 p. – Retrieved from: http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf
8. Criminal complaint by Special Agent Ricci against alleged Russian agents (PDF). United States Department of Justice, 28.06.2010 – http://www.justice.gov/opa/documents/062810complaint2.pdf
9. Jack Kelley. Terror groups hide behind Web encryption. USA Today, Feburary 2001. – http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm



Fig. 2 *Original JPEG-image (before steganographic processing)*



Fig. 3 *JPEG-Image with hidden data (after steganographic processing)*



Fig. 4 *Original PNG-image (before steganographic processing)*



Fig. 5 *PNG-Image with hidden data (after steganographic processing)*

SECURE BIG DATA AND IOT WITH IMPLEMENTATION OF BLOCKCHAIN

Daniela Mechkaroska, Aleksandra Popovska-Mitrovikj and Vesna Dimitrova

Faculty of Computer Science and Engineering,
University "Ss Cyril and Methodius" - Skopje, P.O. Box 393, R. of Macedonia
emails:{daniela.mechkaroska, vesna.dimitrova, aleksandra.popovska.mitrovikj}@finki.ukim.mk.

Abstract: *BlockChain is a distributed database of records or public ledger of all time stamped transactions saved in all computers in one peer-to-peer network. It allows a secure and transparent transfer of digital goods including money and intellectual property. Bitcoin - a digital decentralized cryptocurrency, is the first application of BlockChain. The second application is an agreement called Smart contract that enables exchanging a value or assets between two owners based on a set of conditions included in the contract.*

In this paper, we analyze the possibilities for application of BlockChain in Big Data and IoT. Implementation of BlockChain in Big Data confirms that data is accurate and secure and sharing of data will become more simple. In industries like financial services, government and healthcare there is a need to combine BlockChain and Big Data because these industries have repositories full of important data. They must store and share these large amounts of data. Implementation of BlockChain technology provides security of data and ensures its integrity when shared. BlockChain technology is also seen as a way to secure the Internet of Things (IoT). Application of BlockChain in IoT enables IoT devices to participate in BlockChain transactions and invents new styles of digital interactions. This technology will provide a simple infrastructure for devices to directly and securely transfer data or money using Smart contract.

KEYWORDS*: BLOCKCHAIN, BITCOIN, SMART CONTRACT, PEER-TO-PEER NETWORK, IOT, BIG DATA.*

1. Introduction

BlockChain is a distributed ledger that records transactions in blocks that form a chain. This chain is secure, immutable, and transparent. Therefore, solutions that use BlockChain technology can be a pillar of data handling and processing systems within organizations. Integrating BlockChain with Big Data has many advantages because it enables better management of enormous volumes and variety of information.

Big Data and BlockChain are correlative: Big Data has processing capacities that can handle BlockChain complexities and its big expansion and vice versa. Implementation of BlockChain in Big Data confirms that data is accurate and secure and sharing of data will become more simple.

First, in this paper, we explain what the term Big data means, where they are used, and which tools are used to process them. Then, we will briefly explain the basic principle of work of BlockChain technology.

The rest of the paper is organized on the following way. In section 2 and 3 we explain what is Big Data and BlockChain technology. Next, in section 4, we consider the benefits of application of BlockChain in Big Data and Big Data analytics. Also, in this section, we analyze several implementations of BlockChain technology in Big Data: in the financial service industry, in industries outside of banking and in Supply Chain Monitoring and we give some examples for improving Big Data using BlockChain. In section 5 we investigate benefits of application of BlockChain in IoT. At the end, we give some conclusion.

2. What is big data?

Big Data is a term used for a collection of large and complex data sets. For example, Facebook has collected 300 petabytes of personal data since its inception, as they are the records kept, messages sent, videos published, transaction data from online transactions and shopping among many other sources of big data.

It is hard to process and analyze Big Data with traditional techniques, because it refers to a big volume of structured and unstructured data. An important role in collecting, storing and processing these big amounts of data has the growth of cloud storage in helping companies. Tools like Hadoop, Plotly, Bokeh, etc. can provide massive storage for any kind of data and enormous processing power, internet of things and unstructured sources. Studies show that 2.5 quintillion bytes of data are generated daily.

Despite such a contribution to the effective management of large amounts of data, there is a growing concern about user privacy and big data security. There are many examples that show it, like the large-scale scientific experiment conducted by Facebook without informing its users explicitly or the government has often come under attack for its observation on its citizens without their explicit permission. Today the great businesses are careful in accepting big data, in order to ensure their security and privacy [1].

3. BlockChain technology

BlockChain is a decentralized ledger of transactions, distributed on all computers in one peer-to-peer network where all details of transactions are visible to everyone connected to the network. Namely, this is a growing list of linked blocks. The blocks consist of valid transactions, a timestamp and a hash pointer as a link to the previous block in the chain.

The sequence of linked blocks creates a secure, interdependent chain. Blocks must first be validated to be added to the BlockChain. When a block is verified, it is distributed through the network (added to the existing chain) and each node adds the block to the majority BlockChain. Then the transaction is completed [2].

Three data attributes that are in BlockChain, and which are rarely provided in conventional centralized data management are [3]:

- **Security -** It is almost impossible for data to be changed or corrupted if BlockChain is used.
- **Integrety -** BlockChain data offers audit trails, certainty of origin, and digital signature of the message also provides integrity through the transfer.
- **Value -** Data generated with BlockChain is complete and there is no doubt for its value.

4. Benefit of application of BlockChain in Big Data

Regardless the variety, velocity and volume of data, Big Data tools can process it and BlockChain enables transparency and simplicity to processes in every area. The importance of Big Data and the development of BlockChain technology in the last years enables abandoning of the old information processing structures and business transaction processing. Big Data and BlockChain are correlative: Big Date has processing capacities that can handle BlockChain complexities and its big expansion and vice versa [4].

Some of the benefits of using BlockChain technology in Big Data analytics are [5]:

- reduces costs (significantly reduces storage costs);
- increasing traceability (each product or document has "digital password" which ensures tracking of its origin and journey);
- enhanced data quality (data is complete and structured, weak points in a big data analytics which increase accuracy and makes analysis easier);
- facilitates data access (users from different departments can access the data for the analysis process and this shortens the time cycle of data access and analysis);
- enhancing security (the system is decentralized and transparent, so the risk of fraudulent activities is reduced).

4.1. Analyses of several implementations of BlockChain technology in Big Data

a) Speeding up the financial service industry

The connection of BlockChain and Big Data in financial institutions will allow to estimate risk and identify suspicious patterns in real time. Using BlockChain as a means of conducting transactions will help to protect banks and their customers from fraud, to speed up the process of transactions and reduce the cost of money transfers [6].

For example, in the last few years, in order to simplify money transfers between bank accounts using BlockChain technology, an organization of 47 Japanese banks joined a BlockChain startup called Ripple. The aim of this is to perform real-time transfers at a lower cost. The traditional real-time transfers are expensive, because of the potential risk factors as double spending that can be avoided with BlockChain technology. Big Data analyses together with BlockChain can identify risky transactions faster than the current ones. This reduces the cost with real-time transactions [7].

b) Security in industries outside of banking

To handle data and prevent hacking and data leaks, healthcare, public administration, enterprises have started using BlockChain.

For example:

- **Healthcare**: a project at the MIT Media Lab known as Medrec is starting to create BlockChain system that gives priority to patient agency, which authorizes patients to share their records. In order to make the sharing of permissions to access data easier, Medrec uses a private Ethereum chain [8].

- **Insurance:** A controlled master policy from the UK, and three local policies from the U.S., Singapore and Kenya, have been written into a "smart contract" that enables a shared insight into policy data and documentation in real-time. Clarity into coverage and premium payment at the local and master level is provided by Blockchain. It also enables automated alerting to participants in the network after payment events [9].

c) Supply Chain Monitoring

The goods included in Supply Chain are added to the BlockChain and a Mobile App is used to monitor the status of the goods while being transported. The benefit of using BlockChain in Supply Chain are [10]:

- reduce or eliminate fraud and errors;
- improve inventory management;
- minimize courier costs;
- reduce delays from paperwork;
- identify issues faster;
- increase consumer and partner trust.

For example, in order to improve food safety by increasing the monitoring of products from the place of origin to the time it is sold to the consumer, Walmart uses BlockChain technology. In this way, users get credible insights of the origin of food. Receiving unchangeable, credible and traceable data is of great importance to success of Walmart's operations, because it produces 40 petabytes of data every day [1].

4.2. Examples for improving Big Data using BlockChain

In this subsection we present several examples of implementation of BlockChain in Big Data.

- Example 1: GOLEM

Golem network is a decentralized network of computers that utilizes computer power of the network users to make the supercomputer functional. Laptops, desktops, and data centers are just a few examples of devices that can contribute computing power to the network. A decentralized sharing economy is the form of the network and the computing power is shared. In this way, people can make money from renting their computer power and software. They are also able to lower the costs and not to depend on a centralized company for computing services for running some programs [11].

- Example 2: PATH

Path aspires to unite both BlockChain and Big Data allowing users to rent their extra bandwidth. This comes as a result of the fast acquiring of BlockChain technologies among people and companies. "Path Mining Nodes" are installed onto companies' computers and they work passively in the background - earning tokens for providing insights into performing of their websites or the loading time of their applications etc., back to Path and the clients they service. The real value of BlockChain data is the quality and how it is stored on the public ledger. Thus, this platform, together with the others BlockChain platforms that help companies to improve data, can become middlemen between companies and the users [12].

- Example 3: ESTONIA

Keyless Signature Infrastructure (KSI) is a BlockChain technology designed in Estonia to ensure that network and data are free of compromise and retain data privacy. KSI is used to store public data in BlockChain by Estonia, which is striving to be the world's most advanced digital society. Using this, the government can observe any changes in the database thus ensuring that the data is transparent. This has two benefits: cuts down external falsified/tampered records, and makes harder for unauthorized government officials to interfere with information and data [1].

- Example 4: SKRY

Financial institutions, law enforcement, and Bitcoin companie*s can detect suspicious activities using the first product of Skry. It can also identify legal and illegal entities, which enables following regulations and investigation of cyber-crimes like ransomware extortions, terror financing or drug trafficking on the dark web.

5. Internet of Things (IoT) and BlockChain

Application of BlockChain in IoT enables IoT devices to participate in BlockChain transactions and invents new styles of digital interactions. This technology will provide a simple infrastructure for devices to directly and securely transfer data or money using Smart contract.

5.1. Challenges of a secured IoT model

The current IoT ecosystem is based on a centralized model – client/server model, where all devices are identified, authenticated and connected through cloud servers. This structure is the biggest challenge of IoT security. Even, if the devices are at a short distance the connection between them will have to go through the cloud. These models continue to be used in today IoT networks, although they might not be able to handle the growing needs of giant IoT ecosystems in the future. The costs for existing IoT solutions, that use centralized model, are another big obstacle for the future growth of the IT network. The clouds, large server farms, and networking devices have higher costs for infrastructure and maintenance. Also, in order to protect IoT devices and platforms form physical tampering, new security technologies are needed. In addition, many devices in IoT system use simple operating systems and processors that not support advanced security systems [13].

BlockChain in IoT can be used in tracking connected devices, processing of transactions and coordination between devices. The decentralized nature of BlockChain technology will produce a more flexible system for running the devices and with the cryptographic algorithms data will be more private. The BlockChain ledger cannot be manipulated by malicious users since it does not exist in any single location, which means that it is a tamper-proof. Also, BlockChain enables secure peer-to-peer messaging between IoT devices. Capabilities of BlockChain, such as decentralization, autonomy and confidentiality, make this technology ideal for a fundamental component of IoT solutions [13].

From this, we can conclude that the main benefits of using BlockChain technology in IoT system are:

- build trust
- reduce costs
- accelerate transactions.

5.2. Example of IoT and insurance

Usage-based insurance (UBI) models are some of the new products that will develop accurate actuarial models which is valuable to insurers. For example, in the auto insurance, we can use encrypted data for driving times, distances, acceleration, braking and other behaviors for identification of high-risk drivers and validation of the information included in the applications. On this way, we can provide consumers bigger control over their premiums. The question is how to manage the enormous volume of data and logic because of the communication between millions devices. Large complex networks can be managed by BlockChain with devices communicating between each other on a peer to peer basis, securely and accurately, instead of building an expensive data center. This type of managing devices is cheaper than the data central model [14].

Conclusion

In this paper, we analyze benefits of using BlockChain technology in Big Data and IoT and possibilities for improving security. We present several examples of implementation of BlockChain technology in Big Data and IoT (in the financial service industry, in industries outside of banking, in supply chain monitoring, auto insurance, …).

From the presented analyses we can conclude that the main benefits of using BlockChain in Big Data are: reduced costs, increased traceability, enhanced data quality, facilitated data access and enhanced security.

For IoT the main gains from implementation of BlockChain are: build trust, reduced costs and accelerated transactions.

References

[1] https://medium.com/ethereum-dapp-builder/how-blockchain-will-improve-big-data-da1547dd268

[2] Mechkaroska D., Dimitrova V., Popovska-Mitrovikj A.: A Survey on Applications of BlockChain Technology, Proc. of the 15th International Conference on Informatics and Information Technologies CIIT, 2018 (in print)

[3] https://jaxenter.com/blockcahin-big-data-146218.html

[4] https://blog.dataone.io/big-data-and-blockchain-c84c6c02544c

[5] https://www.forbes.com/sites/bernardmarr/2018/02/07/5-blockchain-opportunities-no-company-can-afford-to-miss/#9893de51a83d

[6] https://jaxenter.com/blockcahin-big-data-146218.html

[7] https://www.kdnuggets.com/2017/09/introduction-blockchain-big-data.html

[8] Casey M., Crane J., Gensler G., Johnson S., Narula N.: The Impact of BlockChain Technology on Finance: A Catalyst for Change, Geneva, International Center for Monetary and Banking Studies 2, 2018.

[9] https://www.datanami.com/2018/06/28/blockchain-solutions-usher-in-era-of-trusted-big-data/

[10] https://www.ibm.com/blockchain/industries/supply-chain

[11] https://blockchain.wtf/cryptocurrency-blockchain/erc20-tokens-projects/golem/

[12] https://www.inc.com/nicolas-cole/web-analytics-will-get-a-massive-improvement-with-blockchain-technology.html

[13] https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain/?utm_source=views&utm_medium=article06&utm_campaign=MITcompany&utm_content=banafa-jan07

[14] https://www.ey.com/Publication/vwLUAssets/EY-blockhain-in-insurance/$FILE/EY-blockhain-in-insurance.pdf

INVESTIGATION OF AWSCTD DATASET APPLICABILITY FOR MALWARE TYPE CLASSIFICATION

Doc. Nikolaj Goranin PhD.[1], Dainius Čeponis[1]
Vilnius Gediminas Technical University, Saulėtekio al. 11, 10223 Vilnius, Lithuania
dainius.ceponis@vgtu.lt

Abstract: *Nowadays, information systems security is a crucial aspect – vulnerable system endpoint can lead to severe data loss. Intrusion detection systems (IDS) are used to detect such unfortunate events. Implementation place defines the type of IDS: network-based (NIDS) for network traffic monitoring or host-based (HIDS), to detect malicious actions on the host level. IDS can be effective only if generated alerts are correctly evaluated and classified, what is typically done by a trained staff, but requires a lot of time and human resources. While a lot research is done with NIDS alerts evaluation, HIDS research is lacking behind. HIDS reported operating system calls could be used to define the importance of alarms and steer analysts to the most critical issues. In this article we demonstrate the applicability of our created Attack-Caused Windows System Calls Traces Dataset (AWSCTD), which is currently the most comprehensive dataset of system calls generated by almost all modern malware types, for training different classification methods on malware type recognition and later alert prioritization. The effectiveness of different classification methods is evaluated, and results are presented. Currently achieved results allow to decrease the load on analytical staff, dealing with malware classification and related alert prioritization by 92.4%, which makes this approach applicable for practical use.*

Keywords: HIDS, ALERT PRIORITISATION, MACHINE LEARNING, WINDOWS, SYSTEM CALLS

1. Introduction

With the significant growth of computer usage in daily tasks – computer systems security question raises naturally. It is important to detect the intrusion and react immediately to minimize the consequences of an attack. One of the first publication, describing the need of intrusion detection system as a component to protect infrastructure, was a United States Air Force report published in 1972 by James Anderson [1]. The report stated that IDS system can be used to minimize the amount of manual work that has to be done for log and audit data analysis – which is a time and personnel consuming task. Later, in 1985, the first real-time IDS based on expert-written rules, was presented [2]. There are two main types of IDS systems: network-based intrusion systems (NIDS) and host-based intrusion systems (HIDS). NIDS are deployed on the network level, but are not able to protect the company if intrusion was able to overcome it and reached the victim system by the means of malware, exploit, etc. HIDS is deployed on the host level and deals with the threats defined above.

Todays IDSes are more sophisticated than just use of a collection of well-crafted rules. Often, they use various machine learning (ML) methods to detect unauthorized entry or malicious activity. They incorporate three main detection methods [3]: anomaly-based, signature-based and hybrid. The anomaly-based method is good against Zero-day attacks but has a high false-positive rate. The signature-based method correctly detects known attacks, but new intrusions are often missed. The hybrid method combines the best practices of the other two. Manual security personnel work is still needed to adequately detect and classify and prioritize an intrusion. Each alert comes with a significant amount of data to be analyzed. The research about artificial intelligence (AI) and IDS merge conducted in 1994 stated that "a user typically generates between 3 - 35 Megabytes of data in an eight hour period and it can take several hours to analyze a single hour's worth of data" [4]. That amount of data much larger in the current version of IDS implementations: mainly because more information is gathered and increased traffic generated by a user.

In general, after IDS deployment, security analyst has not just to deal with the number of alerts but also with an extensive amount of data produced by those alerts. All that information has to be reviewed and analyzed making that task time-consuming and error-prone. Alerts count minimization and most critical attacks prioritization are the main approaches of the IDS management [5]. However, alerts amount minimization task is insufficiently analyzed for HIDS, and all the latest research and effort are focused on NIDS [5]–[8]. For that reason, in this paper we suggest using application generated system calls sequences as one of the components to classify the malware detected by HIDS that can be later used for alert importance prioritization. Alert that came from an application which has 92% similarity to Trojan must be reviewed before WebToolbar generated alert because of a different risk level caused by these malware type. Various ML methods, applied to the AWSCTD [9], which is currently the most comprehensive dataset of system calls generated by almost all modern malware types, were generating commercially acceptable accuracy level of more than 80%.

This paper is divided into two main sections. First, related work and information about IDS alert management are introduced. The second part will present AWSCTD usage for malware classification in the means of Windows OS system calls sequences: how the training is executed, what results is achieved and explanation of them. Finally, the conclusions are provided.

2. Related Work

A system call is an API used by the computer program to request a service from the kernel of the operating system: for opening a file, running a thread, writing to the registry or opening a network connection. Because of that origin (a primary artifact of the OS kernel), system call data is a very popular choice for malware research and detection.

The most simple and the cheapest by the meaning of computing power is the frequency-based features classification for intrusion detection. One of the latest approaches is the ADFA-WD dataset analysis. Authors of the dataset achieved the 72% intrusion detection rate on the preliminary analysis of dataset when Naïve Bayes Net were used as classifiers [10].

System call sequences are another popular method to represent features, which is costly but generates strong detection metrics [11]. The main idea is that system call is a "word" and sequences made of them form meaningful phrases. Since tasks of different application differ, that information can be used to classify them correctly (for example if it is a malware or legitimate application). Hidden Markov Models (HMM), Recurrent Neural Networks (RNN) and Convolutional Neural Networks (RNN) are the top ML methods used for this task type.

Two types of operations have been introduced, to solve the problem of IDS generated alerts classification [5]:

- *Low-level* (also called prioritization) operations deal with each alert individually to enrich its attributes or assign a score to it based on potential risk.

• *High-level* (also called aggregation) alert management techniques, such as aggregation, clustering, correlation, and fusion, were proposed to deal with sets of alerts and provide their abstraction.

Both techniques have some disadvantages. High-level suffers from including alerts that are not significant. That leads to inappropriate results and increased load. The main problem with low-level techniques is that they have to automatically examine all the generated alerts and prioritize them for further inspection, which also leads to improperly classified items [12].

In general, alert prioritization operations use information from various domains that can be gathered from the network. Security policy, network topology, vulnerability analysis of network services and installed software, as well as asset profiles are the mostly used factors affecting the prioritization of alerts [13]–[16]. The proposed systems use internal databases, which provide all required information about monitored network topology. The security analyst can manually manage databases or the system itself can automatically update them with the help of Nmap tool [17].

Some attempts were made to automate malware classification by system calls [18]. However, authors do not motivate that task from the point of view of further attack risk prioritization, and the size of malware dataset they used was twice smaller than in case of our experiments.

To enrich alert prioritization for the HIDS, we propose to use a system call sequences of executed applications as one of the determinants. System calls can be used to determine if the executed application belongs to one of the malware types, such as trojans, worms, bots, and ransomware, etc..

3. AWSCTD usage for the malware classification

AWSCTD was generated with the help of publically available malware collection from VirussShare.com site. Since malware can use code obfuscation and packers in order to hide from static analysis, we have used the dynamic malware analysis to gather data about malware behavior. Custom made system was specially implemented to collect system calls sequences on Windows 7 operating system [9].

The total of 5 malware families was selected from the dataset for our experiment. The main selection criteria – family should have more than 100 samples of unique family representatives and corresponding system calls sequences. Kaspersky provided family descriptor was used. Table 1. shows the number of unique malware samples in each family (“DangerousObject” category according to the Kaspersky: Malicious software is detected by KL Cloud Technologies. This verdict is used for samples that were not classified exactly.).

Table 1. *The number of each malware label.*

Label	Count
Trojan	1755
AdWare	4333
WebToolbar	618
Downloader	710
DangerousObject	105
Total:	**7521**

The different size of families represented helps us to evaluate the influence of the size of initial dataset on the accuracy of classification.

3.1 Feature preprocessing and selected ML methods

We are stating that it is enough to test the first batch off application system calls to determine its family. For that reason, the first 10, 20, 40, 60, 100, 200, and 400 system calls were used to generate the training and testing sets. The sample for 10 first system calls can be seen on Fig. 1. Every system call is represented by the unique number and sequence of these numbers forms the feature vector used for training.

```
@RELATION SystemCalls0010
@ATTRIBUTE SystemCall0  NUMERIC
@ATTRIBUTE SystemCall1  NUMERIC
@ATTRIBUTE SystemCall2  NUMERIC
@ATTRIBUTE SystemCall3  NUMERIC
@ATTRIBUTE SystemCall4  NUMERIC
@ATTRIBUTE SystemCall5  NUMERIC
@ATTRIBUTE SystemCall6  NUMERIC
@ATTRIBUTE SystemCall7  NUMERIC
@ATTRIBUTE SystemCall8  NUMERIC
@ATTRIBUTE SystemCall9  NUMERIC
@ATTRIBUTE class
 {Trojan,AdWare, WebToolbar,
  Downloader,DangerousObject}

@DATA
7,10,10,9,3,3,3,9,10,10,AdWare
7,10,10,9,3,3,3,9,10,10,AdWare
20,20,20,10,10,9,9,9,18,11,Trojan
7,10,10,9,9,9,3,3,3,9,AdWare
9,18,21,22,9,9,26,9,18,23,AdWare
29,19,2,13,31,1,2,28,28,33,Trojan
7,10,10,9,3,3,3,9,10,10,AdWare
```

Fig. 1. *WEKA data file fragment for the first ten system calls.*

A WEKA 3.8 data mining software was used to test various classification methods [19]. None of the WEKA provided default method values were changed or tinkered to achieve better results. Different type of Weka provided ML methods were selected to test the accuracy of malware type classification. Methods with the training values can be seen in Table 2.

Table 2. *Used ML methods with training parameters.*

Method	Training parameters
Bayes Net	-D -Q bayes.net.search.local.K2 -- -P 1 -S BAYES -E bayes.net.estimate.SimpleEstimator -- -A 0.5
Naïve Bayes Net	
Support Vector Machines	-S 0 -K 2 -D 3 -G 0.0 -R 0.0 -N 0.5 -M 40.0 -C 1.0 -E 0.001 -P 0.1 -model \"C:\Program Files\Weka-3-8\" -seed 1
Neural Networks	-L 0.3 -M 0.2 -N 500 -V 0 -S 0 -E 20 -H a
Decision Table	-X 1 -S \"BestFirst -D 1 -N 5\"
J48 (C4.5)	C 0.25 -M 2
LMT (Logistic Model Tree)	-I -1 -M 15 -W 0.0

3.2 Results and discussion

Classifiers were trained and tested with a 10-fold cross-validation technique. Cross-validation is a technique to evaluate predictive models by partitioning the original sample into a training set to train the model, and a test set to evaluate it. Our selected out of the box ML methods allowed to achieve results suitable for practical application. Almost all of them have achieved more than 80% off accuracy for the dataset with the best result of 92.4 by SVM. The percentage of correctly classified malware samples by different methods can be seen in Table 3.

Table 3. *Correctly classified percentage of instances.*

Feat. count	Bayes Net	Naïve Bayes	SVM	NN	Dec. Table	J48	LMT
10	**87.5**	61.6	89.4	87.2	88.1	88.5	89.1
20	73.8	60.9	89.4	87.8	88.0	88.8	89.2
40	74.3	61.7	91.6	88.5	89.4	90.7	91.0
60	75.0	66.1	91.8	90.2	89.3	90.9	91.2
100	75.4	61.8	**92.4**	**91.4**	90.0	**92.1**	**92.1**
200	76.1	68.2	89.8	90.3	90.0	91.9	91.8
400	75.9	**69.3**	87.5	84.8	89.7	92.1	92.1

The best results of classification are represented by the green color in the Table 3. The worst values are in red.

Worst results were obtained by using Bayes classification family: Bayes Net and Naïve Bayes Net. Naïve classification method produces the worst of all results: achieving only 69.8% of correct classification. SVM has achieved the best result of 92.4% with the 100 system call long feature vector. It is clear that 100 features vector is the most optimal subset to achieve more than 90% accuracy. Decision trees algorithms have also produced remarkable results for feature vector length of 100 and 400: it was even better than NN and had an accuracy of 92.1%. That is expected since already in 2008 the C4.5 decision tree algorithm was one of the best ten choices for the data mining [20].

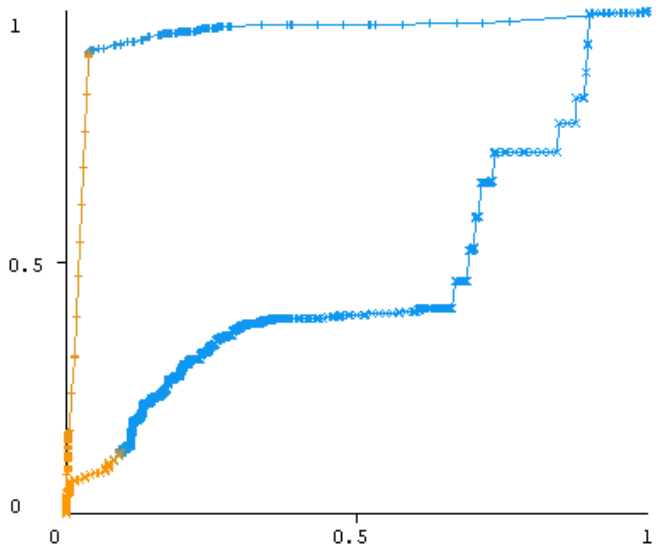


Fig. 2. *ROC curve of J48 (+) and Naive Bayes (x) classifiers. X-axis - False Positive Rate. Y-axis - True Positive Rate.*

Classification performance of J48 vs. Naïve Bayes can be seen on Fig.2. J48 area under ROC (AUC) (0.9486) is bigger than Naïve Bayes (0.4664). AUC of Naïve Bayes indicates that it produces worse results than random classification [21] which produces AUC of 0.5.

Obviously, the best classification results were obtained for malware families that had the biggest number of the samples. In this specific dataset that were Trojans and AdWare (1755 and 4333 samples respectively). Family "Dangerous object", a family with only 105 samples of in fact different types, has shown the lowest detection rate. SVM Confusion Matrix for the 100 features vector can be seen in Fig 3.

```
=== Confusion Matrix ===

    a    b    c    d    e   <-- classified as
 1672   73    0   10    0 |    a = Trojan
  152 4097    5   79    0 |    b = AdWare
    7   17  591    3    0 |    c = WebToolbar
   52   69    0  589    0 |    d = Downloader
  102    2    0    1    0 |    e = DangerousObject
```

Fig. 3. *SVM confusion matrix of the best result.*

When comparing training and testing execution times, decision trees have shown the best results. Both training and testing values are among the shortest. SVM and NN show the worst outcome, even though they produce only 1.3% and 0.3% better performance compared to J48 regarding accuracy. On the contrary NN is 24 times faster than SVM since they are trained, and testing stage is activated. Weka produced elapsed time for training and testing can be seen in Table 3 and Table 4.

Table 4. *Weka produced Elapsed_Time_training values.*

Feat. count	Bayes Net	Naïve Bayes	SVM	NN	Dec. Table	J48	LMT
10	0.05	0.01	1,3	8,4	0,4	0,1	14,2
20	0.07	0.01	1,9	17,2	0,9	0,2	21,1
40	0.09	0.02	3,8	46,3	2,8	0,4	40,2
60	0.29	0.04	4,8	90,4	4,2	0,8	69,2
100	0.31	0.06	7,5	222,4	5,5	1,4	106,6
200	0.93	0.12	16,8	938,3	16,0	3,2	301,0
400	3.61	0.28	40,6	4410,1	33,7	9,1	726,0

Table 5. *Weka produced Elapsed_Time_testing values.*

Feat. count	Bayes Net	Naïve Bayes	SVM	NN	Dec. Table	J48	LMT
10	0,003	0,009	0,130	0,002	0,002	0,005	0,003
20	0,002	0,017	0,184	0,002	0,003	0,000	0,002
40	0,003	0,031	0,309	0,009	0,000	0,002	0,003
60	0,011	0,041	0,396	0,009	0,002	0,003	0,000
100	0,019	0,078	0,586	0,024	0,000	0,000	0,003
200	0,045	0,154	1,303	0,094	0,002	0,000	0,006
400	0,100	0,454	3,098	0,413	0,005	0,000	0,016

The smallest amount of time is represented with the green color and the worst results for training and testing – with the red color.

All tests were performed on a system with an Intel i5-4670 3.40 GHz CPU. In comparison with the [18] used TITAN X GPU, it is a much slower device in the means of computation power. Also, we were using ML methods without any parameters optimization and much smaller features vectors for the training and testing, and, all system calls were used for the feature vector generation (authors of [18] have not included repetitive system calls from their dataset) which provide more information for the ML methods. All these differences let us achieve results that can be also used practically. That leads to the conclusion, that Deep Learning methods are an overhead for a task of this type – correctly classified instanced are over 90% and training time is more suited for the domain that generates new samples every day (model proposed by [18] has a training time that ranges from three to ten hours).

4. Conclusions

A theoretical approach to use malware generated systems calls sequences for IDS reported alerts prioritization was discussed in this paper. The new, Windows OS based malware generated system calls dataset AWSCTD was used to show the applicability of this

approach. Different types of ML methods were applied to classify malware by family. The results have showed that this approach could be used in practical applications – the best detection rate of 92.4 was obtained by using SVM with the 100 features vector. Comparable results were achieved by the use of decision tree algorithms: J48 and LMT. They generated 92.1% classification results. J48 has also showed the best training and testing times, that is very useful when new samples must be introduced for training. The obtained results of time needed for model training flicker, that deep learning or NN techniques are in fact superfluous for that specific task. Generated results suggest, that 100 first malware requested system calls is more than enough to achieve more than 90% classification accuracy, that are typically more than in enough for practical use. ML methods were used without any tinkering – with WEKA proposed default values. This implies for the future work, i.e. tuning configuration parameters for most perspective methods.

5. References

[1] J. P. Anderson, "Computer Security Technology Planning Study," October, vol. 2, no. 93, 1972.

[2] D. E. Denning and P. G. Neumann, "Requirements and model for IDES-a real-time intrusion detection expert system," Document A005, SRI International, vol. 333. 1985.

[3] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Commun. Surv. TUTORIALS, vol. 18, no. 2, 2016.

[4] J. Frank, "Articial Intelligence and Intrusion Detection : Current and Future Directions," Proc. 17th Natl. Comput. Secur. Conf., vol. 10, pp. 1–12, 1994.

[5] K. Alsubhi, E. Al-Shaer, and R. Boutaba, "Alert prioritization in Intrusion Detection Systems," NOMS 2008 - IEEE/IFIP Netw. Oper. Manag. Symp. Pervasive Manag. Ubiquitous Networks Serv., pp. 33–40, 2008.

[6] T. H. Nguyen, J. Luo, and H. W. Njogu, "An efficient approach to reduce alerts generated by multiple IDS products," Int. J. Netw. Manag., 2014.

[7] R. Shittu, A. Healing, R. Ghanea-Hercock, R. Bloomfield, and M. Rajarajan, "Intrusion alert prioritisation and attack detection using post-correlation analysis," Comput. Secur., vol. 50, pp. 1–15, 2015.

[8] C. M. Chen, D. J. Guan, Y. Z. Huang, and Y. H. Ou, "Anomaly network intrusion detection using Hidden Markov Model," Int. J. Innov. Comput. Inf. Control, vol. 12, no. 2, pp. 569–580, 2016.

[9] D. Čeponis and N. Goranin, "Towards a Robust Method of Dataset Generation of Malicious Activity for Anomaly-Based HIDS Training and Presentation of AWSCTD Dataset," Balt. J. Mod. Comput., vol. 6, no. 3, 2018.

[10] W. Haider, G. Creech, Y. Xie, and J. Hu, "Windows based data sets for evaluation of robustness of Host based Intrusion Detection Systems (IDS) to zero-day and stealth attacks," Futur. Internet, vol. 8, no. 3, 2016.

[11] T. R. Glass-Vanderlan, M. D. Iannacone, M. S. Vincent, Qian, Chen, and R. A. Bridges, "A Survey of Intrusion Detection Systems Leveraging Host Data," pp. 1–40, 2018.

[12] F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer, "A comprehensive approach to intrusion detection alert correlation," IEEE Trans. Dependable Secur. Comput., vol. 1, no. 3, pp. 146–168, 2004.

[13] R. Sadoddin and A. Ghorbani, "Alert correlation survey," in Proceedings of the 2006 International Conference on Privacy, Security and Trust Bridge the Gap Between PST Technologies and Business Services - PST '06, 2006, p. 1.

[14] B. Morin, L. Mé, H. Debar, and M. Ducassé, "M2D2: A formal data model for IDS alert correlation," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2516, pp. 115–137, 2002.

[15] P. A. Porras, M. W. Fong, and A. Valdes, "A mission-impact-based approach to INFOSEC alarm correlation," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2516, pp. 95–114, 2002.

[16] E. Chakir, M. Moughit, and Y. I. Khamlichi, "Building an Efficient Alert Management Model for Intrusion Detection Systems," vol. 3, no. 1, pp. 18–24, 2018.

[17] G. Lyon, "Nmap: the network mapper," Nmap.org, 2018. .

[18] B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, "Deep learning for classification of malware system call sequences," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9992 LNAI, pp. 137–149, 2016.

[19] I. H. Witten, E. Frank, and M. A. Hall, Data Mining: Practical machine learning tools and techniques. 2005.

[20] X. Wu et al., "Top 10 algorithms in data mining," Knowl. Inf. Syst., vol. 14, no. 1, pp. 1–37, 2008.

[21] T. Fawcett, "An introduction to ROC analysis," Irbm, vol. 35, no. 6, pp. 299–309, 2005.

DISTRIBUTED SENSING AS A NEW TOOL FOR FIBRE INFRASTRUCTURE PROTECTION

M.Sc. Munster P. PhD.[1,2], M.Sc. Horvath T. PhD.[1,2], M.Sc., M.Sc. Vojtech J. Ph.D.[1]
Department of optical networks – CESNET, the Czech Republic [1]
Faculty of Electrical Engineering – Brno University of Technology, the Czech Republic [2]

munster@cesnet.cz

Abstract: *Distributed fibre optic sensing is well known in defence or oil industry in use as acoustic sensing. Telecommunication networks are threatened by fibre cuts mainly caused by digging activity or theft. Many network operators seeking appropriate solution for self-protecting infrastructure system. Most commercially available solutions of distributed sensing systems allow sensing only on dedicated fibres. Sharing the same infrastructure for data transmission and sensing is, however, more advantageous. On the other hand, it is necessary to solve the possible interaction of both services and thus the interference. We have developed our own sensing systems and we have made several measurements to evaluate the suitability of the most widely used distributed sensing techniques - interferometric, reflectometry and polarization for using in existing data infrastructures on optical fibres with active data traffic.*

Keywords: DISTRIBUTED SENSING, FIBRE INFRASTRUCTURE PTROTECTION, INTERFEROMETRY, POLARIZATION, REFLECTOMETRY, NREN

1. Introduction

Fibre optic infrastructure is essential for all data transmissions because optical fibre is only medium which can satisfy requirements for large bandwidth, high speed, low insertion loss, low cost, and which allows signal multiplexing. Fibre optic infrastructure may be threatened by digging activity which causes an interruption of a signal transmission and also additional costs. Protection of fibre infrastructure may save not only costs but also time necessary for repairs and increase quality of the network, on the other hand.

National research and education networks (NREN) like CESNET (Czech National Research and Education Network) transfer except standard data also non-data services such as precise time or stable frequency. Distributed sensing is a new and highly demanded service which enables secure of fibre infrastructure itself on one hand, and for example, monitoring of seismic activity, train positions, or aircraft landings, on the other hand.

Structure of this paper is follows. Section 1 provides an introduction. Section 2 shortly describes basics of distributed sensing systems. In Section 3 we present some measurement results and Section 4 concludes the paper.

2. Distributed sensing

Distributed fibre optic sensing is known for a long time, but rapidly decreasing costs of main components increase their availability. The paper describes the most used techniques and compare their sensitivity and suitability for use in fibre infrastructure protection.

Fibre-optic interferometers

The light interference is used in many fields of industry for a precision measurement. For acoustic or mechanical vibrations detection mainly two basic configurations are being used – the Mach-Zehnder and the Michelson interferometers. Both configurations mostly use two optical fibres – one is a reference arm and second one is a sensing arm. Except high sensitivity their big advantage is very fast response and possible multiplexing thanks to use of narrow linewidth lasers and relatively low output power. On the other hand, localization of event is complicated and mostly combination of two techniques is necessary which is also associated with the requirement for a special demultiplexing [1].

Main application of interferometers is perimeter securing thanks to the costs of these systems.

Polarization based sensing

Special group of interferometers are polarization interferometers. Standard single mode fibre supports two degenerate modes of orthogonal polarizations. The polarization state of light in a single-mode optical fibre is very similar to that of a plane light wave in free space. It could be linear, circular, or elliptical. Whereas the polarization state is influenced by temperature or strain we can evaluate the polarization changes and based on this we can obtain information about an event [2].

Sensitivity of polarization interferometers is not so high compare to standard dual path interferometers mentioned above however the lower sensitivity can be advantage in use for fibre infrastructure protection because standard telecommunication fibres are always terminated in central offices where are many sources of vibrations resulting in noise.

Phase sensitive OTDR

Optical time-domain reflectometry (OTDR) is being widely used in telecommunications for detection faults in fibre optic networks. Since laser linewidth is relatively broad (GHz to THz) it is not possible to detect local changes caused by temperature or acoustic vibrations. Using an ultra-narrow linewidth laser enables detection of refractive index changes in the optical fibre caused by external events. These systems are knowns as φ-OTDR or DAS (Distributed Acoustic Sensing) and are mainly use for pipeline security or long perimeter intrusion detection. Ing. Fig. 1 is photo of our own developed system.



Fig. 1 *CESNET modular phase OTDR.*

3. Measurement results

In this part we present some measurement results from distributed sensing systems. First, interferometry-based sensing system is evaluated. Fig. 2 shows measurement when walking around the cable lying on the floor in our laboratory. Total length was about 10 km.

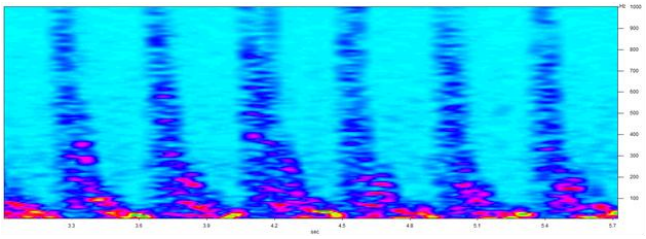


Fig. 2 *Interferometry system. Calculated spectrograph, walking.*

The response of the system was good and detected very small events. However, there were no other sources of noise which can influence the measurement. The second measurement was made in a real network on fibres leading across the Brno city. The signal was noisy but still strong events like for example touching the fibre caused strong response of the system. Fig. 3 shows spectrograph of the received signal when knocking the cable.

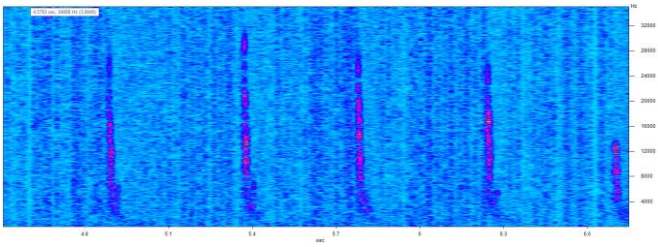


Fig. 3 *Interferometry system. Calculated spectrograph, knocking the cable.*

In case of polarization sensitivity of the system was lower. In Fig. 4 is depicted Poincar sphere and state of polarization change caused by shaking the fibre in laboratory conditions. Although the response of the system seems to be high enough it is necessary to realize that it is really a shaking with a cable. Response of the system on vibrations near the cable is show on Fig. 5. [3]

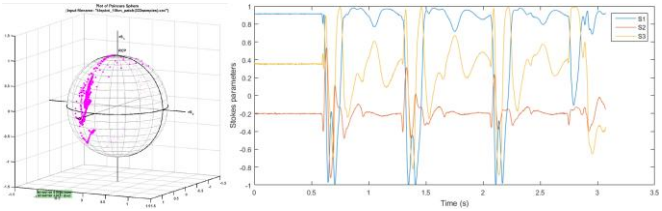


Fig. 4 *SOP change caused by shaking the fibre. L: the Poincar sphere, R: Stokes parameters.*

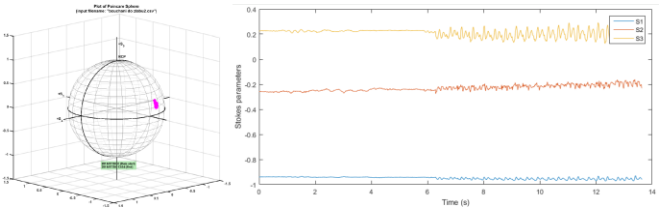


Fig. 5 *SOP change caused by shaking the fibre. L: the Poincar sphere, R: Stokes parameters.*

We also tried to compare sensitivity of both systems mentioned above. In experimental measurement described in [1] the same conditions were applied. Both systems measured correctly the set frequency 1025 Hz, but power levels were different, as can be seen in Fig. 6. While intensity for interferometry-based system was −28 dB in case of polarization system the peak was about 55 dB lower, about −83 dB.

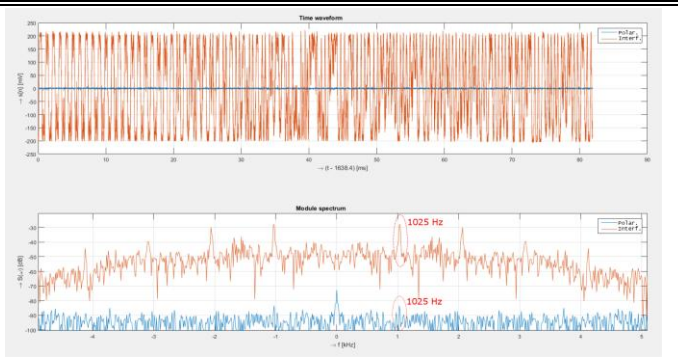


Fig. 6 *Received signals from both sensing systems (interferometer – red signal, polarization – blue signal) and their spectra (below) for 1025 Hz.*

The last system is a phase sensitive OTDR and it is the most complex setup with a very difficult signal post-processing. Moreover, since the back-reflected signal is very weak it is necessary generate high power pulses which can influence other signals in the fibre if WDM is applied. On the other hand, the system enables single-end measurement with precise localization of event. Fig. 7 shows waterfall plot from the fibre where the detected event is located at 61 km from the beginning.

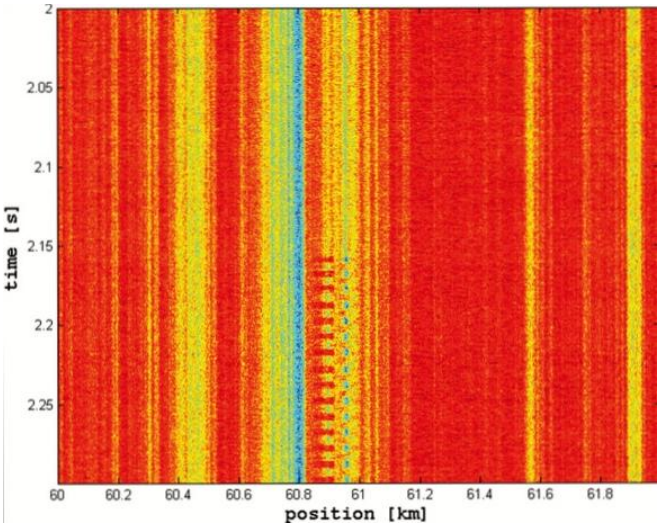


Fig. 7 *Waterfall plot from phase sensitive OTDR.*

Table 1 lists basic comparison of distributed sensing systems. For all systems only, basic configuration is considered to allow for a suitable comparison [4].

Table 1: *Comparison of distributed sensing systems.*

	Phase sensitive OTDR	**Polarization based sensing**	**Interferometers**
Sensitivity	++	+	+++
Number of required fibres	1	1	2
Single-ended measurement	Yes	No (passive mirror at least)	No (passive mirrors at least)
Measurement range	Tens of km	Tens of km	Tens of km
Localization of event	Yes	No (in basic configuration)	No (in basic configuration)
Price	High	Low	Moderate

Special requirements	Elimination of reflections in optical route, channel spacing >200 GHz away from data.

Conclusion

We presented description and comparison of interferometric, polarization and reflectometry sensing systems in both, laboratory and real conditions. Interferometry-based system has great sensitivity however in the real network the received signal is very noisy, and it is very difficult to extract useful information. Polarization system sensitivity is lower and detects only mechanical vibrations however the signal is not so noisy and hence the post-processing is easier. The best results can be obtained using phase sensitive OTDR. Compare to previous systems enables also localization. Unfortunately, because of its complex setup, complicated post-processing and high costs this system is unusable for fibre infrastructure protection.

Acknowledgments

Research described in this paper was financed by the Ministry of Interior under grant no. VI20152020045. This work was also partially supported by project E-Infrastructure – Modernization, Registration number CZ.02.1.010.00.016_0130001797 and by the National Sustainability Program under grant LO1401.

References

[1] Munster P. Comparison of interferometry based and polarization based sensing systems for use in fibre infrastructure protection. In *2017 International Workshop on Fibre Optics in Access Network (FOAN)*, pages 1-3, Nov 2017.

[2] Wolifiski T.R. Polarization Properties Of Optical Fibres. In *International Conference On Transparent Optical Networks (Cat. No. 99Ex350)*, 61-. IEEE. doi:10.1109/ICTON.1999.781845.

[3] Munster P. Distributed Sensing Based on Interferometry and Polarization Methods for Use in Fibre Infrastructure Protection. In *6th International Symposium on Sensor Science (I3S 2018) 06/08/2018-08/08/2018, Kenting*, 2018.

[4] Vojtech J. Proactive protection of DWDM infrastructures. In *ECOC conference*, Rome, *2018*.

TRIBOLOGICAL PROCESSES EVALUATION DUE TO BULLET-RUBBER CHOPPER WHEEL INTERACTION PHENOMENA

АНАЛИЗ НА ТРИБОЛОГИЧНИТЕ ПРОЦЕСИ ПРОЯВЯВАЩИ СЕ ПРИ ПРЕМИНАВАНЕТО НА КУРШУМ ПРЕЗ ГУМЕН ОБТЮРАТОР

M.Sc. Ing. Dimitrova Ya.
Faculty of "Artillery, air defense and CIS" – National Military University "Vasil Levski", Veliko Tarnovo, the Bulgarian Republic

dimitrovax2yana@gmail.com

Abstract: *Due to the complexity of anti-terrorist operations the use of special firearms' equipment is necessary. Part of this special equipment is the silencers and on the other hand the special ballistic protection equipment. That requires research of the tribological characteristics' while shooting with small arms and silencer influence which is the purpose of that report.*

Keywords: SMALL ARMS, SILENCER, TRIBOLOGY.

1. Introduction

With the development of information technologies terrorist organizations skillfully decentralize their structures, infiltrating the democratic society and diversify their tactics making it difficult to neutralize them. Fight against terrorist organizations requires a change in the traditional perceptions of military action and tactical use of firearms.

Due to the complexity of anti-terrorist operations it is necessary to use special equipment for the firearms. Major element of the special equipment used for firearms are the silencers. They allow the shot's noise suppression. In addition the use of special equipment for individual ballistic protection requires weapons with high efficiency.

The survey upon the available literature reveals that silencers affect the deviation of grouping and the mean point of impact (MPI). But there is no information about tribological processes influence due to bullet interaction with elements of the silencer.

Based on the paragraphs above and to evaluate tribological processes due to bullet-rubber chopper wheel interaction phenomena in this report friction between polymers and solid materials are scrutinized.

The report's subject is the PBS-1 which is a chamber type silencer with rubber chopper wheel.

2. Tribological processes evaluation due to bullet-rubber chopper wheel interaction phenomena

2.1. Purpose: Evaluation of tribological processes due to bullet-rubber chopper wheel interaction.

2.2. Tasks:

- to identify the tribological processes that emerge from friction processes between polymers and solid materials;

- to develop a mathematical model of the tribological processes that emerge from friction processes between polymers and solid materials.

3. Results of discussion

It is necessary to identify the tribological processes that emerge from friction processes between polymers and solid materials in order to develop a mathematical model.

3.1. Identification of tribological processes that emerge from friction process between polymers and solid materials

As a result of the shot phenomenon and the structure of firearm barrels, bullet receives a progressive and rotation motion. The rotation motion stabilizes bullet during flight and the progressive motion gives him the necessary speed.

During shooting with fitted chamber type silencer PBS-1 after leaving the barrel bullet collide with the rubber chopper wheel. While bullet paste out rubber chopper wheel the following tribological processes reveal:

- sliding friction;
- rolling friction;
- gas flow influence;
- polymer adhesion;
- wear of polymer.

These tribological processes alter the initial velocity and rotation motion of bullet. Variation of initial velocity and rotation leads to changes in bullet trajectory and impact point.

Fig. 1 presents a scheme of the input and output information variables, which changes due to the influence of the tribological processes while the bullet passes through the elements of the silencer.

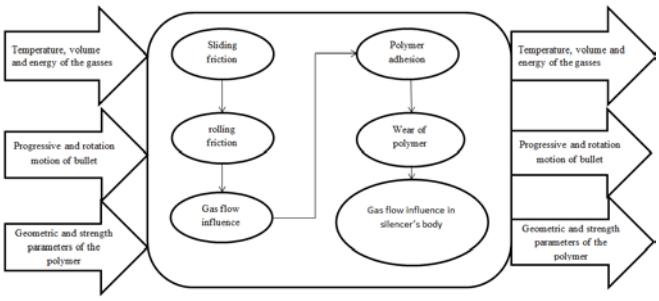


Fig. 1 *Scheme of the variables and tribological processes due to bullet-rubber chopper wheel interaction phenomena.*

Tribology looks upon the material body like surface layers with a multitude of micro- and macro-roughness which depend of the nature of solids, the method and precision of surface preparation. Properties of solid surfaces are crucial to surface interaction because they affect real area of contact, friction, wear, and lubrication.

The frictional force is the relative movement of one body against another due to the contact of the materials roughness.

Fig. 2 graphically presents some variables and forces which influence on bullet while passed out the rubber chopper wheel.

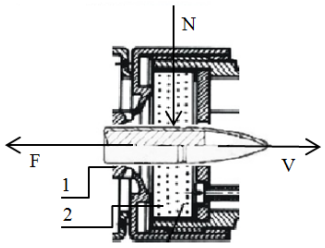


Fig. 2 *Graph of the bullet passing out a rubber chopper wheel.*

1 – muzzle cut of the barrel; 2 – rubber chopper wheel.

External surfaces exist only in solid and liquid phases since the gas phase has no own volume. From fluid dynamics it is certain that the bodies moving in fluid flow receive a frictional resistance which is caused by the occurrence of internal friction and fluid vortexing behind the body. Force of internal friction counteracts of the body and part of the mechanical energy converts into the energy of the vortex. Last one under effect of friction force convert into internal energy of the environment.

3.2. Developing a mathematical model of the tribological processes, that emerges from friction processes between polymers and solid materials.

Bullet acceleration changes due to frictional force, which is a result from friction process while bullet passed through rubber chopper wheel and silencer's body. Force of friction equals sum of two forces, adhesion force F_a and sliding friction force T, using following formula:

$$(1)\ F = F_a + T$$

Sliding friction force T can be calculated using following mathematical apparatus:

$$(2)\ T = (\mu . HB . Sr) + \left(\eta . S_a . \frac{\upsilon}{h}\right) + \left(f . \frac{N}{R}\right)$$

where:

- μ – coefficient of friction while sliding;
- f – coefficient of friction while rolling;
- HB – Brinells' hardness of softer bodies;
- S_a – nominal area of contact, it is the surface of bullet;
- Sr – real area of contact;
- η – viscosity of gasses;
- $\frac{\upsilon}{h}$ - gradient of velocity;
- N – normal load;
- R – bullet's radius.

Real area of contact is determined by:

$$(3)\ Sr = \eta . S_a$$

Adhesion is the phenomenon that occurs when two surfaces are pressed together, either under a pure normal force (load) or under combined normal and shear forces. To pull the two solids apart is requires a finite normal force, called adhesive force. To calculate the adhesion force F_a it is use following formulas:

$$(4)\ F_a = \sigma . A_r$$

where:

- σ – tensile strength or resistance of material that can bear until it is fracture;
- A_r – initial cross-section area of whole micro compound.

Tensile strength is determent by:

$$(5)\ \sigma = \mathrm{E} . \varepsilon$$

where:

- E – elastic module of the polymer ;
- ε – resistance of polymer deformation or Brinells' hardness.

The initial cross-section area of whole micro compound for polymer adhesion is determined by following equation:

$$(6)\ A_r = S_a \left[1 - k_1 . e^{-\delta\left({}^{N^*}/_{S_a . E}\right)^{2/3}}\right]$$

where:

- $k_1 = 0{,}8 \div 1$ – coefficient of polymer friction;
- δ – the total displacement (normal approach);
- N^* – resulting load.

The normal approach is determined by the fowling equation:

$$(7)\ \delta \cong 1{,}2 \left(\alpha\, {}^{R}/_{R_z}\right)^{1/3}$$

where:

- R_z – height of cross-section roughness;
- α – adhesion parameter.

Adhesion parameter is defined as:

$$(8)\ \alpha = {}^{n_o}/_{n_m}$$

where:

- - n_o – average roughness number;
- - n_m – roughness per unit nominal area.

For computing resultant load on the normal load it is adding adhesion pulling, using following mathematical apparatus:

$$(9)\ N^* = \mathrm{N} + \mathrm{N}_a = \iint_{S_a} q . dS_a$$

where: q – intensity of contact pulling; N_a – adhesion pulling.

Intensity of contact pulling can be calculated using following equation:

$$(10)\ q = \mu . p_a . V . \frac{S_a}{S_r}$$

where: p_a – contact tension; V – initial velocity of bullet.

The contact tension is determined by:

$$(11)\ p_a = \frac{N_a}{S_a}$$

Bullet rotation velocity changes due to torque friction, which is a result from bullet rolling and sliding around the opening in rubber chopper wheel. Torque friction can be calculated using formula:

$$(12)\ \mathrm{M_T} = \left(\frac{2.\pi.\eta.\omega.R^3.L}{h}\right) + (F.R)$$

where:

- L – bullet's length;
- h – gap between bullet and rubber chopper wheel.

Consequently repeated surface and subsurface tensions, generated by contact areas, result in forming of wear particles, which alters after each consequent shot and gradually fracture the material. The wear changes value of frictional force, with which initial velocity and rotation motion of bullet are altered. The wear of rubber chopper wheel arises from consequently repeated elastic-plastic deformation's actions. For calculating the wear, formulas for elastic-plastic deformation are used from reference [2].

The wear due to sliding is generated from continuously colliding one body against another during sliding. Continuously repeated impact of a bullet against rubber chopper wheel might lead to exhaust of subsurface structure of polymers. Bullet's impact force on rubber chopper wheel can be calculated using formula:

$$(13)\ F_{(t)} = F_0 . sin\left(\frac{\pi . t}{t_i}\right)$$

where:

- t – a time bullet require to pass the rubber chopper wheel;
- t_i - a time bullet require to pass the rubber chopper wheel starting from muzzle cut;
- F_0 – maximum impact force.

Maximum impact force F_0 remains almost the same, but impact force $F_{(t)}$ changes due to the wear of rubber chopper wheel from continuous shooting, determine by using following formula:

$$(14)\ F_0 = \left(\frac{5}{3}.m.V^2\right)^{3/5}.\left[\frac{4.\epsilon}{3.(1-\upsilon^2)}.R^{1/2}\right]^{2/5}$$

where: m – bullet's mass; υ – wear's volume after consequent shooting.

Wear's volume for whole surface can be calculated by:

$$(15)\ \upsilon = \frac{k.m.V^2}{2.\mu.HB}$$

where: k – coefficient depending on surface's roughness of contacting materials.

The wear's depth is determined by following mathematical apparatus:

$$(16)\ d = k.p.V\left(\frac{1}{HB} + \frac{1}{E^*.\left(\sigma_p/R_p\right)^{1/2}}\right)$$

where:
- p – expected normal tension;
- E^* – effective modulus of elasticity;
- σ_p – standard deviation of roughness ;
- R_p – height of roughness (distance between the highest and the mean line of asperity).

Normal tension can be calculated by:

$$(17)\ p = \frac{N}{S_a}$$

Length c of lateral cracks is calculated by:

$$(18)\ c = \alpha_1.\left[\frac{\left(\epsilon/HB\right)^{3/5}}{K_c^{1/2}.HB^{1/8}}\right].N^{5/8}$$

where:
- α_1 – constant depending on the asperity shape;
- ϵ – dimensionless erosion ratio;
- K_c – resistance to fracture.

Erosion ratio can be calculated using fowling mathematical apparatus:

$$(19)\ \epsilon = \frac{k\rho V^2}{2H}$$

where: ρ – the density of the material being eroded.

Depth d_c of lateral cracks is calculated by:

$$(20)\ d_c = \alpha_2\left(\frac{\epsilon}{HB}\right)^{2/5}\left(\frac{N}{HB}\right)^{1/2}$$

where: α_2 – another constant depending on the asperity shape.

Wear's volume v_c after consequent shooting is determined by following mathematical apparatus:

$$(21)\ \upsilon_c = \alpha_3.N\frac{\left(\epsilon/HB\right).N^{9/8}}{K_c^{1/2}.\varepsilon^{5/8}}$$

where: α_3 – another constant depending on the asperity shape.

4. Conclusions

1. Identification of tribological processes that emerge from friction process when bullet passes through the elements of the silencer PBS-1 show the complexity of the friction forces. The developed mathematical model of tribological processes presents a mean for determination the influence of friction forces.

2. The conducted research gives information of friction forces and a bullet speed dependency. From that analyze it can be predicted how to improve the bullet speed with reduction of the tribological process.

REFERANCES:

1.Беркович И.И., Громаковский Д.Г., Трибология. Физические основы, механика и технические приложения., Самара, 2000.

2.Bhushan B. Introduction to Tribology, 2nd Edition, USA, 2013.

3.Кирилов В. М. Основи за устройството и проектирането на стрелковото оръжие. София: ДВИ, 1975.

4. Министерство обороны СССР, Прибор для беззвучной и беспламенной стрельбы из 7,62 мм модернизированных автоматов калашникова (АКМ и АКС). Руководство службы (Издание второе), М, 1972.

5. Кандева-Иванова М., Цикъл лекции по инженерна трибология.

6. Цонев Ц. Г., Давидов К. С., Основи за устройството на стрелковото оръжие – част I, Ш., 2013.

EVALUATION METHOD OF THE ARTILLERY'S EFFECTIVENESS AGAINST UNITARY TARGET

МЕТОД ЗА ОЦЕНКА НА ЕФЕКТИВНОСТТА НА АРТИЛЕРИЯТА СРЕЩУ ОТДЕЛНА ЦЕЛ

M.Sc. Ing. Katsev I., Assistant
Faculty of "Artillery, air defense and CIS" –National Military University "Vasil Levski", Veliko Tarnovo, the Bulgarian Republic

katsev.i@abg.bg

Abstract: *Artillery is major land forces' combat element, which enforces firepower against enemy units in operations. Artillery's effectiveness heavily depends on how accurate will be weapon delivery, which is a function of dependent and independent errors related to weapon-target interaction and how much will be artillery shell's lethality.*

Keywords: Damage probability, Carleton damage function, Unitary target.

1 Introduction

Artillery is a major combat element of the land component for engaging various enemy targets located in the area of operation. The main content of the combat use of artillery formations is fire support. Fire support is one of the main battle functions and represents firepower enforcement by using the fire of weapon systems in artillery formations. The main job of the artillery is to minimize the combat potential of the enemy group and to limit its capabilities in battle. The success of operation depends heavily on the effectiveness of fire support, which in turn depends on the effectiveness of the forces involved in the fire support. As the primary tool of the ground component involved in fire support, artillery plays a vital role in achieving and retaining fire superiority in the operation.

Artillery formations conduct fire tasks against different enemy targets and objects. Targets and objects in the opposing force in operations can be generally divided into unitary and area targets. To fulfill the purpose of this study, we will focus on the unitary targets and an evaluation method of the artillery's effectiveness against unitary targets.

The efficiency of artillery fire against unitary target depends mainly on the probability that the target will be damaged or destroyed. This probability changes as a result of the deviation in the distance and direction of the mean point of impact from the target center (aiming point). Deviations in distance and direction are caused by a number of random errors associated with the specificity of the work of the artillery formations in the preparation of fire data, such as miscalculation of latitude, longitude, distance, wind effect, or uncertainty in target's locating . Random errors are typically divided into two groups. First ones are the repetitive errors. They are repeatable for all shots and these errors are associated with inaccuracies in the targeting due to errors in the calculation of the fire position, observation post and target locations, errors in aiming the weapon systems, errors in determining the meteorological and ballistic conditions, and others. The second type of random errors are the non-repetitive errors, which refers to ballistic projectile errors caused by variations in the shape of the ammunition, the angle of projectile discharge, the amount of gunpowder used in the shells and others.

2. Artillery fire effectiveness determination.

2.1. **Purpose:** Presenting a theoretical evaluation method for the artillery's effectiveness against unitary target.

2.2. Objectives:

- to determine standard deviation of random errors regarding weapon systems accuracy;

- to determine the weapon lethal area and damage function;

- to determine artillery fire effectiveness against unitary target.

The model for assessing the efficiency of damage from fire systems is based on determination of a precision function and a damage function.

The accuracy function depends on the repetitive errors in the fire data preparation. These errors can be represented by a range error probable and deflection error probable as a quantum of random errors. Those random errors are normally distributed and independent from each other.

$$(1)\quad E_x = \sum_{i=1}^{n} E_{x_i}$$
$$(2)\quad E_y = \sum_{i=1}^{n} E_{y_i}$$

where E_{x_i} and E_{y_i} - random error of i-th element, i - elements involved in the fire data preparation, E_x and E_y – repetitive errors in range and defection direction.

Errors due to ballistic dispersion occur for each round fired from weapon systems and may be denoted by E_{d_x} for random dispersion error in range and E_{d_y} random dispersion error in deflection.

In order to determine the efficiency of artillery fire from closed fire positions against unitary observable ground targets, standard deviation of errors is used and according to the normal distribution law, the standard deviation is calculated by following formulas:

$$(3)\quad \sigma_{mpi_x} = \frac{E_x}{0.6745}$$
$$(4)\quad \sigma_{mpi_y} = \frac{E_y}{0.6745}$$
$$(5)\quad \sigma_{d_x} = \frac{E_{d_x}}{0.6745}$$
$$(6)\quad \sigma_{d_y} = \frac{E_{d_y}}{0.6745}$$
$$(7)\quad \sigma_x = \sqrt{{\sigma_{mpi_x}}^2 + {\sigma_{d_x}}^2}$$
$$(8)\quad \sigma_y = \sqrt{{\sigma_{mpi_y}}^2 + {\sigma_{d_y}}^2}$$

where σ_{mpi_x} and σ_{mpi_y} – standard deviations or repetitive errors in preparation of fire data, σ_{d_x} and σ_{d_y} – standard deviations or non-repetitive errors due to ballistic dispersion, σ_x and σ_y – standard deviations of the sum of standard deviations of errors due to normal distribution law.

The damage function determination depends on the power of the weapon systems, the artillery shells and type of the target. The damage function of a fragmentation projectile is represented by the Carleton damage function. To determine the power of the weapon systems and the impact of the projectiles on the target, we calculate the lethal area of the target from a single round by:

Carleton damage function is used for calculating fragmentation lethal area of an artillery shell with basic data considered for projectile mass, caliber and amount of shrapnel. The damage function also consider impact angle and output data is effective weapon area:

$$(9)\quad a = 1 - 0.8 * cos\,\theta$$
$$(10)\ S_r = \sqrt{AL * a}$$
$$(11)\ S_d = \frac{S_r}{a}$$

where a - impact angle coefficient, θ - impact angle, AL - target lethal area, S_r - effective weapon length,S_d - effective weapon width.

In some cases, unitary targets require a hit by single shot to be destroyed, that demands the single sortie probability of damage to be determine. This probability is calculated by using the cumulative function of the normal distribution by the formulas:

$$(12)\ P_x = 2 * \left(normcdf\left(\frac{S_r}{2}, 0, \sigma_x\right) - 0.5\right)$$
$$(13)\ P_y = 2 * \left(normcdf\left(\frac{S_d}{2}, 0, \sigma_y\right) - 0.5\right)$$
$$(14)\ P_{hit} = P_x * P_y$$

where P_x - probability of damage in range direction, P_y - probability of damage in deflection direction, P_{hit} - single sortie probability of damage.

The probability of damage due to the number of shots, fired from weapon systems is determined by the formula:

$$(15)\ P_{=1}^{k} = 1 - (1 - P_{hit})^n$$

where $P_{=1}^{k}$ - the probability of damage after firing the n shots, n - number of shots fired.

Some targets require more than one hit to be damaged, such targets must be struck by a certain number of shots to be destroyed, so we have to determine the probability of the target being hit by the minimum number of rounds necessary for its destruction. For this purpose we use the cumulative function of binomial distribution:

$$(16)\ P_{\geq 1}^{k} = 1 - binocdf(u - 1, n, P_{hit})$$

where $P_{\geq 1}^{k}$ - probability of damage, u - number of hits required for target destruction.

3. Results and discussion;

In this section we are going to examine an example of a case study of artillery engaging unitary target and the effectiveness of artillery fire against that target.

Example: We are given - random errors in range $E_x = 20m$ and deflection $E_y = 10m$, ballistic dispersion in range $E_{d_x} = 20m$ and deflection $E_{d_y} = 10m$, target lethal area $AL = 300m^2$, impact angle $\theta = 45^o$and number of shots fired $n = 20$**.**

The solution of the task is initialized by calculating the quadratic deviations of the random errors due to the errors in the preparation and the dispersion.

$$\sigma_{mpi_x} = \frac{E_x}{0.6745} = \frac{20}{0.6745} = 29.7m$$
$$\sigma_{mpi_y} = \frac{E_y}{0.6745} = \frac{10}{0.6745} = 14.8m$$
$$\sigma_{d_x} = \frac{E_{d_x}}{0.6745} = \frac{20}{0.6745} = 29.7m$$
$$\sigma_{d_y} = \frac{E_{d_y}}{0.6745} = \frac{10}{0.6745} = 14.8m$$
$$\sigma_x = \sqrt{{\sigma_{mpi_x}}^2 + {\sigma_{d_x}}^2} = 41.9m$$
$$\sigma_y = \sqrt{{\sigma_{mpi_y}}^2 + {\sigma_{d_y}}^2} = 20.9m$$

After calculating the accuracy, the damage effect of weapon systems needs to be determined. Fragmentation lethal area calculations results in the following:

$$a = 1 - 0.8 * \cos\theta = 0.58$$
$$S_r = \sqrt{AL * a} = 13.2m$$
$$S_d = \frac{S_r}{a} = 22.7m$$

The probability of damage due to mistakes in preparation and dispersion will be determined by the formulas:

$$P_x = 2 * \left(normcdf\left(\frac{S_r}{2}, 0, \sigma_x\right) - 0.5\right) = 0.125$$
$$P_y = 2 * \left(normcdf\left(\frac{S_d}{2}, 0, \sigma_y\right) - 0.5\right) = 0.413$$
$$P_{hit} = P_x * P_y = 0.052$$

From the calculations above, it is clear that the single shot has $\mathbf{5.2}\%$ probability to damage the target.

$$P_k = 1 - (1 - P_{hit})^n = 0.653$$
$$P_{\geq 1}^{k} = 1 - binocdf(u - 1, n, P_{hit}) = 0.276$$

20 shots fired results in $\mathbf{65,3}\%$ probability that a single shot hits the target, while the probability of two shots hits the target is $\mathbf{27.6}\%$.

Table 1: *Case studies for different occasions, which shows probability of damage changing due to errors, rounds and lethal area parameters change.*

PARAMETERS	CASE STUDY				
	1 base line	2	3	4	5
#Rounds	20	**10**	20	20	**30**
Random errors in range, m	20	20	**40**	20	**30**
Random errors in deflection, m	10	10	**20**	10	**15**
Ballistic dispersion in range, m	20	20	**40**	20	**30**
Ballistic dispersion in deflection, m	10	10	**20**	10	**15**
Target lethal area, m^2	300	300	300	**600**	**450**
Probability of damage, %	65.3	41.1	23.6	87.3	65.6
Probability of two hits, %	27.6	9.1	3	59.7	28.3

Table 1 show how the probability of damage changes because of variation of random errors in preparation, dispersion errors, number of rounds and target lethal area. Knowledge about evaluation method characteristics and probability of damage alteration plays a significant role in achieving firepower enforcement against unitary target.

4. *Conclusion*

Probability of damage is primary factor to be taken into account when evaluating artillery formations' combat effectiveness. There also can be calculated inverse task, determining artillery shells expenditure for achieving certain amount of probability for damaging opposing forces' targets and objects.

Determining probability of damage against enemy targets in operation is a major factor in planning the forces' battle actions in combat domain. The ratio of forces and resources, expenditure of munitions and the efficiency of fire support are essential elements to be taken into account by the commander when deciding combat operation scenario.

REFERENCES:

1. Chusilp, P., Charubhun, W., Koanantachai, P., Monte Carlo Simulations of Weapon Effectiveness Using Pk Matrix and Carleton Damage Function, International Journal of Applied Physics and Mathematics, vol4, pp 280-285, 2014.

2. . Driels, M., Weaponeering: Conventional Weapon System Effectiveness - 2nd Edition, American Institute of Aeronautics and Astronautics (AIAA), Education Series, Reston, 2014.

3. Eckler A., Burr S., Mathematical models of target coverage and missile allocation, Military operations research society, 1972.

4. Klopcic J., "A comparison of damage functions for use in artillery effectiveness codes", Technical report, Ballistic research laboratory Aberdeen proving ground, Maryland, 1990.

5. Washbur A., Notes on firing theory, Naval postgraduate school, Monterey, California, 2002. Washburn A., Diffuse-Gaussian multiple shot patterns, Military operations research, vol8, n3, 2003.

EXPERIMENTAL DEVELOPMENT OF A SMART ARTILLERY AND MINE ORDNANCE FUZE BASED ON ARDUINO MICROCONTROLLER PLATFORM

Cad. Dimitrov Mir.*, Assoc. Prof. Ing. Ganev V. PhD.**,M.Sc.Ing. Dimitrova Ya.***
Faculty of "Artillery, air defense and CIS" –National Military University "Vasil Levski", Veliko Tarnovo, the Bulgarian Republic

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

Abstract: *Today's battlefield is ever-changing in terms of weaponry demands and engagement criteria. Older artillery ordnance is often struggling to meet the modern battlefield demands and does not provide the operator with a wide range of capabilities. This combination of constraints coupled with the performance of conventional artillery munitions has often limited the commander's options and decreased the effectiveness of artillery. Meeting the modern battlefield demands requires the performance and capabilities of existing ordnance to be increased. This paper researches the creation of a smart fuze that will provide increased flexibility and capabilities at a price that permits its use in tactically significant quantities as well as for training.*

Keywords: ARTILLERY FUZE, SMART FUZE, INCREASED CAPABILITIES.

1. Introduction.

Although maneuver warfare is valid under certain circumstances, the nature of war and the realities of the modern battlefield call for more flexible weaponry [1]. Current ordnance faces an increased demand in percussion and efficiency in order to fulfill its battlefield role efficiently. The smart fuze researched in this paper aims to transform existing artillery projectiles into affordable "SMART" weapons.

The smart fuze project enhances and increases current capabilities of artillery projectiles. The smart fuze further mentioned in this report only as "SF" is a fuze sized module used in lieu of a standard fuze on existing artillery projectiles. The fuze installs in the projectile fuze well on already existing ordnance – in the field as needed.

The SF is a modular, multipurpose device designed to incorporate multiple fuze functions in one package. The device consists of a fuze-like kit that contains a microcontroller, power supply, customizable range of sensors, electronic circuitry and different fuze function modes. The SF is a combination fuze that incorporates wide range of capabilities and functions. The SF incorporates the following fuze capabilities and functions: Munition time fuze (MTF), Proximity or variable fuze (VTF), Percussion or impact fuze function [2]. The SF has the capability to operate both as a no delay type fuze that functions immediately on contact with any thin material (for example, the thin sheet metal skin of an aircraft) or with a delay to keep the burster from going off until after penetration [2]. The fuze is capable to go off either on impact or after the time set, whichever occurs first.

The SF functions in conjunction with command and control software that provides additional range of capabilities. The software is open source and provides the user with ease of use and high level of customizability. The operator has the freedom to choose the needed function from what the objective dictates given the circumstances and battlefield conditions. That provides the SF with the much needed edge over other mechanical fuze platforms and utilizes the full potential of the system. The SF strives to provide the necessary precision and flexibility at a price that permits its use in tactically significant quantities as well as for training. The SF utilizes electronic components that replace their mechanical counterparts found in the majority of the traditional fuzes.

Based on the shown above in this report, research is made in the creation of this low-cost, highly reliable, fuze-sized device that provides additional as well as improved traditional fuze functions on the modern battlefield.

2. Assembling, testing and configuring different fuze sensors and components.

2.1. Objective: Setting up, configuring and installing different sensor components.

2.2. Tasks:

- Configuring the microcontroller;

- Setting up, configuring and testing the ultrasonic proximity sensor;

- Setting up, configuring and testing the Passive Infrared (PIR) sensor;

- Setting up, testing and configuring the gyro-sensor and accelerometer.

- Configuring the microcontroller.

In order for the goal of this report to be achieved all the hardware components inside the fuze need to be carefully assembled, programmed and configured to function harmoniously with the software and the operator. The main component of the fuze that executes the software and controls the other hardware components is the microcontroller. The microcontroller in the fuse is based on the Arduino platform. The choice of the Arduino platform is driven by the fact that Arduino is an open-source electronics platform based on easy-to-use hardware and software [3]. Arduino boards are able to read inputs - light on a sensor, execute software instructions, or another electronic device - and turn it into an output - activating a motor, turning on an LED [3], executing a command etcetera. The board is instructed what to do by the use of the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing [3]. The main assembly model of the SF utilizes the Arduino Uno platform. Arduino Uno is a microcontroller board based on the ATmega328P microchip[4]. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button [4].

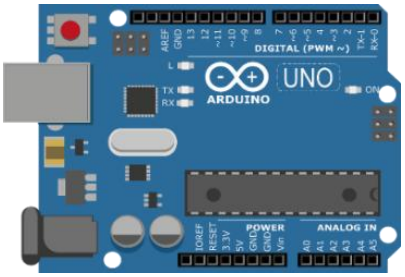


Fig. 1: *Arduino Uno board overview.*

Arduino Uno is fitted with the ATmega328 single-chip microcontroller. The functionality and configuration of all the components is tested with the microcontroller before they are assembled and fitted in the fuze model. The Arduino Uno board used in the project can be replaced with a much smaller board with the same functions and capabilities as the Arduino Nano board, making a much smaller fuze model.

- Setting up, configuring and testing the HC-SR04 ultrasonic proximity sensor;

The ultrasonic range finder is a module that measures distance. The module is able to determine the distance to an object, or to detect when something is near the sensor, like a motion detector. The module is ideally suited for projects involving navigation and object avoidance. The module is capable of operating in day and night conditions. The ultrasonic range finder used in the SF is the HC-SR04, which can measure distances from 2 cm up to 400 cm with an accuracy of ±3 mm [5].



Fig. 2: *HC-SR04 Ultrasonic Sensor.*

The transmitter emits 8 bursts of a directional 40KHz ultrasonic wave when triggered and starts a timer [6]. Ultrasonic pulses travel outward until they encounter an object, which causes the wave to be reflected back towards the unit. The ultrasonic receiver would detect the reflected wave and stop the stop timer. The velocity of the ultrasonic burst is 340 m/s in air [6]. Ultrasonic range finders measure distance by emitting these ultrasonic sound pulses that travel through the air until they hit an object. When that pulse of sound hits an object, it's reflected off the surface and travels back to the ultrasonic range finder. The ultrasonic range finder then measures how long it takes the sound pulse to travel in its round trip journey from the sensor and back. It then sends a signal to the Arduino with information about how long it took for the sonic pulse to travel. Knowing the time, it takes the ultrasonic pulse to travel back and forth to the object, and also knowing the speed of sound, the Arduino can calculate the distance to the object. The formula relating the speed of sound, distance, and time traveled is:

(1) $S = \frac{d}{t}$

Where S – speed, d – distance, t – time.

Rearranging this formula, we get the formula used to calculate distance:

(2) $D = s \, . \, t$

The time variable is the time it takes for the ultrasonic pulse to leave the sensor, bounce off the object, and return to the sensor. This time is divided in half since we only need to measure the distance to the object, not the distance to the object and back to the sensor. The speed variable is the speed at which sound travels through air. In order for the sensor to achieve best results and maximum range, the object that the sensors detect should be larger than 0.5 cubic meters, the nearer the target object, the smaller it may be [7]. On the front of the ultrasonic range finder are two metal cylinders. These are transducers. Transducers convert mechanical forces into electrical signals. In the ultrasonic range finder, there is a transmitting transducer and receiving transducer. The transmitting transducer converts an electrical signal into the ultrasonic pulse, and the receiving transducer converts the reflected ultrasonic pulse back into an electrical signal. The HC-SR04 ultrasonic range finder has four pins: Vcc, Trig, Echo, and GND. The Vcc pin supplies the power to generate the ultrasonic pulses. The GND pin is connected to ground. The Trig pin is where the Arduino sends the signal to start the ultrasonic pulse. The Echo pin is where the ultrasonic range finder sends the information about the duration of the trip taken by the ultrasonic pulse to the Arduino. To initiate a distance measurement, a 5V high signal is send to the Trig pin for at least 10 µs. When the pulse hits the receiving transducer, the Echo pin outputs a high voltage signal.

For the purpose of this paper a rangefinder module is assembled that outputs the distance measurements to the microcontroller. The microcontroller then utilizes the obtained data and activates the fuze at a distance set in the software by the operator. This distance set in the software is the proximity distance at which the operator wants the fuze to execute the explosive function of the projectile. The microcontroller is connected to the fuse's detonator thus when voltage is applied to the detonator from the microcontroller the projectile's detonation is initiated. The detonator in the prototype is simulated via the red LED and the detonation is indicated by the buzzer. Using Autodesk circuits, a working model is simulated before the creation of the prototype model (Fig.3).

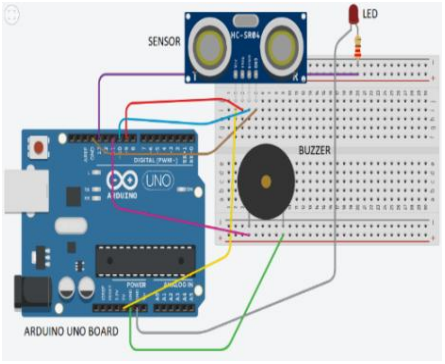


Fig. 3: *Project simulation using Autodesk circuits.*

After simulating the project and testing the working capabilities of the hardware the software is uploaded to the microcontroller. The assembled prototype board is shown in (Fig.4).

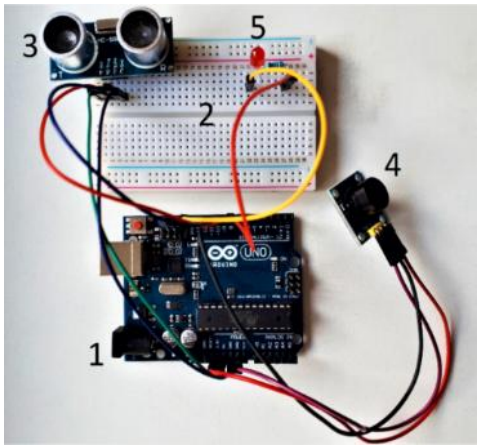


Fig.4: *Project assembly.*

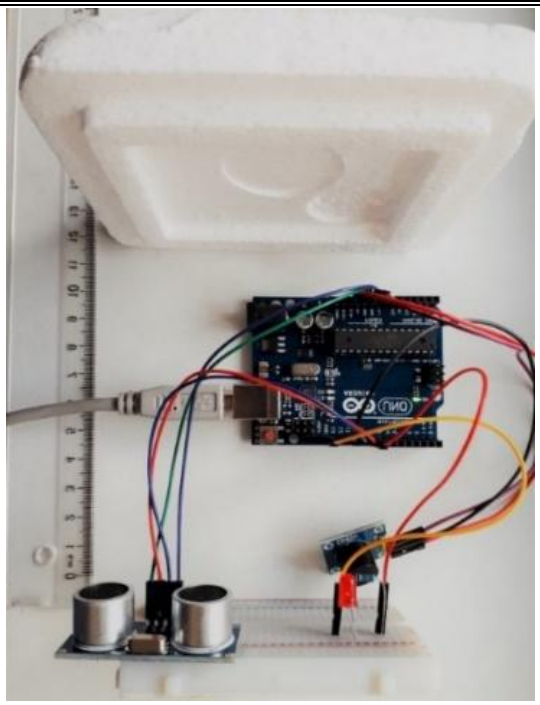


Fig. 5: *Testing the assembly model.*

In ***Fig.5*** the Arduino successfully detects the presence of the object in front of the sensor and turns on the LED when the object is at the desired distance set in the software. The components used in the assembly project are listed in (Table.3):

Table. 1: *Components list.*

Number	Component
1	Arduino Uno
2	Breadboard
3	HC-SR04
4	Buzzer
5	LED and Resistor

Using SOLIDWORKS software a 3D model housing the sensor is created. The HC-SR04 sensor will be fitted inside the model after which the model will be assembled on the fuze.

- Setting up, configuring and testing the Passive Infrared (PIR) v1.0 and v.1.1 sensors;

The PIR sensor provides the fuze with the capability to detect personnel and therefore initiate the explosive function of the projectile. The PIR, "Passive Infrared", "Pyroelectric", or "IR motion" sensor is capable of detecting personnel moving in and out of the sensor's range. The PIR sensor is made of a pyroelectric sensor [10], which can detect levels of infrared radiation. Along with the pyroelectric sensor, the chip is also equipped with supporting circuitry, resistors and capacitors [8]. The chip uses the output of the sensor and after processing emits a digital output pulse from the analog sensor.

The PIR sensor itself is equipped with two slots in it. Each slot is made of a material that is sensitive to IR. There is some distance between the lens and the sensor itself. [8]. When the sensor is idle, both slots detect the same amount of IR, the ambient amount radiated from the room, or walls or outdoors. When a heat signature, for example, a human or an animal passes by, it first intercepts one half of the PIR sensor, which causes a positive differential change between the two halves. When the warm body leaves the sensing area, the reverse happens, whereby the sensor generates a negative differential change.

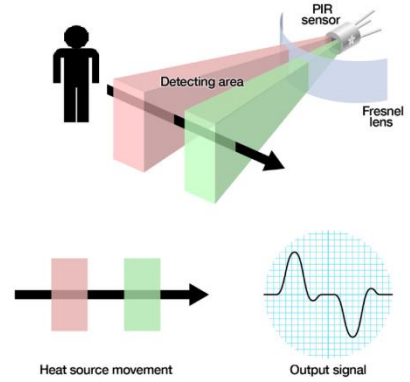


Fig. 5: *PIR sensor working principle.*

The IR sensor itself is housed in a hermetically sealed metal can to improve noise/temperature/humidity immunity. There is a window made of IR-transmissive material [9] that protects the sensing element. Behind the window are the two balanced sensors.

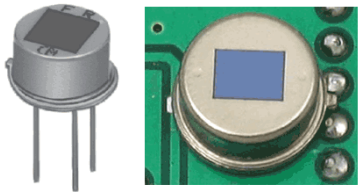


Fig.7: *Pyroelectric Infrared Sensor [9].*

The lens of the PIR is the component that determines the change in the breadth, range and the sensing pattern. The sensor uses a simple lens. They condense a large area into a small one, for this reason the sensor is actually equipped with Fresnel lenses. The Fresnel lens condenses light, providing a larger range of IR to the sensor (Fig10).

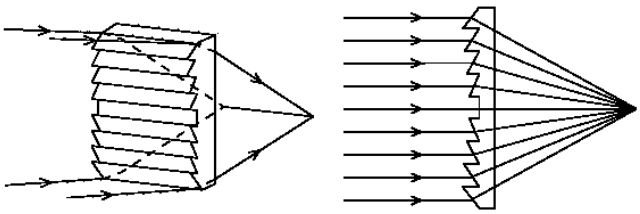


Fig.8: *PIR sensor's Fresnel lens dome.*

The PIR sensor is added to the fuze like model. The PIR sensor in the model will feed data to the microcontroller which in turn will initiate the explosive function of the projectile when the sensor detects a heat signature. The experimental circuit schematics made are presented in (Fig. 10). The output pin of the sensor is connected to pin-8 on the Arduino Board and when an object is detected the pin-7 will activate a voltage relay connected to the fuze detonator.

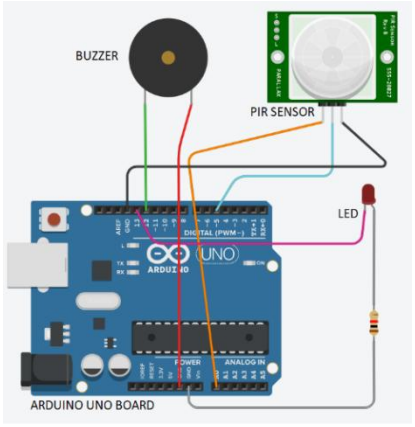


Fig.9: *Project simulation using Autodesk circuits.*

After simulating the project and testing the working capabilities of the hardware, the software is uploaded to the microcontroller. The assembled prototype board is presented in (Fig.10).

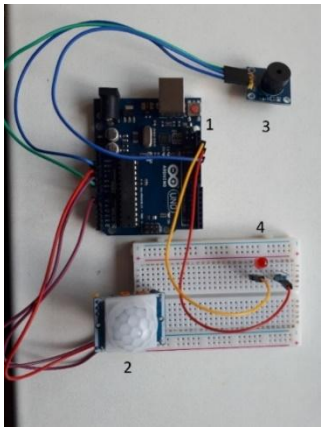


Fig. 10: *PIR sensor project assembly.*

The components used in the assembly are listed in (Table.4):

Table. 2: *Components list.*

Number	Component
1	Arduino Uno
2	PIR sensor
3	Buzzer
4	LED and Resistor

Using SOLIDWORKS software a 3D model is created. The PIR sensor will be fitted inside the model after which the model will be assembled on the fuze. After everything is assembled and connected the command code is written and uploaded to the Arduino board. Different PIR sensor (Fig.11) is also used working on the same principles.

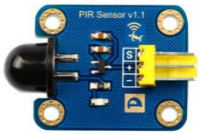


Figure 11: *PIR Sensor v1.1.*

A prototype model is assembled and presented in (Fig.12). The microcontroller used is the Arduino Uno board.

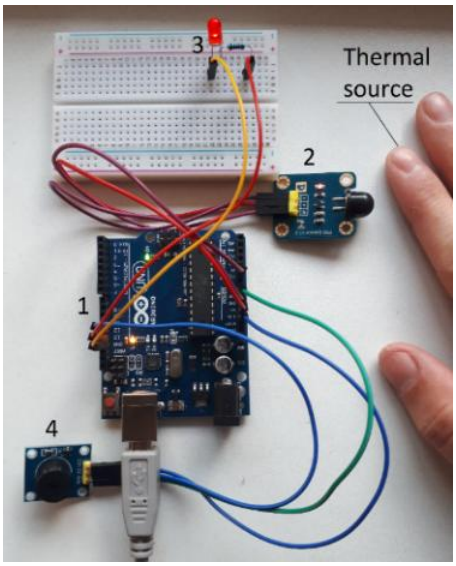


Fig 12: *PIR v1.1 project assembly.*

The components used in this assembly are listed in (Table 3).

Table. 3: *Components used in the assembly.*

Number	Component
1	Arduino Uno
2	PIR sensor v 1.1
3	LED and Resistor
4	Buzzer

The PIR sensor in the model is able to detect the thermal presence of the human hand and initiate the LED. Using SolidWorks 3D model are created for both PIR sensor. The models are fitted on top of the fuze body.

-Setting up, testing and configuring the ADXL345 gyro-sensor and accelerometer.

The MEMS are very small systems or devices, composed of micro components with a very small size. These components are made of silicon, polymers, metals and/or ceramics, and they are usually combined with a CPU (Microcontroller) for completing the system [10]. The working principle of the Micro-Electro-Mechanical-Systems (MEMS) sensors will be briefly explained below.

MEMS measure acceleration by measuring the change in capacitance. Its micro structure is displayed in (Fig.13). The MEMS chip has a mass attached to a spring which is confined to move along one direction and fixed outer plates. So when an acceleration in the particular direction is applied the mass moves and the capacitance between the plates and the masses changes. This change in capacitance will be measured, processed and will correspond to a particular acceleration value.

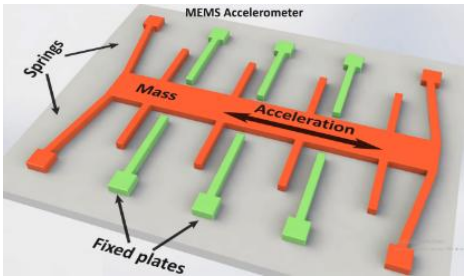


Figure 13: *MEMS chip working structure and principle of action.*

The accelerometer used in the project is the ADXL345 chip (Fig14).



Figure 14: *ADXL345 overview.*

The ADXL345 is a small, thin, low power, 3-axis accelerometer with high resolution (13-bit) measurement at up to ±16 g. Digital output data is formatted as 16-bit twos complement and is accessible through either a SPI (3- or 4-wire) or I2 C digital interface [11].The ADXL345 is well suited for mobile device applications. It measures the static acceleration of gravity in tilt-sensing applications, as well as dynamic acceleration resulting from motion or shock. Its high resolution (4 mg/LSB) enables measurement of inclination changes less than 1.0° [11]. Several special sensing functions are provided. Activity and inactivity sensing detect the presence or lack of motion and if the acceleration on any axis exceeds a user-set level. Tap sensing detects single and double taps. Free-fall sensing detects if the device is falling. [11].

Considering the applications listed above the ADXL345 is the perfect choice for the SF. The ADXL345 will function as the fuze safety feature as it will act as a safety-detonation mechanism. The safety-detonation mechanism will detect whether or not the fuze has been fired from the artillery cannon, ensuring that the fuze only works when intended to do so. This process is achieved in conjunction with the hardware and software. Given the sensing capabilities of the accelerometer in particular: free-fall sensing and activity, inactivity sensing. The ADXL345 can detect acceleration and measure it in G-force. Setting up the software to arm the fuze only after an acceleration greater than 3G is detected by the accelerometer ensures that the ordnance will not detonate during transportation or when handled or dropped. The acceleration safety setting is set for 3G. Such a high level of acceleration is sufficient to ensure safety given ordnance is handled accordingly to the safety measures or dropped unintentionally. Because the ADXL345 sensor is the main safety feature of the fuse, the device must function properly at all times in order for safety to be guaranteed. The ADXL345 is the module connected with the fuze safety feature. In order for safety to be guaranteed it is critical that this device functions properly at all times. Thus the ADXL 345 is equipped with a self-test capability. The self-test change is defined as the difference between the acceleration output of an axis with self-test enabled and the acceleration output of the same axis with self-test disabled [11]. This definition assumes that the sensor does not move between these two measurements, because if the sensor moves, a non–self-test related shift corrupts the test [11].

Using Autodesk circuits, the ADXL345 module is simulated with conjunction with the Arduino board (Fig 15).

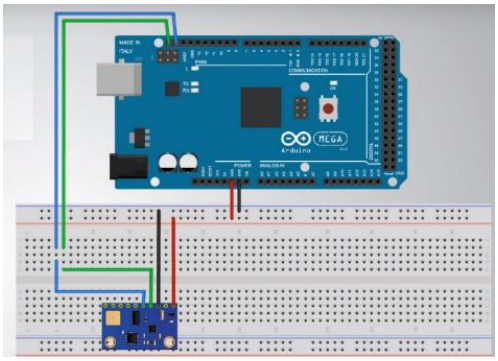


Figure 15: *Autodesk circuits smulation.*

Testing the working capabilities of the sensor is shown in (Fig.16).



Figure 16: *Testing the module.*

The pen on fig 18 shows the x axis of the sensor so if the sensor is rotated around the axis we can detect the changes on the serial monitor. Unfortunately, the gyro results are not stable due to the fact that they drift as the time goes so in order to get more accurate angles data the gyro needs to be combined with the accelerometer data,

3. Conclusion.

The components configured in this paper have the capabilities to function as a fuze with multiple fuzing capabilities. With the following fuze functions: personnel detection, proximity detection and time fuzing. The SF model is provided with a safety mechanism, allowing for safe ordnance handling and transportation.

The microcontroller used in the project was successful in executing the software commands. The microcontroller was able to control the different sensor components to gather and analyze data from them working in conjunction with the software. The Arduino Uno is a suitable component for the SF as it meets the needed requirements.

The ultrasonic proximity sensor researched in this paper provides distance measuring and proximity sensing capabilities at a very limited range. The HC-SR04 Ultrasonic sensor range proves to be unsuitable for the needs of the smart fuze project as it has a range of 400cm that proves to be insufficient for the fuze purposes. The sensor accuracy is also inadequate as it proves to degrade rapidly at larger distances. Considering the limited range and accuracy the sensors is it unsuited for use in the SF. A specialized sensor designed purely for military purposes, which has a higher range and accuracy, must be designed in order to be used in an optimal fashion and meet the modern day battle criteria.

The PIR sensor researched in this paper was successfully able to detect heat signatures entering and exiting the sensor's effective range. The PIR sensor effective range and accuracy proved insufficient for the purpose of the smart fuse as they were very limited which in turn demands for a specialized sensor to be researched purely for military purposes.

The accelerometer chip used in the project was able to measure accelerating. The chip meets the necessary requirements for the smart fuze, thus it is a valuable choice for a fuze like kit like the SF. Furthermore, with the build in self-test the device adds additional safety to the SF as it is ensured to function properly.

In perspective the stress applied to the fuze body when fired must be investigated further. More research needs to be conducted with the use of more sophisticated electronic components for the proximity and distance sensors that have a higher degree of accuracy and precision, as the ones currently used prove to be insufficient to provide the fuze with the required range and functionality.

References:

1. https://www.globalsecurity.org/military/library/report/1991/WAD.htm .
2. U.S. Navy Ammunition, Historical and Functional Data, NAVSEA SW010-AB-GTP-010.
3. https://www.arduino.cc/en/Guide/Introduction.
4. https://store.arduino.cc/arduino-uno-rev3.
5. http://web.eece.maine.edu/~zhu/book/lab/HC-SR04%20User%20Manual.pdf
6. https://www.mpja.com/download/hc-sr04_ultrasonic_module_user_guidejohn.pdf
7. HC-SR04 UserGuide - Marlin P. Jones https://www.mpja.com/download/hc-sr04_ultrasonic_module_user_guidejohn.pdf
8. https://cdn-learn.adafruit.com/downloads/pdf/pir-passive-infrared-proximity-motion-sensor.pdf
9. https://cdnlearn.adafruit.com/assets/assets/000/010/137/original/pyroelectrics21e.pdf
10. https://cdn-learn.adafruit.com/downloads/pdf/pir-passive-infrared-proximity-motion-sensor.pdf
11. https://howtomechatronics.com/how-it-works/electrical-engineering/mems-accelerometer-gyrocope-magnetometer-arduino/
    able

EVALUATION OF HIT'S GROUPING DEVIATION DUE TO TRIBOLOGICAL PROCESSES IN BULLET-RUBBER CHOPPER WHEEL INTERACTION

АНАЛИЗ НА ОТКЛОНЕНИЕТО НА ГРУПИРАНОСТТА ВСЛЕДСТВИЕ НА ТРИБОЛОГИЧНИТЕ ПРОЦЕСИ ПРИ ПРЕМИНАВАНЕ НА КУРШУМ ПРЕЗ ГУМЕН ОБТЮРАТОР

M.Sc. Ing. Dimitrova Ya. D.
Faculty of "Artillery, air defense and CIS" – National Military University "Vasil Levski", Veliko Tarnovo, the Bulgarian Republic

dimitrovax2yana@gmail.com

Abstract: *The use of special weapons in counter-terrorist operations with fitted suppressors and the necessity of reliable target damage even while using individual ballistic armor protection details initiate the need of evaluation of hits grouping deviation. In the report is evaluated hit's grouping deviation due to tribological processes in bullet-rubber chopper wheel interaction with scrutinizes of the experimental fire shooting data.*

Keywords: SILENCER; HITS GROUPING DEVIATION; TRIBOLOGICAL PROCESSES.

1. Introduction

Fight against terrorist organizations requires a change in the traditional perceptions of military action and tactical use of firearms. Due to the complexity of anti-terrorist operations it is necessary to use special equipment for the firearms.

Parts of this special equipment are the silencers. Silencer reduces the sound of the firearms when they fired, by lowering the temperature and velocity of the effluent gases. In addition the use of special equipment for individual ballistic protection requires weapons with high efficiency. High efficiency is achieved by increased precision and shots grouping.

Thinks to consider in counter-terrorist operations are special equipment and special ammunition usage. Both of them lead to changes in weapon's ballistic characteristics. Last ones are base for achieving maximum efficiency and reliable target damage while using individual ballistic armor protection in combat operation scenario.

The report's subject is the PBS-1 which is a chamber type silencer with rubber chopper wheel. The research of the information in available literature ensures that the rubber chopper wheel serves to initiate the automatic action of the weapon and does not affect the noise suppression. Records can be found, in many information sources that the rubber chopper wheel changes the hit's grouping, but there is no experimental data of conducted researches. Available literature analysis shows that there is no data of evaluated deviation dependencies of hit's grouping due to tribological processes in bullet-rubber chopper wheel interaction.

Therefore the experimental shootings data have been used to determine the dependency between the hit's grouping deviation and the tribological processes. As a milestone in achieving maximum efficiency is the determination of target area limits in semi-automatic fire mode using fitted chamber type suppressor with rubber chopper wheel.

Based on the paragraphs above in the report several researches have been conducted and as a result is evaluated hit's grouping deviation due to tribological processes in bullet-rubber chopper wheel interaction.

2. Evaluation of hit's grouping deviation dependencies

2.1. Purpose: Evaluation of deviation dependencies of hit's grouping due to tribological processes amendment in bullet-rubber chopper wheel interaction while reducing the power of contact tension.

2.2. Tasks:

- to determine the mathematical expectation and the standard deviation from the experimental shooting's data in case of new rubber chopper wheel;

- to determine the mathematical expectation and the standard deviation from the experimental shootings data in case of different diameter of rubber chopper wheel's opening;

- to determine the dimensions of shots grouping using the rule of the three σ on the vertical and the horizontal planes in which the 100% of the bullet hits the target in case of different diameter of rubber chopper wheel's opening and without opening.

3. Results of discussion

In order to achieve the purpose of this report the deviation of hits from the control point are obtained from experimental shootings during single fire with fitted silencer PBS-1 on AK-47 assault-rifle in case of different openings diameter and without opening in the rubber choper wheel.

3.1. Determination of the mathematical expectation and the standard deviation

For evaluation of deviation dependencies of hit's grouping due to tribological processes amendment in data analysses represented are made several study cases. These cases difers from one another by diameter of the opening in rubber chopper wheel and some of them are made before shooting, others have been normally created by bullet passing through the rubber chopper wheel.

The rubber chopper wheel's opening diameters are:

- $d_n = 0$ mm – new rubber chopper wheel;

- conic opening after 20 shots were fired with input diameter – $d_{co} = 4$ mm and output – d = 1 mm;

- conic opening after 100 shots were fired with input diameter – $d_{co} = 6$ mm and output – d = 2 mm;

- conic opening after 180 shots were fired with input diameter – $d_{co} = 8$ mm and output – d = 4 mm;

- $d_{cy} = 7$ mm – cylindrical opening handmade before shooting;

- $d_{cy} = 8$ mm – cylindrical opening handmade before shooting;

- $d_{cy} = 9$ mm – cylindrical opening handmade before shooting.

Table 1 and table 2 represents the deviation of hits from the control point in horizontal and vertical planes in case of different openings diameter and without opening in the rubber choper wheel.

Table 1: *Deviation of hits from the control point horizontally*

Number of hits	Deviations of hits from the control point horizontally, in centimetres						
	The rubber chopper wheel's opening diameter, [mm]						
	dn = 0	dco = 4	dco = 6	dcy = 7	dcy = 8	dcy = 9	dco = 8
1	0	-8,3	-16,4	-25,6	-0,8	-3,6	-27,3
2	-7	-8,4	-18,2	-26,4	-1,2	-5,3	-28,4
3	-7,7	-9,5	-19,8	-27,8	-1,9	-6,3	-31,2
4	-10	-10,2	-20	-28,8	-3,6	-6,5	-32,5
5	-10,2	-11	-20,5	-28,9	-3,7	-6,6	-35,8
6	-12,5	-12	-22,8	-30,3	-4	-6,7	-35,8
7	-12,7	-14	-23,5	-30,7	-6,2	-6,9	-36
8	-13,2	-16	-23,5	-31	-11	-7,1	-36,6
9	-14,4	-17,3	-23,7	-31,6	1,6	-7,3	-36,7
10	-15,2	-18	-24,1	-32,8	2,6	-9,4	-37
11	-15,6	-18,2	-25	-33,1	5,3	-9,5	-39,5
12	-16,3	-19,6	-26	-33,8	5,4	-9,7	-40,2
13	-17,4	-20,7	-26,3	-34,4	6	-9,8	-40,4
14	-18,9	-21,1	-26,4	-35,2	6,6	-10,2	-40,6
15	-19,3	-22,1	-27,8	-35,4	8,2	-10,9	-40,7
16	-19,4	-24	-28,8	-36,6	8,4	-11	-41,2
17	-20	-24,2	-29,5	-37,4	9,3	-11,9	-41,5
18	-22,6	-25,3	-31,8	-38,1	10	-13,8	-43,2
19	-25,5	-26,3	-32	-38,8	12,8	-15,1	-46,4
20	-28,5	-31	-38	-39,4	14,3	-15,6	48,5

Table 2: *Deviations of hits from the control point vertically*

Number of hits	Deviations of hits from the control point vertically, in centimetres						
	The rubber chopper wheel's opening diameter, [mm]						
	dn = 0	dco = 4	dco = 6	dcy = 7	dcy = 8	dcy = 9	dco = 8
1	6,8	5,6	-2	-1	9,6	-1,1	-4
2	11,8	17,9	-2,2	-2,8	11,6	-2	17,5
3	12,8	24	-2,4	-3,4	12,1	1,1	18,8
4	13	26,2	-2,6	-4,6	12,2	1,4	19,2
5	13,5	26,8	-3,2	-5,2	12,8	1,5	20,8
6	14,2	27,4	-3,4	-6,4	14,6	2,6	24,3
7	15	28	-3,7	-7,8	14,7	3	24,4
8	15,3	29,2	-3,9	-9,4	14,8	3,4	26,2
9	15,5	29,7	-4,2	-10,5	15,2	4,3	26,4
10	15,8	30	-4,5	-11,4	15,3	5,1	26,8
11	16,1	30,6	-5	-12,3	15,6	5,9	28,2
12	17	30,9	-5,2	-12,6	16,1	6,2	29
13	17,2	31,5	-5,9	-12,8	16,6	6,3	29,3
14	17,6	31,9	-6,4	-14,1	16,8	6,6	30,6
15	18	32	-6,8	-15,2	17,2	7,4	31,4
16	18,8	32,2	-7,5	-16,8	19,1	7,5	33,8
17	22	32,4	-7,6	-18,5	20,8	7,8	34,4
18	22,9	32,6	-8,3	-23	21,6	8,8	34,5
19	25,4	33	-8,5	-23,6	21,8	12,1	35,6
20	27,8	34,4	-9,2	-30,6	22,8	12,2	39

To determent the satisfying minimum required number of shots, that provide confidence interval of 99.9%, the following equation is used:

$$(1)\ n = \frac{S^2 u_{\frac{\alpha}{2}}^2}{\varepsilon^2} = \frac{5{,}862^2 . 3{,}37^2}{4{,}623^2} = 18{,}26$$

In this equation, the quantities are defined as:

- $u_{\frac{\alpha}{2}}$ – is a quantile of the normal distribution that provide confidence level of 99.9%

-S – standard deviation;

-ε – accuracy of the estimation of mathematical expectation.

Standard deviation can be calculated using the formulas:

$$(2)\ S = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \chi)^2};$$

Accuracy of the estimation of mathematical expectation is determined by fowling mathematical apparatus:

$$(3)\ \varepsilon = t_{\frac{\alpha}{2}} \frac{S}{\sqrt{n}},$$

- $t_{\frac{\alpha}{2}}$ a quantile of the Student's normal distribution.

The minimum required number of shots are 19 during the investigation twenty shots in series were fired which satisfy the requirment.

Using mathematical software Math Lab it is define the mathematical expectation - (χ) and the standard deviation - (σ) of the deviation of hits from the control point in horizontal and vertical planes which are presented in table 3.

Table 3: *Mathematical expectation and standard deviation of hit's deviation from the control point in horizontal and vertical planes in case of different openings diameter and without opening.*

The rubber chopper wheel's opening diameter, [mm]	value of χ in centimetres		value of σ in centimetres	
	horizontal plane	vertical plane	horizontal plane	vertical plane
dn = 0 mm	-15,32	16,825	6,647	4,851
dco = 4 mm	-17,86	28,315	6,594	6,545
dco = 6 mm	-25,205	-5,125	5,205	2,276
dcy = 7 mm	32,805	-12,1	4,128	7,682
dcy = 8 mm	2,905	16,065	6,796	3,648
dcy = 9 mm	-9,16	5,005	3,249	3,855
dco = 8 mm	-33,125	26,31	19,808	9,295

3.2. Determination of the dimensions of shots grouping

From the analysis made, using the values of mathematical expectation - (χ) and the standard deviation - (σ) and the rule of the three σ – are determined the dimensions of ellipse of dispersion of hits in the vertical and the horizontal planes in which the contains 100% of hits. The values of normal distributed random variable's ellipse of dispersion based on the rule of the three σ are presented in table 4.

Table 3: *The dimensions of dispersion ellipse of normal distributed random variable*

The rubber chopper wheel's opening diameter, [mm]	$\bar{x}$ - 3σ		$\bar{x}$ + 3σ	
	horizontal plane	vertical plane	horizontal plane	vertical plane
dn = 0 mm	-35,262	2,27	4,622	31,38
dco = 4 mm	-37,644	8,68	1,924	47,95
dco = 6 mm	-40,822	-11,954	-9,587	1,704
dcy = 7 mm	-45,189	-35,167	-20,421	10,946
dcy = 8 mm	-17,485	5,121	23,295	27,008
dcy = 9 mm	-18,909	-6,562	0,589	16,572
dco = 8 mm	-92,551	-1,575	26,301	54,195

On Fig. 1 to Fig. 7 graphically represents mathematical expectation and ellipse of dispersion in the vertical and the horizontal planes for different opening diameters in the rubber chopper wheel.

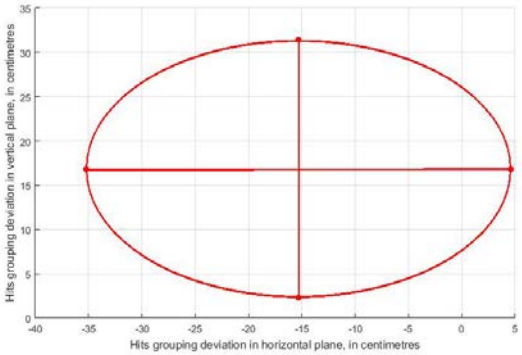


Fig. 1 *Graph of mathematical expectation and ellipse of dispersion in the vertical and the horizontal planes in case of the new rubber chopper wheel – d_n = 0 mm.*

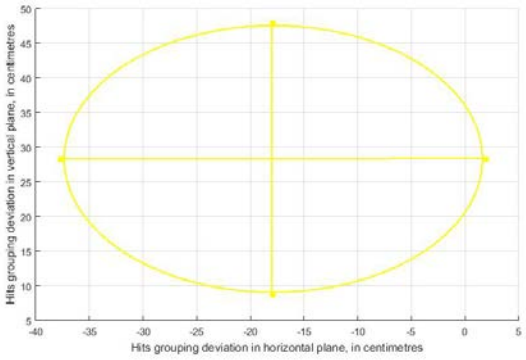


Fig. 2 *Graph of mathematical expectation and ellipse of dispersion in the vertical and the horizontal planes in case of the rubber chopper wheel's diameter opening – d_{co} = 4 mm.*

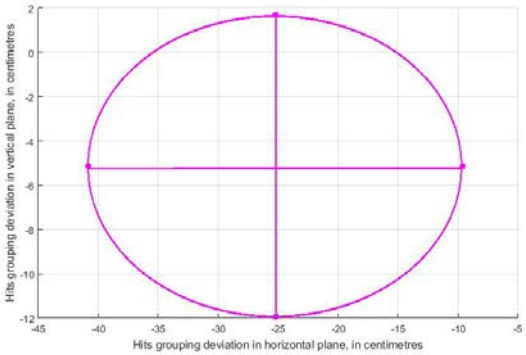


Fig. 3 *Graph of mathematical expectation and ellipse of dispersion in the vertical and the horizontal planes in case of the rubber chopper wheel's diameter opening – d_{co} = 6 mm.*

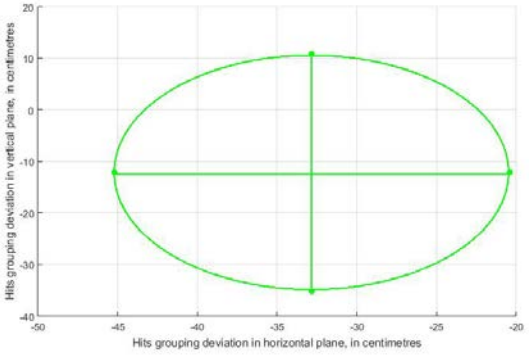


Fig. 4 *Graph of mathematical expectation and ellipse of dispersion in the vertical and the horizontal planes in case of the rubber chopper wheel's diameter opening – d_{cy} = 7 mm.*

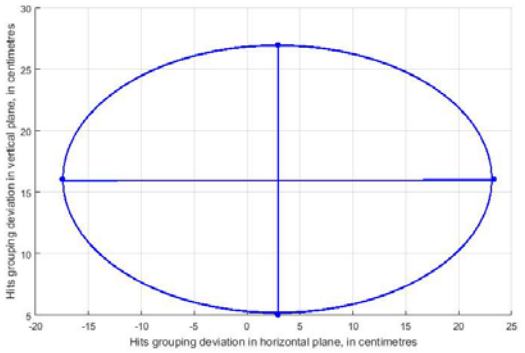


Fig. 5 *Graph of mathematical expectation and ellipse of dispersion in the vertical and the horizontal planes in case of the rubber chopper wheel's diameter opening – d_{cy} = 8 mm.*

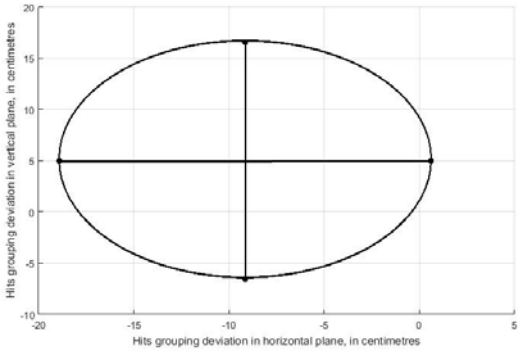


Fig. 6 *Graph of mathematical expectation and ellipse of dispersion in the vertical and the horizontal planes in case of the rubber chopper wheel's diameter opening – d_{cy} = 9 mm.*

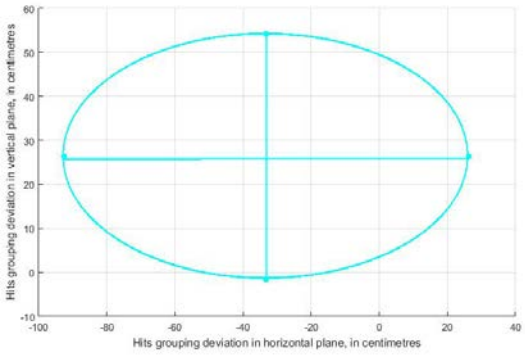


Fig. 7 *Graph of mathematical expectation and ellipse of dispersion in the vertical and the horizontal planes in case of the rubber chopper wheel's diameter opening – d_{co} = 8 mm.*

Fig. 8 graphically presents comparison of hit's grouping deviation for different opening diameter in the rubber chopper wheel. Mathematical expectation and ellipse of dispersion in vertical and the horizontal planes for different occasion are compared.

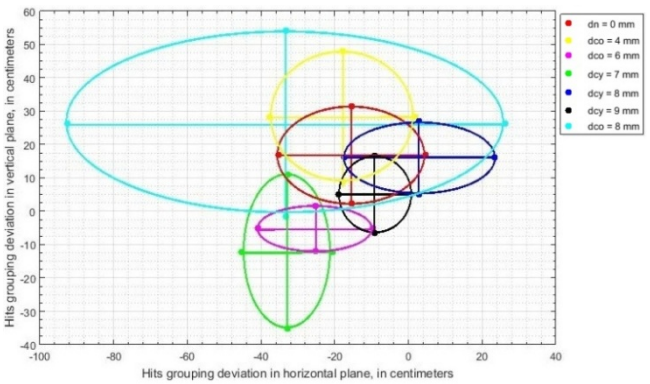


Fig. 8 *Summarized graph of hits grouping deviation.*

4. Conclusions

1. From the conducted research it can be concluded that the deviation of hits grouping with a fitted chamber type suppressor with a rubber chopper wheel has tribological process dependencies. It can be concluded that the amendment of the tribological characteristics lead to alteration in the deviation of the shots grouping in the vertical and the horizontal planes.

2. The research shows a phenomenon of a handmade opening in rubber chopper wheel before shooting. Based on the PBS-1 service manual information the diameter of normal grouping of hits is 15 centimeters. From Figure 6 presented above, it can be summarize that the hits grouping tends to be normal when contact between the bullet and the rubber chopper wheel of the suppressor is missing.

3. Based on the data analysis it can be concluded that dispersion of hits in range and deflection is at least eight times smaller when shooting with cylindrical handmade opening with diameter – d_{cy} = 8 mm than conic opening with same input diameter.

4. The evaluated hit's grouping deviation due to tribological processes in bullet-rubber chopper wheel interaction present that after 180 shots with conic opening $d_{co} = 8$ mm in rubber chopper wheel the diameter of grouping has the greatest size. That determines the wear of the rubber chopper wheel has a significant impact on the hits grouping.

REFERANCES:

1. Вентцель Е.С., Теория вероятностей и ее инженерные приложения, Москва, 2010 г.
2. Вълков Н. В., Давидов К. С., Цонев Ц. Г., Ганев В. В. Основи и правила за стрелба с огнестрелни оръжия. Материална част на стрелковото оръжие. Варна: Стено, 2008 г. ISBN 978-954-449-411-7.
3. Вълчев Х., Йорданова П. Статистиката, Шумен, 2003 г.
4. Иода Е. В., Герасимов Б. И., Статистика, Тамбовский государственный технический университет, 2004 г.
5. Кирилов В. М. Основи за устройството и проектирането на стрелковото оръжие. София: ДВИ, 1975 г.
6. Монтгомери Д. К., Планирование эксперимента и анализ данных., Ленинград: Судостроение, 1980 г.
7. Патарински В., Теория на вероятностите, МНО, ДВИ, София 1976 г.
8. Потемкин В. Г., Система инженерных и научных расчетов MATLAB, Том 1 и 2, М., 1999 г.
9. Хамитов Г.П. Вероятности и статистики, Иркутск, 2006 г.
10. Цонев Ц. Г., Богданов А. И., Проверка боя и привеждане на стрелковото оръжие към нормален бой, Шумен 2006 г.
11. Чернова Н. И. Теория вероятностей, Новосибирск, 2007г.

INFORMATION TECHNOLOGIES EMPLOYED IN ARMAMENT DESIGN FOR EDUCATION

Delchev L.*; Beevski A.**; M.Sc. Ing. Antonov S.***; Prof. Lilov I.****

National Military University "Vasil Levski", Artillery, AAD and CIS Faculty,

*lubodelchev@mail.bg; **beevski@abv.bg; ***stamantonov@abv.bg;**** inl@abv.bg

Abstract: *In the report is explored employment of armament design information technologies for education purposes and usage of automation, calculation, design and engineering methods for analysis and testing of armament models in virtual environment.*

Key words: *CAD-CAM-CAE SYSTEMS, MATHCAD, INFORMATIONAL TECHNOLOGIES.*

1. Introduction

The calculation, design and engineering analysis are complicated processes which is easily processed by the engineering software products "Mathcad" and "SolidWorks"

Mathcad has several mathematical packages available on the software products market, where complex, mathematical tasks are solved quickly, simply and effectively, even in symbolic (analytical) form. Such are Maple, Matlab and others. Mathcad is a class of applications called PSE - a Task Scheduling Environment. This means that its work is not uniquely determined by user actions, such as in text editors, but is largely the result of the operation of in-package algorithms that are inaccessible to the user. The script of the various commands from Mathcad follows the popular command description of "Windows" applications in a way, with the sequence of choosing commands and subcommands being separated by a slash. (fig.1.)

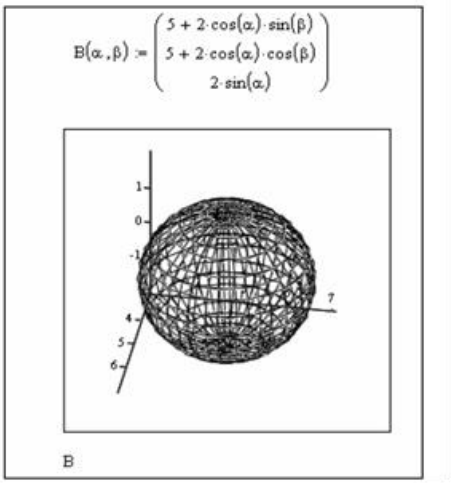


Fig.1. *A Mathcad's capabilities*

SolidWorks is a 3D CAD-CAM self-contained program for creating three-dimensional details and assembled constructions, allowing direct building and visualization of objects.

The software creates solid-state models. But it can also insert, create and manipulate surface patterns, view patterns in contour shape, and generate 2D-3D drawings.

It also offers an interface for a wide range of simulations and analyzes as well as the possibility of adding additional package extensions for fill simulations, shapes and shaping tools, fluid and kinematic analyzes, electronic components and more (Fig. 2.)

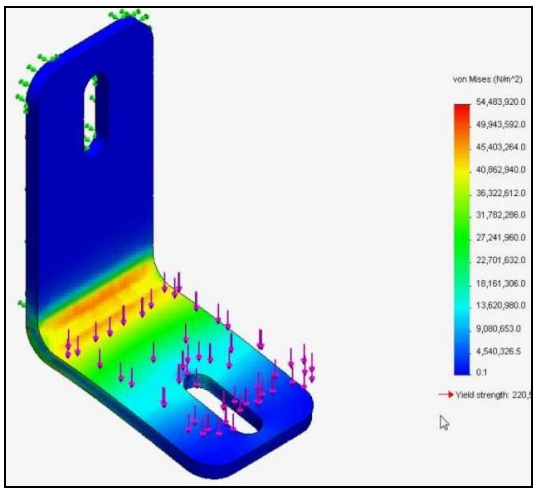


Fig.2*. SolidWorks analysis*

2. Research

The research contains the method of designing which includes calculation, design and 3D modeling of a hydraulic recoil brake and gun elevation mechanism for artillery system 2S1 "Gvozdika" (Self-propelled howitzer) and their analysis.

2.1. Calculation

Initially, the program product is prepared to work, fix some basic settings and introduce the main (constant) data in the algorithm. After all of the mathematical calculation about hydraulic recoil brake and gun elevation mechanism, are made. The result of the calculation is the basic data (dimensions, material and structure) necessary for the upcoming processes of design and analysis. (Fig.3)

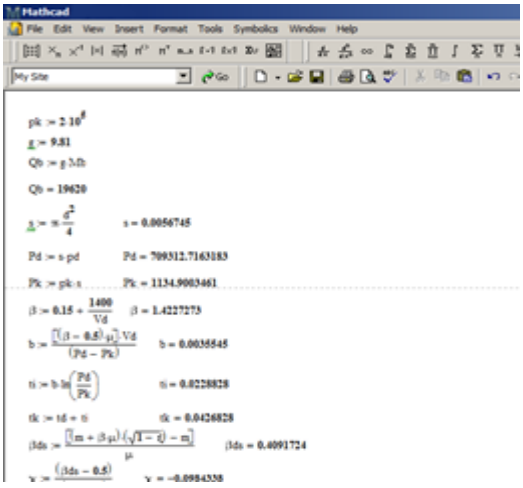


Fig. 3*. Example of the basic calculations*

2.2. Design and 3D modeling

After solving the mathematical algorithm and reaching the values necessary for the modeling of the product, the process continues with making a three-dimensional model. For this purpose, SolidWorks engineering product are used.

The creation of a three-dimensional physical model will help defense engineers to clear up their visualization, defining all types of dimensions.

Due to the fact that a hydraulic recoil brake and gun elevation mechanism consists of many kinds of different parts and elements, it is necessary that each part be created separately and then assembled. The created parts are:

- Hydraulic recoil brake (Fig.4.) – Cylinder; Cylinder cover; internal compensator cylinder; Moderator; Seal; Teflon sleeve; Ram; Brake compensator. (Fig. 5.)

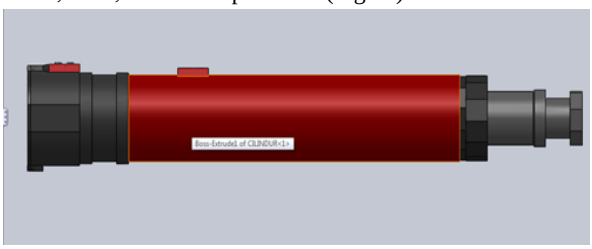


Fig.4. *Assembly of the Hydraulic recoil brake*

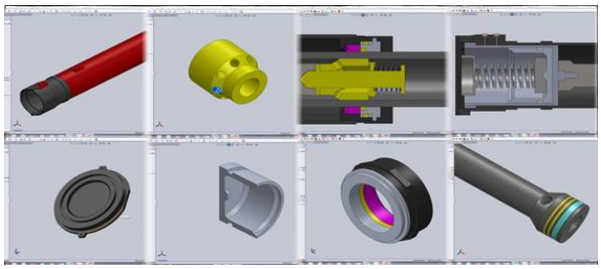


Fig. 5*. Separated parts of the recoil brake*

- Gun elevation mechanism

Body; Cover; Worm gear; Worm shaft; Shaft; Splines; Spur-wheel; Bearings; Bearing caps; Plugs. (Fig. 6.)

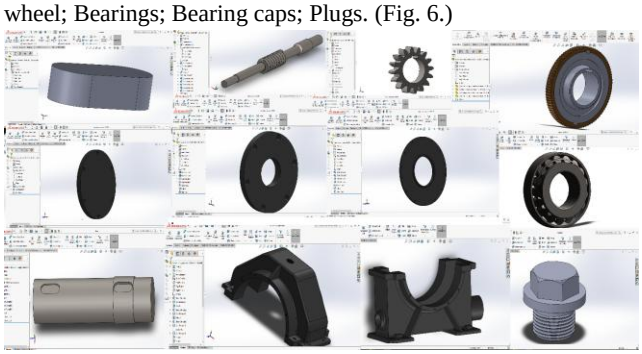


Fig.6. *Separated parts of the Gun elevation*

3. Analysis

The main idea of the analysis is to check the purpose and the work of you future designed details. It replaces the old fashion way of calculating the stress on the details on a sheet with a pen, and improves the quality of the calculated features. The main idea of the simulation is to save time and be an economy factor when it comes to designing parts. In this project the simulation part is concentrated mostly on stress test, pressure test and a motion flow test inside the Cylinder of the Hydraulic recoil brake. The results of the tests in the motion study are concise in the deformation after the force of the pressure when different constants of pressure are added. Secondly, the gun elevation mechanism is also tested with the SolidWorks features "Simulation analysis expert". The test there are different than the ones on the Hydraulic recoil brake, because the forces which put pressure on the details are highly concentrated on twisting, bending and applied pressure on the surface of the details. The objects that are tested in the Hydraulic recoil brake analysis are:

-The cylinder with added pressure 200 N/m2 (Fig.7.)
-The cylinder with added pressure 2000 N/mm2 (Pa) (Fig.8.)
-The Stem with added pressure 200 N/m2 (Fig.9.)
-The Stem with added pressure 2000 N/mm2 (Pa) (Fig.10.)

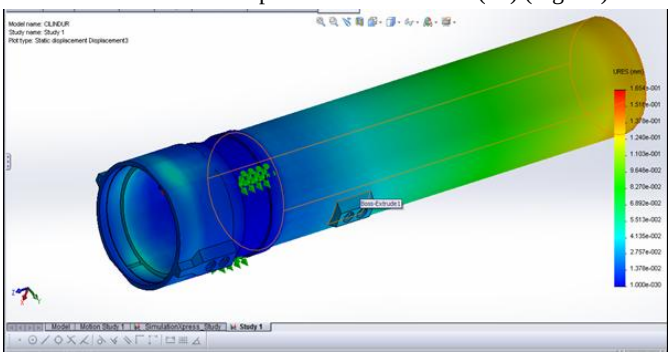


Fig.7 *-The cylinder with added pressure 200 N/m2*

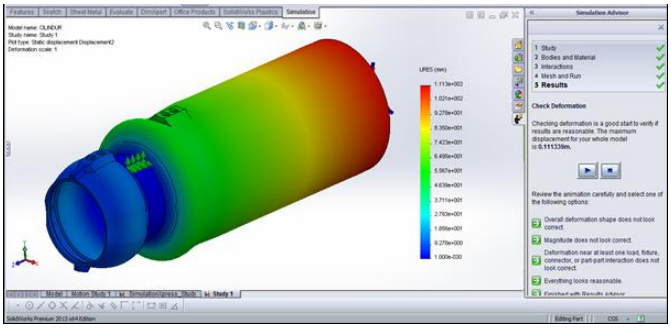


Fig.8 *-The cylinder with added pressure 2000 N/mm2 (Pa)*

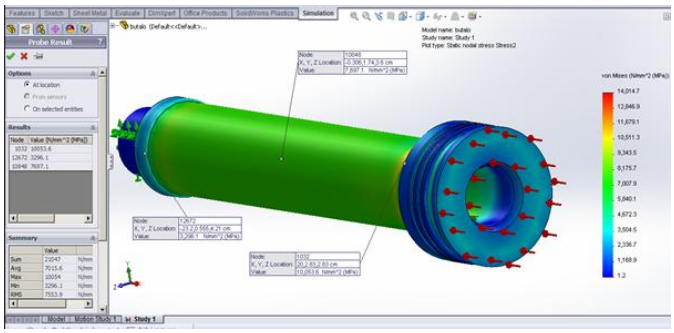


Fig.9.*The Stem with added pressure 200 N*

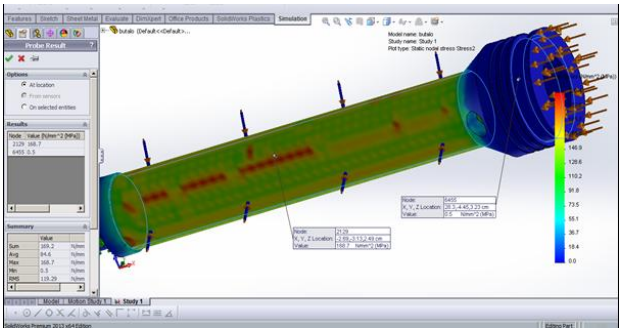


Fig.10. *The stem with added pressure 2000 N/mm2 (Pa)*

After the test with pressure, flow simulation test were conducted. The results show the speed of the fluid, the direction of the fluids and the places where friction is expected.

Furthermore, a motion study was conducted to see how the fluids move inside the Hydraulic recoil absorber and to observe the effectiveness of it by animation study. By using the same methods the parts of the Gun elevation mechanism were also tested by applying forces with their direction and size on the different objects of the mechanism. The parts which were tested are:

- The Worm shaft by applying the forces

P_{t1}= 322,2681N; P_{a1}= 606,8356N;

P_{r1}= 220,8701N. (Fig. 13)

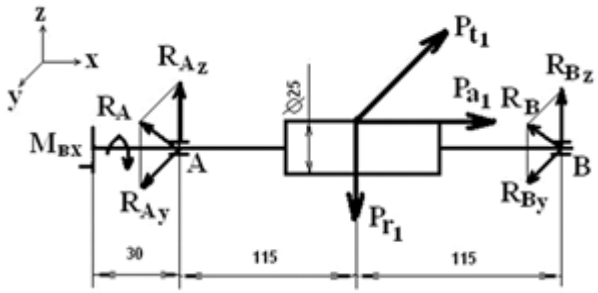


Fig.11. *The forces acting on the worm shaft and their directions.*

- The Shaft with worm gear and spur-wheel

P_{t2}= 606,8356N; P_{r2}= 202,8701N; P_{a2}= 322,2681N;

P_{t3}= 98100 N; P_{r3}= 35705, 48N. (Fig. 14.)

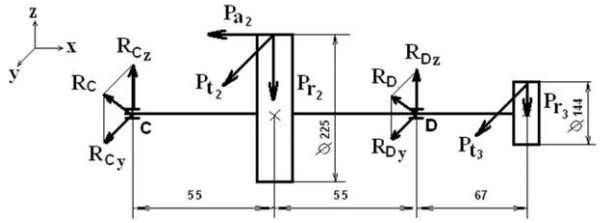


Fig.12 *The forces acting on the shaft and their directions.*

In figure 15 are shown the tests on the part of the Gun elevation mechanism. The tests show the deformation of the bodies when the forces, explained above, are added also, the weakest spots in the body of the object with constants.

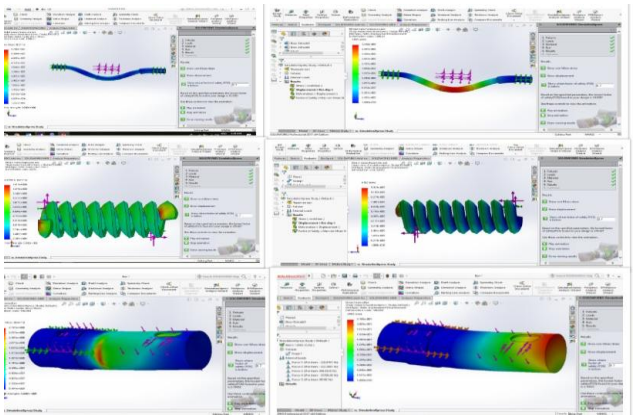


Fig.13. *Analysis on the pats of the Gun elevation mechanism*

4. Conclusion

The programs for mathematical calculations, design and analysis are making the education method more effective, faster and easier. Furthermore, for the armament specialists working process those programs are a great economy of deadlines, money and efforts. By using those programs the mistakes are less and the analysis are more accurate. They are also very helpful when it comes to educate cadets in armament design.