SCIENCE & MILITARY

No 2 | Volume 13 | 2018

Dear readers,

You are about to read the second edition of the Science & Military journal. This issue is published at Christmas time – in the time, when we can stop for a while, look back at all we have done this year and make plans for the upcoming year.

As the editor-in-chief, I am especially glad that the journal is becoming popular with more and more readers and experts from Slovakia and foreign countries. It proves that the quality and attractiveness of the journal is growing.

The Science & Military journal is one of few opportunities that enables regular publishing of original scientific articles focused on basic and applied research in the fields of military science.

And what are the plans of the editorial board for the future? Besides requirements regarding continuous improvement of the journal's quality in terms of its content and specialisation, we have set a demanding goal, which is to increase the journal's impact factor by indexing Science & Military into the SCOPUS database. A very important criterion for including the journal into this citation database is its high quality reviewed and evaluated by international experts as well as the publisher's reputation, diversity of writers and structure of an editorial board. The next criterion is the journal's popularity and availability, e. i. the number of its citations in the SCOPUS database.

Dear readers, let me briefly inform you about the contents of the latest edition, which contains six new and undoubtedly interesting scientific articles, which have been successfully reviewed.

The first among the reviewed articles, which was written by Jozef Perďoch and Zdeněk Matoušek titled **"Actual Trends in ELINT Objects Signal Classification"**, describes the approach to processed signals using information entropy as a parameter for evaluating the quality of information. This article deals with the simulation of sensors dislocation, which is affected by the same measurement error or different error for each individual sensor.

Another article titled **"Internet of Things – Environmental Security Vector"** was written by Martin Obert and Marcel Harakaľ. The aim of this article is to provide an outlook on current security issues in the field of Internet of Things (IoT). In the first part of the article, authors focused on IoT design and conditions that influence its design on protocol level as we see it today. The second part is focused on different types of attacks analysis in IoT environment. Finally, authors introduced Attack vector in IoT environment and coincident product-life security matrix as static base for further research.

The author Daniel Roman wrote article **"Critical Infrastructure Protection in the Context of the Security Network"**. In this article author has intended to argumentatively support the need for an integrated approach to the security of the identified "pillar systems" by focusing on critical infrastructure protection and designing, planning and deploying military actions. For the first time, based on integrating the dynamics of the risks and the vulnerabilities of the social systems, author have argumentatively developed the concept of network interaction. By monitoring and analysing the essential descriptive parameters of each security field it is possible to decipher their security states due to the identified network connections, and moreover, anticipate a potential crisis or the possible occurrence of a major negative event.

The following article **"Risk Assessment for Critical Infrastructure in the Conditions of Ukraine"** by Serhii Ivaniuta deals with the character of changes in natural and man-made threats for critical infrastructure in the conditions of Ukraine. Risk assessment for critical infrastructure from emergency situations in Ukraine with regard to the European Union approach is provided.

Among the articles in this issue, you can find the article written by Roman Markovič titled "**The Effects of Two Different Physical Training Programs on Movement Performance of Professional Soldiers"**. The aim of this article is to investigate the influence of two different physical education programs on increasing the movement performance of professional soldiers and their results in the annual physical fitness test.

In 2015, political alteration at a central level took place in Poland. The conservative right-wing party Law and Justice (Polish: PiS) emerged as the winner of the parliamentary elections. A range a changes followed. One of them was establishment of the fifth type of the Armed Forced of the Republic of Poland - the Territorial Defence Forces. This is the main topic of the final article titled "**The Territorial Defence Forces as the Fifth Type of the Armed Forces of the Republic of Poland** (Genesis and Political Background of their Formation as Well as Attitude to them Among Society)" written by Katarzyna Dojwa-Turczynska

Dear readers, on my behalf and on behalf of the editorial board, I would like to wish you all the best for the coming year 2019 and thank you for your interest and quality articles.

Col. (ret.) Prof. Eng. Marcel HARAKAĽ, PhD.
Chief of the editorial board

Reviewers

Assoc. Prof. Mgr. Dr. Vladimír **BLAŽEK**, CSc.	Academy of the Police Force in Bratislava, SK
Prof. Eng. Ladislav **BUŘITA**, CSc.	University of Defence Brno, CZ
Prof. Eng. Jaroslav **ČECHÁK**, PhD.	URC SYSTEMS, Brno, CZ
Assoc. Prof. Eng. Peter **FUCHS**, PhD.	Slovak University of Technology in Bratislava, SK
Assoc. Prof. Eng. Martin **HROMADA**, PhD.	Tomas Bata University in Zlín, CZ
Assoc. Prof. Eng. Josef **KELLNER**, CSc.	University of Defence Brno, CZ
Assoc. Prof. Eng. Bohuš **LEITNER**, PhD.	University of Žilina, SK
Prof. dr hab. Jan **MACIEJEWSKI**	University of Wroclaw, PL
Mgr. Martin **MOKOŠÁK**, PhD.	Comenius University in Bratislava, SK
Prof. nadzw. dr hab. Antoni **OLAK**, Dr.h.c.	Higher School of Business and Entrepreneurship in Ostrowiec Swietokrzyski (PL)
PhDr. Jiří **SEKANINA**, PhD.	University of Defence Brno, CZ
Assoc. Prof. Eng. Branislav **SOBOTA**, PhD.	The Technical University of Košice, SK

ACTUAL TRENDS IN ELINT OBJECTS SIGNAL CLASSIFICATION

Jozef PERĎOCH, Zdeněk MATOUŠEK

Abstract: The main task of electronic intelligence is to detect, measure and analyze parameters, identify and track electronic objects that works with pulse modulation of signals. Electronic intelligence objects identification means the process in which every electronic intelligence object is assigned to its appropriate class, type, or model. The lower level of the electronic intelligence objects identification is ensured in the classification process. A further part of this article will be devoted to analyzing current trends in the electronic intelligence objects classification.

Keywords: electronic intelligence; intrapulse modulation; radar signal processing; signal analysis; signal processing algorithms.

1 INTRODUCTION

Intelligence preparation of the battlefield (IPB) is an integral part of the decision–making process of commanders and staffs. The structure of IPB includes, among other types of intelligence, the technical types of intelligence, so called signal intelligence (SIGINT). From the point of view of intelligence typology, the SIGINT can be divided into three basic groups:

1. Communication Intelligence – COMINT.
2. Electronic Intelligence – ELINT.
3. Measurement and Signature Intelligence – MASINT.

The main task of electronic intelligence is to detect, measure and analyze parameters, identify and track electronic objects that works with pulse modulation of signals. ELINT objects identification means the process in which every ELINT object is assigned to its appropriate class, type, or model. Objects identification is typically performed on the basis of their signal characteristics analysis.

The structural schema of the ELINT objects identification is shown in the Figure 1.

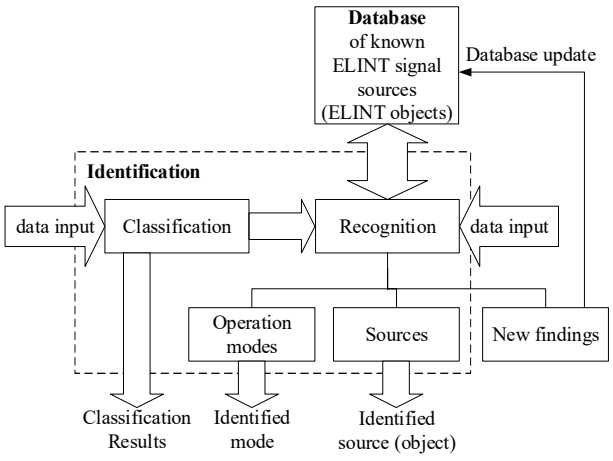


Fig. 1 The structural schema of the ELINT objects identification
Source: authors.

According to the achieved level (grade of quality), the ELINT objects identification can be divided into ELINT objects classification and ELINT objects recognition.

The lower level of the ELINT objects identification is ensured in the classification process. The ELINT objects classification is understood as a systematic process of sorting them into predefined groups based on established criteria.

A further part of this article will be devoted to analyzing current trends in the ELINT objects classification.

2 ELINT OBJECTS

The progressive trend in the technical area of modern ELINT objects (hereinafter referred to as Objects) is the use of complex signals, including intrapulse modulated radio pulses. These signals must meet both the minimal values of Low Probability of Intercept (LPI) and the need to increase the probability of correct target detection at decreasing values of Signal–to–Noise Ratio (*SNR*). For the classification of objects which uses intrapulse modulation it is necessary to extend the measurements and analysis of their parameters also to the time – frequency domain.

Depending on changes in monitored parameters within a single radio pulse, intrapulse modulation (IM) used in modern objects can be divided into two basic groups:

1. Frequency IM.
2. Phase IM.

2.1 ELINT objects with frequency intrapulse modulation

Pre–determined changes in carrier frequency are observed during the duration of one radio pulse in the signals of these objects. These changes may be continuous or discrete.

Linear (LFM–IM – upward or downward) or nonlinear (NLFM–IM – logarithmic, quadratic, convex, or concave) frequency changes may occur in signals received from objects operating with continuous frequency IM (FM–IM).

For discrete frequency IM (MFSK–IM), intrapulse modulations are defined as 2FSK, 4FSK, multiple FSK and Costas codes.

2.2 ELINT objects with phase intrapulse modulation

Pre–determined changes in phase are observed in duration of one radio pulse for these objects signals. These changes may be two–state (binary) or multi–state (multiphase, polyphase).

For objects operating with a binary phase IM signals (BPSK–IM), Barker and Walsh–Hadamard codes are used in particular.

Frank codes, Golomb codes, Zadoff–Chu codes, P1, P2, P3, or P4 codes are used in particular for objects operating with a polyphase IM.

The schematic partition of ELINT objects in terms of the used IM is shown in the Figure 2.

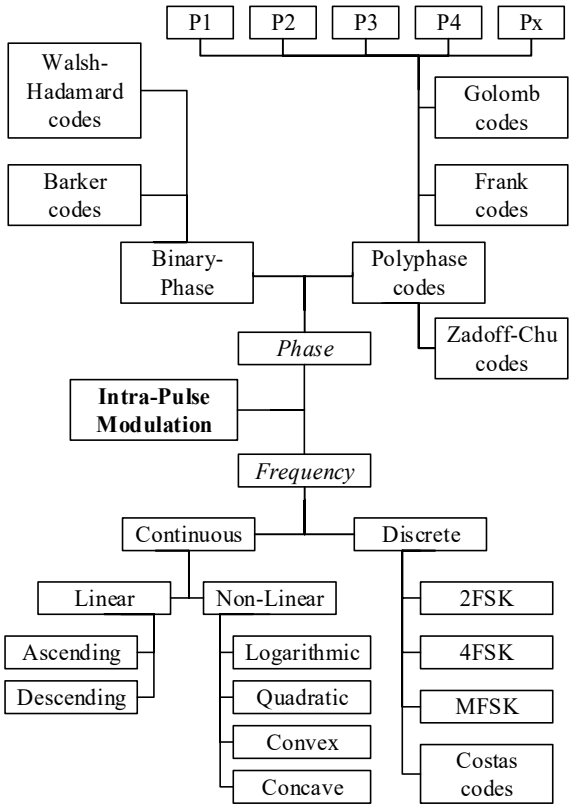


Fig. 2 The schematic partition of ELINT objects in terms of the used IM
Source: authors.

When classifying objects, it is necessary to work on the level of separate radio pulses. According to the analyzed descriptors of their signals it is then possible, for the purposes of performing the classification, to divide the objects into the above mentioned groups (Figure 2).

3 ELINT OBJECTS CLASSIFICATION

An indispensable and important part of objects analysis and identification is their initial classification into individual, predefined groups. Objects classification can be, similar to [1], divided into two basic steps:

1. Input signal preprocessing.
2. Application of the classification algorithm itself.

In addition to the primary task, which is the preparation of the analyzed signal for classification, the preprocessing of the object signals can include other additional algorithms. These algorithms can be included, for example, algorithm for noise reduction, carrier frequency measurement algorithm, algorithm for evaluating the level of signal and noise, and the like.

The design of the signal preprocessing algorithm is dependent on the objects classification algorithm used. The basic requirement of this algorithm is, as a rule, to create appropriate conditions to ensure the maximum probability of correct classification P_C at minimal values of *SNR*. It follows from this that both the preprocessing algorithm and the classification algorithm itself form a compact whole. Algorithms for performing the objects classification itself can be split into the following groups [2]:

1. Likelihood–based (LB) classifiers.
2. Statistical (distribution test) – based classifiers.
3. Feature–based (FB) classifiers.
4. Classifier algorithms based on artificial intelligence and machine learning.
5. Algorithms based on a combination of previous algorithms.

3.1 Likelihood-based classifiers

Likelihood–based (LB) classifiers can be interpreted as multiple testing of so–called modulation hypotheses [2].

In the algorithm, the H_i hypotheses are tested by assigning the i – type of object (IM type) to the input signal, $i = 1,...,N_{MOD}$, where N_{MOD} is the total number of defined object types (defined IM types).

A probability density function is created from the samples of the analyzed signal. Tested probability density function is then compared with the theoretical models of probability density functions for different object types.

LB classifiers are divided into [2]:

1. ML classifiers [3] (ML – Maximum Likelihood).
2. ALRT classifiers [1], [4] (ALRT – Average Likelihood Ratio Test).
3. GLRT classifiers [1], [4] (GLRT – Generalized Likelihood Ratio Test).
4. HLRT and quasiHLRT classifiers [1], [4] (HLRT – Hybrid Likelihood Ratio Test).

The essence of the LB classifiers consists of two steps [2]. In the first step, the probability of the object being related to a predefined object model – modulation hypothesis is evaluated [2]. Probability density functions are derived by the selected model.

In the second step, the calculated probability values of the individual modulation hypotheses are compared in order to decide on belonging to the one of predefined groups of objects.

If necessary, the use of thresholds can also be included to the decision algorithm. It is possible to increase the reliability of the entire classification algorithm by including thresholds.

The simplest criterion for deciding on belonging to one of the groups of objects is the adoption of a modulation hypothesis with a maximal probability of belonging (ML classifiers).

The disadvantage of LB classifiers is the high demands on the computational power and the need for all information about the effects of the transmission path to the classified objects signal.

3.2 Statistical (distribution test)-based classifiers

If the samples of objects signal are sufficiently long, distribution function of this signal becomes an interesting from the viewpoint of its classification. According to [2] it is clear that the course of the distribution function of signals is influenced in particular by the following two factors:

1. Used intrapulse modulation.
2. Parameters of transmission path.

Assuming the transmission path parameters are known, only the kind of intrapulse modulation is the variable in the distribution function of the signal.

If the distribution functions of different object groups (etalons) are available, there is one, which best matches the distribution function of the objects signal that we want to classify. The evaluation of similarity between the individual distribution functions of objects signal is known as a Goodness of Fit (GoF) test. This test indicates how the distribution function of the classified signal matches the reference distribution function. In the last step, the classification process is completed by selecting the hypothetical distribution function of the signal that best meets the compliance criteria (highest achieved value in the GoF test).

The most commonly used GoF tests to analyze and classify objects signals (IM signals) belongs:

1. Kolmogorov- Smirnov test (K–S test) [5], [6].
2. Cramer- von Mises test (C–vM test) [6].
3. Anderson- Darling test (A–D test) [6].

The disadvantage of statistical approaches in the area of ELINT objects classification is the high demand for computational performance. Their advantage is that they use so-called nonparametric statistical tests that do not have specific requirements for the probability distribution pattern of the analyzed data. For this reason, nonparametric statistical tests are sometimes referred to as distribution free tests.

3.3 Feature-based (FB) classifiers

Likelihood-based and statistical-based classifiers, which are based on decision-making processes in the domain of theoretical knowledge, provide a relatively high probability of proper classification (P_C). However, their demands for high computational performance have led to the development of classifiers based on parametric approaches (FB classifiers).

These algorithms provide a sufficient probability of proper classification, and require lower computational power. In the classification, predetermined signal parameters are compared with defined threshold values. The most commonly used FB classifiers can be categorized:

1. Spectral analysis–based algorithms.
2. Wavelet transform–based algorithms.
3. Signal high order statistics–based algorithms (cumulant–based features and moment–based features).
4. Signal cyclostationarity–based algorithms.
5. Instantaneous amplitude, phase and frequency–based algorithms.

A key role in design of classifiers working on the principle of the above algorithms, is the need to create a so–called decision tree. In the decision tree, the individual modulation groups must be subdivided into several subgroups until each object is distinct from the remaining objects. An example of schematic structure of decision tree is shown in the Figure 3.

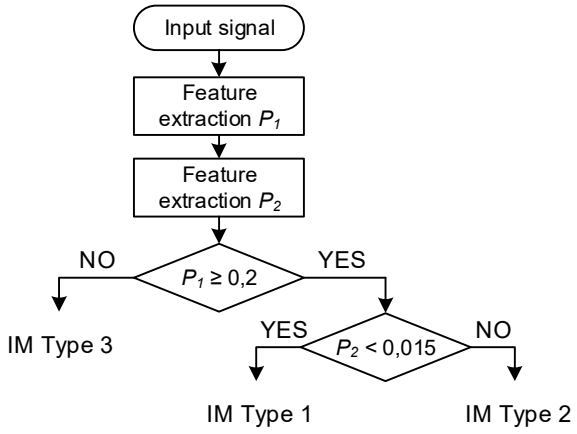


Fig. 3 An example of schematic structure of decision tree
Source: authors.

The easiest way to make the right decisions within the decision tree is to set thresholds at each branch of the algorithm. Threshold levels are determined most often for the theoretical objects signals without additive noise.

Group of algorithms based on parametric approaches can also include an algorithm that is based on evaluating changes in the instantaneous frequency and changes of the instantaneous phase of the classified object signal [7]. This algorithm works with a complex I/Q signal that is defined by equations

$$s_I(n) = A(n)cos\{2\pi f_C / f_s n + \varphi'(n) + \varphi\}, \quad (1)$$

and

$$s_Q(n) = A(n)sin\{2\pi f_C / f_s n + \varphi'(n) + \varphi\}, \quad (2)$$

where $s_I(n)$ is the real part of the complex signal, $s_Q(n)$ is the imaginary part of the complex signal, $A(n)$ is the signal amplitude, f_C is the carrier frequency, f_S is the sampling frequency, $\varphi'(n)$ is the intrapulse modulation function and φ is the initial phase.

In this algorithm, a decision tree is also used, in which the values of signal parameters are compared with set thresholds. Within the framework of the algorithm, the objects signal classification is realized into the following classes:

1. Objects without IM (WO–IM).
2. Objects with LFM–IM.
3. Objects with BPSK–IM.

The differences in the instantaneous phase of the signal between the samples are the basis for calculating the behavior of the changes in its instantaneous frequency over time (one-order phase difference). Examples of behavior of instantaneous frequency changes over time for above object classes are shown in the Figures 4, 5 and 6.

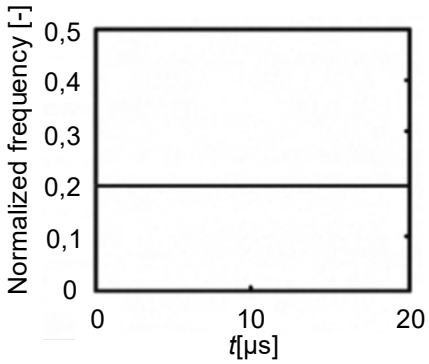


Fig. 4 Instantaneous frequency changes over time for WO–IM signals
Source: [7].

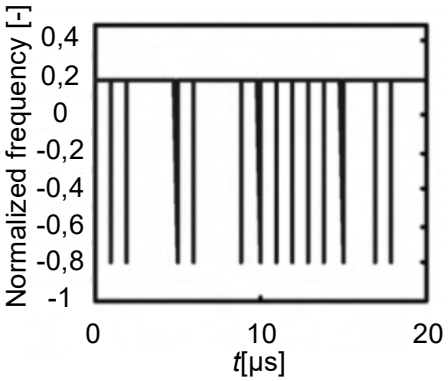


Fig. 5 Instantaneous frequency changes over time for BPSK–IM signals
Source: [7].

For the objects signal operating without IM or with BPSK–IM there is a typical zero frequency deviation, which is interrupted by typical peaks in BPSK-IM signal at the time of phase changes.

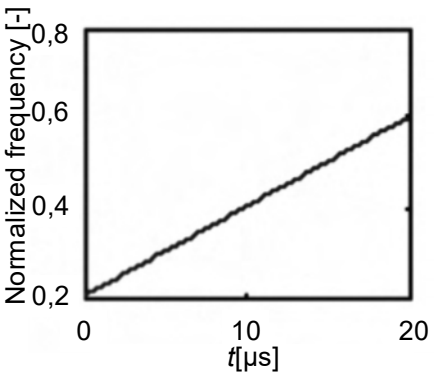


Fig. 6 Instantaneous frequency changes over time for LFM–IM signals
Source: [7].

For the objects signal working with linear FM–IM there is a typical frequency deviation in the behavior of instantaneous frequency.

The graphical representation of the achieved results of the ELINT objects classification by the algorithm based on the evaluation of the instantaneous frequency and phase is shown in the Figure 7.

Experiments to verify the functionality of the algorithm were performed for objects signals operating at a 10 MHz carrier frequency at a sampling rate of 100 MHz. The pulse width was constant during the simulations ($PW = 2$ μs) and the frequency deviation value for LFM–IM signals was $\Delta f = 5$ MHz. For BPSK–IM signals, random coding was used at 0.4 μs sub–pulse width. The probability of correct classification was evaluated at *SNR* levels from 0 to 10 dB, with 1 dB step, using Monte-Carlo method with 500 tests for each *SNR* level.

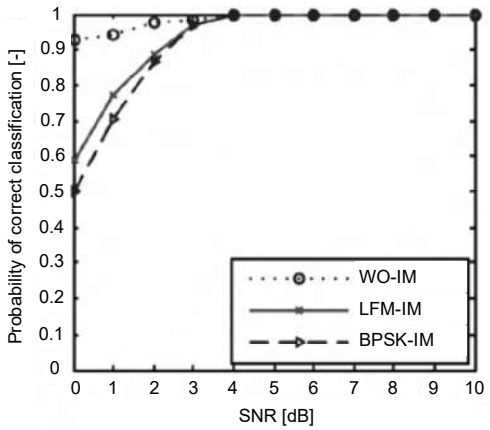


Fig. 7 Graphical representation of the achieved results of the objects signals classification by the algorithm based on the evaluation of the instantaneous frequency and phase
Source: [7].

Simulations found that this algorithm works with the probability of correct classification of 0.9 at SNR = 3dB and above. The practical implementation of the proposed algorithm was accomplished by its implementation into the digital signal processor type TS201. By testing in real conditions, the time required for recognition was also evaluated, which did not exceed 0.1 milliseconds.

3.4 Classifier algorithms based on artificial intelligence and machine learning

In likelihood-based classifiers, statistical-based classifiers and feature-based classifiers are mostly used multi-step decision trees where a different property of the analyzed signal is used at each stage of the decision process. The use of the decision tree and the subsequent optimization of the thresholds in the decision-making process brings with it higher demands on computational performance and the time-consuming nature of the whole objects classification process. In order to minimize the deficiencies of these algorithms, various algorithms of machine learning and artificial intelligence were gradually tested and subsequently applied in the classification process. Such algorithms can be divided into the following groups [2]:

1. K-Nearest Neighbor (KNN) classifier algorithms [8], [9].
2. Support Vector Machine (SVM) classifier algorithms [10].
3. Generalized linear regression algorithms [11].
4. Genetic Algorithms and Genetic Programming [12], [13].
5. Artificial Neural Network algorithms.

Using the above classifier algorithms, it is possible to classify objects signals with a probability of correct classification from 0.9 to 0.98 for SNR values above from –3 dB to 6 dB. The total time required to classify a single pulse varies from 0.1 milliseconds to 10 milliseconds. The main advantages of objects signal classification using machine learning and artificial intelligence techniques include lesser demands on computational performance and a significant acceleration of the classification process itself. Among their disadvantages are e.g. the need to re-learn neural networks when classifying new objects signals.

The group of algorithms based on artificial intelligence and machine learning can also include the algorithm for the automatic objects signal classification mentioned in [14]. The algorithm uses two parallel working neural networks in its operation. A parametric vectors are supplied to their inputs. Parametric vectors are created by selected statistical signal parameters, its power spectral density (PSD), frequency and Choi – Williams distribution. Using this algorithm, it is possible to classify objects signal into the following eight classes:

1. Objects with LFM–IM.
2. Objects with MFSK–IM and Costas codes.
3. Objects with BPSK–IM.
4. Objects with Frank codes.
5. Objects with polyphase P1 codes.
6. Objects with polyphase P2 codes.
7. Objects with polyphase P3 codes.
8. Objects with polyphase P4 codes.

A complex $y(n)$ signal, which consists of a mixture of the detected complex signal $x(n)$ and the additive white Gaussian noise (AWGN) $N(n)$, is used in the classification. The model of the classified signal is given by the equation

$$y(n) = x(n) + N(n) = Ae^{-j\varphi(n)} + N(n), \qquad (3)$$

where A is the complex amplitude and $\varphi(n)$ is the phase of complex signal.

The proposed solution utilizes a three-stage preprocessing of the input signal:

1. The carrier frequency evaluation, which is defined as the mean frequency of the signal bandwidth.
2. Evaluation of the signal sub-pulse width.
3. Creation of parametric vectors (PV).

Based on the sub-pulse width, the sampling frequency for digital processing is set in the next step. Object classification itself is performed through two parallel multilayer perceptron (MLP) based neural networks.

The schematic structure of the algorithm for the automatic classification of the objects by neural networks using the selected statistical parameters of their signals is shown in the Figure 8.

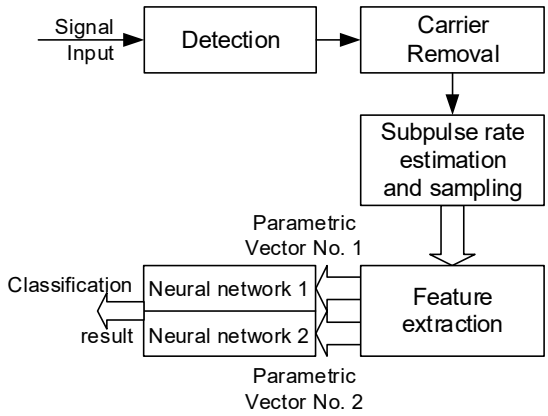


Fig. 8 Schematic structure of the algorithm for the automatic objects classification by neural networks using the selected statistical parameters of their signals
Source: [14].

The graphical representation of the results obtained by the algorithm for the automatic classification of the objects by neural networks using selected statistical parameters of their signals is shown in the Figure 9.

On the basis of the experiments performed, it can be stated, that the proposed objects classifier works with the probability of correct classification $P_C = 0.98$ at *SNR* above 6dB.

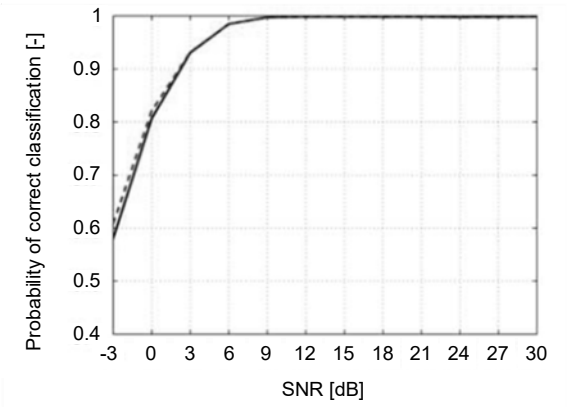


Fig. 9 Graphical representation of the results obtained by the algorithm for the automatic classification of the objects by neural networks using selected statistical parameters of their signals
Source: [14].

3.5 Algorithms based on a combination of previous algorithms

Given the ever-evolving process of generating different specific types of object signals, it is very difficult to unify the categorization of all kinds of classification algorithms. Algorithms that use combinations of the above algorithms are increasingly used. This creates a combination of object signals classification algorithms, such as:

1. Algorithm based on the ambiguity function [15].
2. Algorithm based on the modulation components analysis (MCA) [16].

3.5.1 Algorithm based on the ambiguity function

To ensure proper operation of this algorithm, ambiguity function (AF) is calculated in the preprocessing part. Ambiguity function is defined by the equation

$$\chi'(\tau, f_D) = \int_{-\infty}^{\infty} s(t)s^*(t+\tau)e^{j2\pi f_D t}\,dt, \qquad (4)$$

where $s(t) = u(t)e^{j2\pi f_C t}$, f_C is carrier frequency, τ is delay, f_D is Doppler frequency shift and * means complex conjugation.

Using Amplitude of Ambiguity Function (AAF), it is possible to create an energy distribution of objects signals in the time-frequency domain. For different IM classes, it is then possible to see significant differences between these energy distributions. With this algorithm, it is possible to classify objects into the following classes:

1. Objects without IM (WO–IM).
2. Objects with LFM–IM.
3. Objects with BPSK–IM and QPSK–IM.
4. Objects with 2FSK–IM and 4FSK–IM.

To quantify the differences in the energy distribution of object signals in the time-frequency domain are used:

- Frequency Energy Accumulation Function (FEAF) $E(f_D)$.
- Time-Domain Extremum Function (TEF) $M(\tau)$.

Other parameters that are used in the classification process with this algorithm are:

- Measurement of Bandwidth (MB).
- Measurement of Triangular Shape (MTS).
- Measurement of the Number of Peaks (MNP).

Experiments to verify the operation of the algorithm were performed for each considered IM type. The sampling frequency for the analyzed signals was set to 100 MHz, pulse width values *PW* were set to 3, 5 and 7 microseconds, *SNR* values were set from –3dB to 5dB in 1dB increment. This classifier worked with a probability of correct classification greater than 0.9 for the following *SNR* values:

1. For objects without IM and objects with LFM–IM for *SNR* values above –2 dB.
2. For objects working with the other listed IM for *SNR* values above –1 dB.

3.5.2 Algorithm based on the modulation components analysis (MCA)

Object signals classification is divided into two stages in these algorithm. In the first stage, object signals are classified into the following three main groups:

1. Objects working without IM and with continuous FM–IM.
2. Objects working with FSK–IM.
3. Objects working with PSK–IM.

The first stage is labeled MCA (Modulation Components Analysis) and instantaneous frequency rate *IFR*(*t*) is evaluated in this stage. *IFR*(*t*) is calculated according to the equation

$$IFR(t) = \frac{1}{2\pi}\frac{d^2\varphi(t)}{dt^2}, \quad (5)$$

where $\varphi(t)$ is phase of analyzed signal.

For different object signals classes, the *IFR*(*t*) function curves are characterized by different sequences. An examples of *IFR*(*t*) function curves for the above object signals classes are shown in the Figures 10, 11 and 12.

In the second stage, a more detailed classification of objects signals is made within one of the above main classes. For this purpose, the so–called *IFL* curve (Instantaneous phase and Instantaneous Frequency Law) was defined. Calculation of the *IFL* curve is realized according to the equation

$$IFL(t_i) = \underset{f}{argmax}\left|\int_R GCM_2^1[s,t_i](\tau)e^{-j2\pi f t}d\tau\right| \quad (6)$$

for $\tau\epsilon\langle -T_W, T_W\rangle$,

where *GCM* is generalized complex moment described in [16].

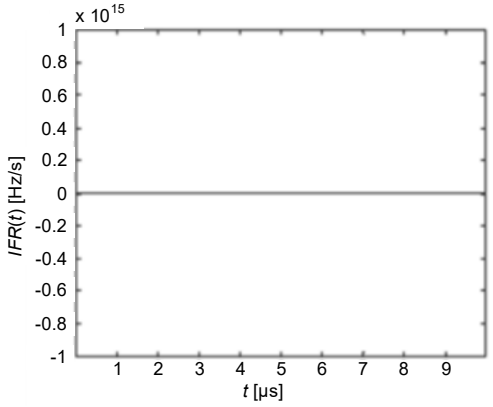


Fig. 10 *IFR*(*t*) function curve for continuous FM-IM signal
Source: [16].

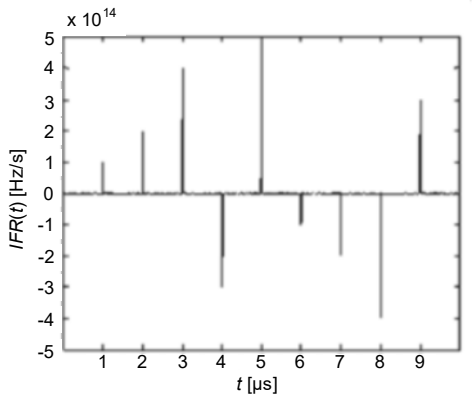


Fig. 11 *IFR*(*t*) function curve for FSK-IM signal (Costas code)
Source: [16].

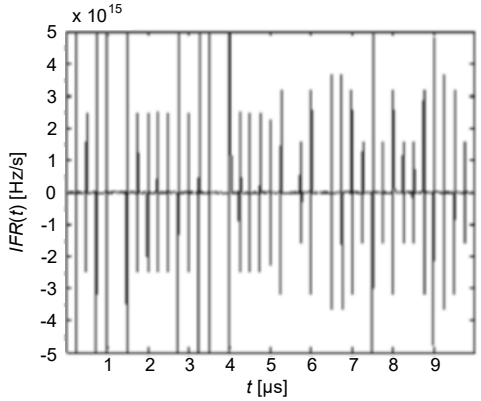


Fig. 12 *IFR*(*t*) function curve for PSK-IM signal (QPSK)
Source: [16].

According to the *IFL* curve, it is possible, for example, in the FSK–IM group to distinguish the number of frequencies used within one radio-pulse. The graphical representation of the results of the object signals classification algorithm based on the modulation components analysis is shown in the Figures 13, 14 and 15.

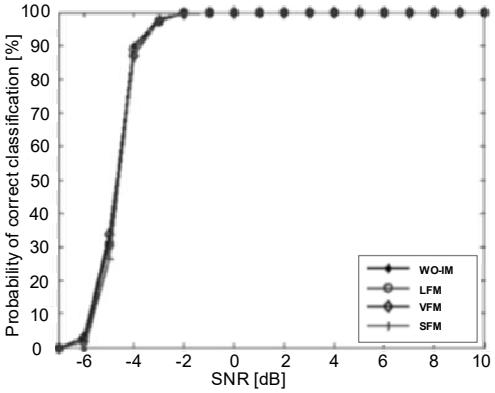


Fig. 13 Object signals classification algorithm based on the modulation components analysis – results for cWO–IM and FM–IM signals
Source: [16].

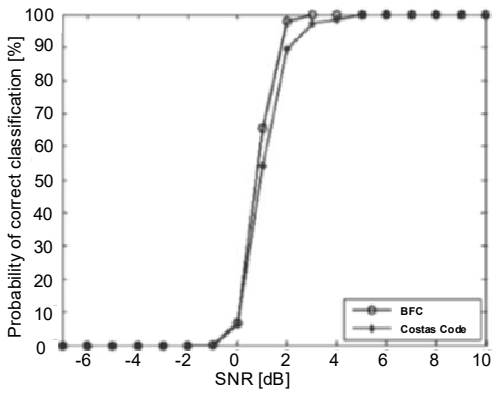


Fig. 14 Object signals classification algorithm based on the modulation components analysis – results for FSK–IM signals
Source: [16].

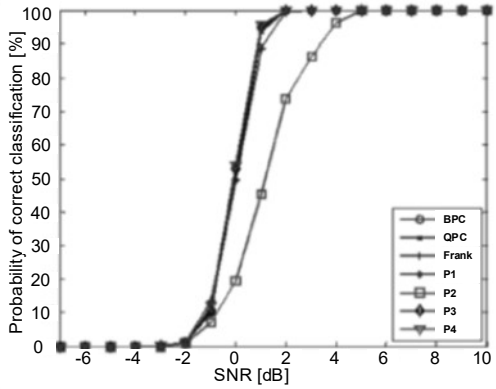


Fig. 15 Object signals classification algorithm based on the modulation components analysis – results for PSK–IM signals
Source: [16].

Experiments to verify the operation of this algorithm have been performed for each objects signals group separately in [16]. *SNR* values have been set from –3 to 10 dB. The probability of correct classification of 0.98 was exceeded on the following *SNR* values:

1. Objects without IM and with continuous FM–IM for *SNR* values above –3 dB.
2. Objects with FSK–IM for *SNR* values above 3 dB.
3. Objects with PSK–IM for SNR values above 4 dB.

4 CONCLUSION

Different algorithms for ELINT object classifiers have been described in the paper. The disadvantage of LB classifiers is the high demand on computational performance (CP) and the need for all information about the effects of the transmission path to the classified objects signal. The disadvantage of statistical approaches is the high demand on CP. Their advantage is that they use so-called nonparametric statistical tests that do not have specific requirements for the probability distribution pattern of the analyzed data. FB algorithms require lower CP. The main advantages of ELINT objects signal classification using machine learning and artificial intelligence techniques include lesser demands on CP and a significant acceleration of the classification process itself. Among their disadvantages are e.g. the need to re-learn neural networks when classifying new objects signals. Overall, the values of the probability of correct classification of described algorithms varies from 0,9 to 0,98 on SNR above –3 dB.

References

[1] DOBRE, O. A., ABDI, A., BAR-NESS, Y., SU, W.: Survey of automatic modulation classification techniques: classical approaches and new trends. In *IET Communications,* Vol. 1, No. 2, pp. 137-156, April 2007. doi: 10.1049/iet-com: 20050176.

[2] ZHECHEN, Z., ASOKE, K. N.: *Automatic Modulation Classification Principles. Algorithms and Applications.* London, UK : Brunel University. ISBN 978-1-118-90649-1.

[3] WEN, W., MENDEL, J. M.: Maximum-likelihood classification for digital amplitude-phase modulations. In *IEEE Transactions on Communications*, Vol. 48, No. 2, Feb 2000, pp. 189-193.

[4] KARAMI, A.: *Automatic Modulation Detection.* Dalhousie University, Electrical Engineering Department, 2015.

[5] WANG, F., XU, R., ZHONG, Z.: *Low complexity Kolmogorov-Smirnov modulation classification.* 2011 IEEE Wireless Communications and Networking Conference, Cancun, Quintana Roo, 2011, pp. 1607-1611.

[6] AZIM, A. W., KHALID, S. S., ABRAR, S. *Analysis of modulation classification techniques using Goodness of Fit testing*. 2013 IEEE 9th International Conference on Emerging Technologies (ICET), Islamabad, 2013, pp. 1-6.

[7] ZENG, D. G., XIONG, H., LONG, K., Y., TANG, B.: *A fast recognition algorithm for three kinds of intra-pulse modulation signals*. 2009 IET International Radar Conference, Guilin, 2009, pp. 1-4.

[8] BHATIA, N. and VANDANA: Survey of Nearest Neighbor Techniques. In *International Journal of Computer Science and Information Security*, Vol. 8, No. 2, 2010.

[9] GUO, G., WANG, H., BELL, D.: *KNN Model based Approach in Classification.* Springer Berlin, Vol 2888, OTM 2003: On the Move to

Meaningful Internet Systems 2003: CoopIS, DOA and ODBASE, 2003, pp. 986-996.
[10] AWAD, M., KHANNA, R. Support Vector Machines for Classification. In *Efficient Learning Machines.* Apress, Berkeley, CA, 2015. pp. 39-66. ISBN 978-1-4302-5989-3.
[11] JAMES, G., WITTEN, D., HASTIE, T. TIBSHIRANI, R.: *An Introduction to Statistical Learning.* Springer, 2013. ISBN 978-1-4614-7137-0.
[12] ROBU, R., HOLBAN, S.: *A genetic algorithm for classification. Recent Researches in Computers and Computing - International Conference on Computers and Computing.* ICCC'11, 2011, pp. 52-56. ISBN 978-1-61804-000-8.
[13] PEI, M., GOODMAN, E. D., PUNCH, W. F., DING, Y.: *Genetic Algorithms for Classification and Feature Extraction*, 2018. 355-7516.
[14] LUNDÉN, J., KOIVUNEN, V.: Automatic Radar Waveform Recognition. In *IEEE Journal of Selected Topics in Signal Processing*, Vol. 1, No. 1, June 2007. pp. 124 – 136.
[15] ZENG, D., XIONG, H., WANG, J., TANG, B.: *An Approach to Intra-Pulse Modulation Recognition Based on the Ambiguity Function.* Circuits Syst Signal Process (2010) 29, April 2010. pp. 1103–1122.
[16] WANG, P., QIU, Z., ZHU, J., TANG, B.: Autonomous radar pulse modulation classification using modulation components analysis. In *EURASIP Journal on Advances in Signal Processing*, 2016, 2016:98. Available at: https://doi.org/10.1186/s13634-016-0394-3.

Eng. Jozef PERĎOCH
Armed Forces Academy of General M. R. Štefánik
Department of Electronics
Demänová 393
031 06 Liptovský Mikuláš
Slovak Republic
E-mail: jozef.perdoch@aos.sk

Assoc. Prof. Eng. Zdeněk MATOUŠEK, PhD.
Armed Forces Academy of General M. R. Štefánik
Department of Electronics
Demänová 393
031 06 Liptovský Mikuláš
Slovak Republic
E-mail: zdenek.matousek@aos.sk

Jozef Perďoch – was born in Čadca, Slovakia in 1979. He received his M.Sc. (Eng.) at the Armed Forces Academy of general Milan Rastislav Štefánik in Liptovský Mikuláš. He started his dissertation studies in 2017, his research interests are focused on intrapulse modulated ELINT signals analysis and identification. Currently he is working as an assistant professor at the Electronics Department, Armed Forces Academy of general Milan Rastislav Štefánik in Liptovský Mikuláš.

Zdeněk Matoušek – was born in Frýdlant, Czech Republic in 1961. He received a M.Sc. (Eng.) from the Radar Technology Department, Military Academy in Liptovský Mikuláš in 1985. In 2000 he successfully finished his PhD. studies in electrical engineering. In 2008 he finished his habilitation thesis at the University of Defence in Brno, Czech Republic. Currently he is working as an associate professor at the Electronics Department, Armed Forces Academy of general Milan Rastislav Štefánik in Liptovský Mikuláš. His areas of research are intelligence, electronic intelligence, RF antennas and radioelectronics systems.

INTERNET OF THINGS - ENVIRONMENTAL SECURITY VECTOR

Martin OBERT, Marcel HARAKAĽ

Abstract: Aim of this paperwork is to provide an outlook on current security issues in the field of Internet of Things (IoT). IoT technology is rapidly spreading technology not only within industrial area. In the first part of the article, we focus on IoT design and conditions that influence its design on protocol level as we see it today. To highlight the differences, we use comparative approach in order to compare IoT with conventional Internet. The second part is focused on different types of attacks analysis in IoT environment. Finally, we introduce Attack vector in IoT environment and coincident product-life security matrix as static base for further research.

Keywords: Attack vector; Internet of Things; traditional Internet; machine to machine; cyber-physical space; cyberthreat; fog computing; cloud computing.

1 INTERNET OF THINGS COMPARISON

Before we will start to analyse the security issues of the Internet of Things (IoT), we should figure out differences between the IoT and conventional Internet (in some sources also recognized as "Traditional Internet" [2]) in their principles. Traditional Internet, as we know today, has been developed mainly to support people with certain level of data automation processing. From technical point of view, it is an interaction between human being and software via input and output hardware resources. Once data is sent over input device to a computing system, it will be computing according to pre-programmed algorithm, result can be directly returned to a user or can be used to make any changes in program's data or do both. The role of the Internet in this conventional meaning is to create connectivity between users and computers with their peripheral devices. If we look at the traditional Internet, the program control is processed only by a human interaction with data environment. In spite of this traditional approach, IoT has a brand-new and enhanced philosophy, which is nowadays based on intelligent communication among smart things (sensors and actuators) more often controlled by artificial intelligence. Such enhancing of the commonly used communication models has implied into one extra layer and it is interaction among objects (generally adopted as things). In [2] the IoT and Traditional Internet is characterized, over cyber-physical space interaction, as follows:

1. Interaction purely sensed and actuated by humans. It is designated as Human to Human (H2H) communication.
2. Interaction sensed and actuated by machines but controlled by humans locally. It is designated as Human to Machine (H2M) communication.
3. Interaction purely sensed and actuated by machines and controlled by humans only remotely. This is designated as Machine to Machine (M2M) communication.

Such classification is a chronological conclusion of developing of the global networks, the Internet and consequently World Wide Web [2]. However, for our purpose we will be deeper collaborated only with the state of interaction as is described in the point 3.

2 CYBER THREAT DEFINITION IN INTERNET OF THINGS

The difference between traditional Internet and IoT implies a new question; how it can influent the cyber security? The cyberthreat in IoT has been enhanced by possible impact to the physical world as well [2].

For better imagination in Figure 1 is shown TCP/IP model of conventional (traditional) internet in comparison with IoT model as is described in [3]. Regarding to further study, there is also necessary to mention that an object in IoT is a kind of parallelism to a host in traditional internet. However, there is significant difference in their amounts. Cisco in its white papers [5] published that in the year 2020, there will be 6.58 connected device per person on the Earth. Assumed the world population in the year 2020 is estimated on 7.6 billion. Because of the IoT represents wide spectral heterogeneous environment, traditional internet-working concepts are not agile enough to reflect this aspect, or even totally fails. Such environment can be challenge especially for rooting, however we will examine the security aspect.

As we can see from the Figure 1, the IoT model has Perception layer as the lowest level. The feature of this layer is to cover all objects, which are communicating together. However, this shielding is not only related with networking on physical level as we have known from TCP/IP model for traditional internet, but it also covers numerous of computational functionalities among the objects in order to ensure their low-level consistency and sustainability. For instance, smart actuators are supposed to be used in Industry 4.0. The smart actuator is equipped by one or multiple sensors to be able to control defined process autonomously. As concrete example can be process air controlling by a flap, where respective sensors are monitoring air velocity, humidity and temperature. Smart flap has implemented is own logic (usually Fuzzy logic

is suitable) to evaluate the opening angle autonomously. Upper system (PLC, IPC, etc.) is not informed about each monitored value, however only opening angle of the flap is forwarded, because the smart actuator itself calculates proper parameters for ensuring respective quantity and quality of the process air. There must be also data downstream defined, when the superior process demands new values for the air. Superior system sends new values to the smart actuator and it will compute a new opening angle based on actual parameters. The example is simplified for better understanding of data aggregation process, because for such unified data we usually do not need formal protocol, but only signalling. We can easily imagine the functionalities of this layer as an inner complex computational system in the IoT model. As we are moving to the higher level as more similar is data to the traditional internet.

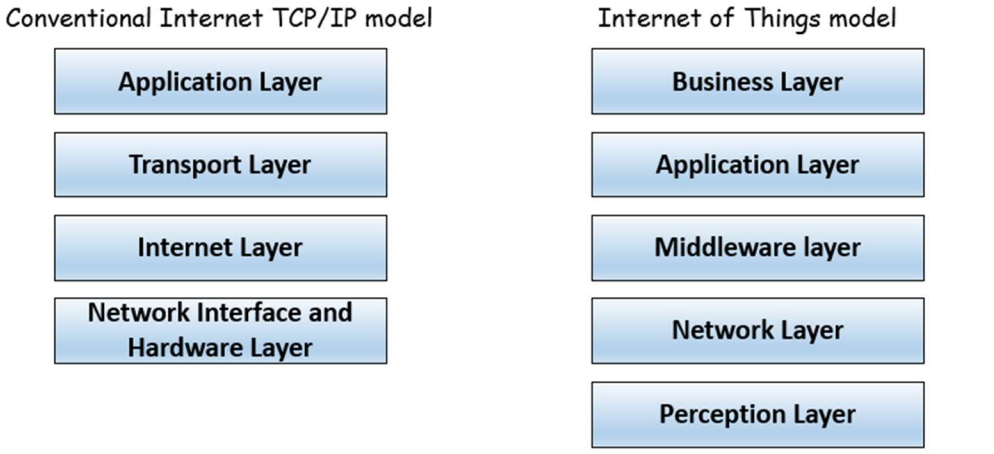


Fig. 1 Traditional data network model vs. IoT data network model
Source: authors.

The IoT has very convenient nature for numerous of military applications too. The main benefits for military applications can be concluded as follows:

1. Heterogeneous capability of the Perception layer. It is a great feature when different type of data from different echelons are collecting through different bandwidth.
2. Clustering and zonation capability. Fog versus Cloud concept allows us to deeply but simply customize design regarding the scope of operation.
3. Global networking. It brings us unlimited scenario organization and localization in order to keep the most valuable assets fully protected.
4. Advancing the artificial intelligence significantly mitigate the human presence by replacing it with robotic systems.

Above-mentioned benefits are rapidly stimulate the IoT using in spread spectrum of military operations. The most success has been recently recognized in anti-terroristic operations led by US Army. During these operations, unmanned surveillance and intelligent systems were used in advance to collect critical data. Consequently, robotic systems were loaded by the aggregated data from surveillance and intelligent to be dispatched to ensure safe and secure environment for live troops. Live troops were also equipped by sensorial network to be seen their health status and position in real time for robotic systems in order to react properly. The key parameters from the live scenario were aggregated and sent via global network to Pentagon, where key personal could make the highest decision (i.e. cease, reinforce, or change the operation). This example gives us a clear evidence of dynamicity, variety and customizability of the IoT concept.

However, on the other hand all these benefits brings opportunities for potential cyber-attack. Therefore, only way how to mitigate a cyber-attack is to conceal the details about the operation at least it is not accomplished.

3 SPLIT HORIZON DEFINING BETWEEN FOG AND CLOUD COMPUTING

We can assess from previous description that computational complexity can grow with power. We can use following notation:

$$CC_O = TI_c * PL_C. \quad (1)$$

CC_O – IoT Computational Complexity

TI_c – Traditional Internet Complexity

PL_C – Perception Layer Complexity

For better imagination, we will use a simplified avionic scenario. The Boeing 787 can produce more than 0.5 TB IoT related data during a fly [4]. If we realize that this is only traffic

switching between the plain and ground station, it does not seem to be so much, however we have to consider also regular traffic generates by traditional network (audio video communication, Internet and intranet). Hence, we can clearly see that the processing data traffic from the sensors is an extra load significant only for IoT concept. Moreover, there is other problem appearing, heterogeneous nature of the traffic. While traditional internet has mostly settled and unified communication procedures (each layer has specified set of protocols to handle with data frame), the diversity of IoT is much extended due to sensors and processes. Certain data can be demanded on real-time base, certain data has to have specified priority or ordering and topology is typically Ad-Hoc creating (in case of the airbus it is infrastructure topology due to fixed sensorial system). From equation (1) is clearly predictable problem with traffic congestions. Hence, splitting is demanded in order to compute local data as soon as possible before their sending forward. Optimal solution for heterogeneous data is pre-computing and formatting the data within a fog cluster. We call this as low- level computing and its result is reduced data fully compatible with conventional Internet. One of the most important feature is to aggregate only respective data to the upstream. For better illustration, we can figure out the above-mentioned example, the plane is in cruising mode. In spite of the mode, all sensors send the data periodically, due to real-time based communication model. Also the sensors respective to landing procedure are supporting the data, in spite of we are not in landing mode so we do not need this data for computing at the moment. This is the main reason to propose such model, which could be able to handle with low-level profile data. Cisco has introduced this layer in White paper [5] and called it 'Fog Computing' (resp. Edge Computing). In spite of its primary intent to use it for IoT, White paper specifies this structure generally and can be apply in other numerous applications.

Mentioned example was only trivial, however CISCO says that in the year 2020 there will be about 50 billion interconnected IoT devices [5]. Here is summarization of issues, which can be solved by Fog Computing:

1. Pre-compute the raw data from sensors in order to eliminate its volume before sending to the upper lever.
2. Allow to hand over the semi-results among the smart sensors in order to solve pre-mapped problems at object level.
3. Time latency significant decreasing, due to immediate and decentralized computing what is feasible especially for real time based applications.
4. Store the data for shorter time and send selected analytical and control data to the cloud for long term storing.
5. Possible segmentation into zones within extraordinary diverse heterogeneous environment.

To figure out what is IoT, we can find many similarities in the nature. The best example can be a tree as a biological system. The main parts of the tree are leaves connected to branches connected trunk and the trunk finally connected to roots. Every part is feasible and the tree cannot leave without it. We see that all vital substance is delivered from roots to leaves and backwards via only one trunk. Let's imagine that leaves are smart objects of our natural IoT concept. They really are, because the unique photosynthesis process is proceeding in every green leave. In every leave, there is a complex bio-factory, which transform carbon dioxide, carbohydrates and minerals into complex organic materials based on glucose and oxygen as a side product of this fabrication. Each leave can do it autonomously due to procedure encoded in DNA (Deoxyribonucleic Acid). After that, the trunk is used only for supplying the leaves with water and organic resp. mineral materials. We can only hardly imagine a model, where the root controls completely photosynthetic process. Every molecule and information had to be delivered from the leaves to the root and consequently back. Even we have enough robust trunk to be able to do that; it will not work, because of real-time factor is omitting. It is the sun light, which must act on the leaves in real time in order to launch photosynthesis process. Here we can see that nature, based on billions of years' evolution, has incredibly worked out methods and we should motivate by them.

To be motivated with this natural example, we would apply the same pattern in IoT. In spite of many original concepts copying TCP/IP pattern of traditional Internet (connect, route and deliver all data to application layer in order to be computed there) we found some reputable sources [5] confirm the theory. For better imagination, we can see data volume balancing proposal shown in Figure 2.

The figure shows data volume in pyramid perspective. In traditional Internet, there is always the same pattern starting by generating useful data load also known as a payload. When the payload data achieve Network interface and hardware layer, multi-layer encapsulation process is launched. It means that each layer attaches to the input data packet is extra information and hence the data volume is still greater as the data is passing across the layers from the bottom to the top and of course vice-versa.

In spite of the traditional internet, the Internet of Things has different shape of the data volume during passing through the layers. At the bottom, there are objects, which collect high volume of process data from the sensors. If we used concept of traditional internet and hence forward all data across all layers,

it would cause a data congestion very soon. Such congestion can be fatal in some response-critical applications (i.e. traffic control, nuclear cycle control, etc.). The other aspect of the data-reducing necessity is that some objects generating data do not need in time. For example, above mentioned plane in cruising mode the data deals with pressure in tyres, water level in water tank, even Doppler distance measuring system, etc. are not relevant, because of it has no effect to cruising mode. Hence, we need to distinguish between process relevant and process non-relevant data [1]. This analysis implied into defining a split horizon between Fog computing and Cloud computing as is shown in the Figure 2.

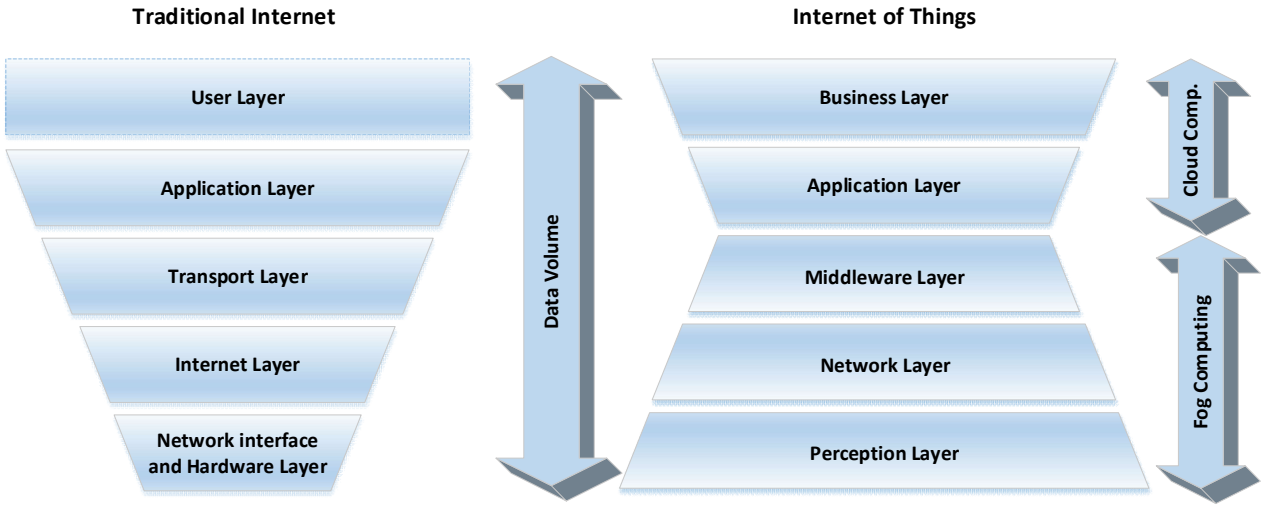


Fig. 2 Data volume balancing
Source: authors.

In many of sources the Fog computing is compared with Edge computing [i.e. 5] what means, that split horizon between fogs and clouds is between Perception and Network layer what practically means that computing can be executed only within sensors themselves but without data aggregation. However, such split horizon definition does not have any sense for data eliminating functionality because is dispersed only horizontally not vertically. Practically, it allows to compute and process data only to a constrained and homogenous cluster of objects (resp. sensors) bordered by network access point. We suppose in our Fog definition broader functionality. For illustration, we can see some general heterogeneous structure in Figure 3. In the figure, there are different IoTs networked clusters organized into individual fog structures. Important in designing the fog structures, is ability to collaborate within the fogs in horizontal as well as in vertical level. The reason is to process as much as possible and as deep as possible to aggregate the data before it leaves the fog clusters. Therefore, the data should be complementary across the fog in spite of its possible heterogeneous attitude. If we consider one of the fog cluster from the figure, Traffic Fog, we can identify following low level data sources (primary data generated by smart sensors):

1. Data generated by smart sensors of traffic control and infrastructure.
2. Data generated by autonomous vehicles.
3. Data generated by trains and power trains.
4. Data generated by avionic vehicles.
5. Data generated by sea vehicles.

We can assume following facts:

1. Each segment needs a specific type of network with specific conditions.
2. All segments are tied off with certain infrastructure, therefore they all need to interact with infrastructure.
3. To ensure that infrastructure is compatible across all devices, we have to suppose heterogeneous models only.

Up on these facts, we can suppose that fog structure would be responsible for computing the data up to middleware layer (as is shown in Figure 2), and the model for computing with the data should be bordered by segments within the fog. We can also consider fact that we are dealing with heterogeneous networking systems even among the objects. Moreover, these network systems are heterogeneous from many aspects (synchronization, prioritization, physical topology, logical topology, human interaction, etc.).

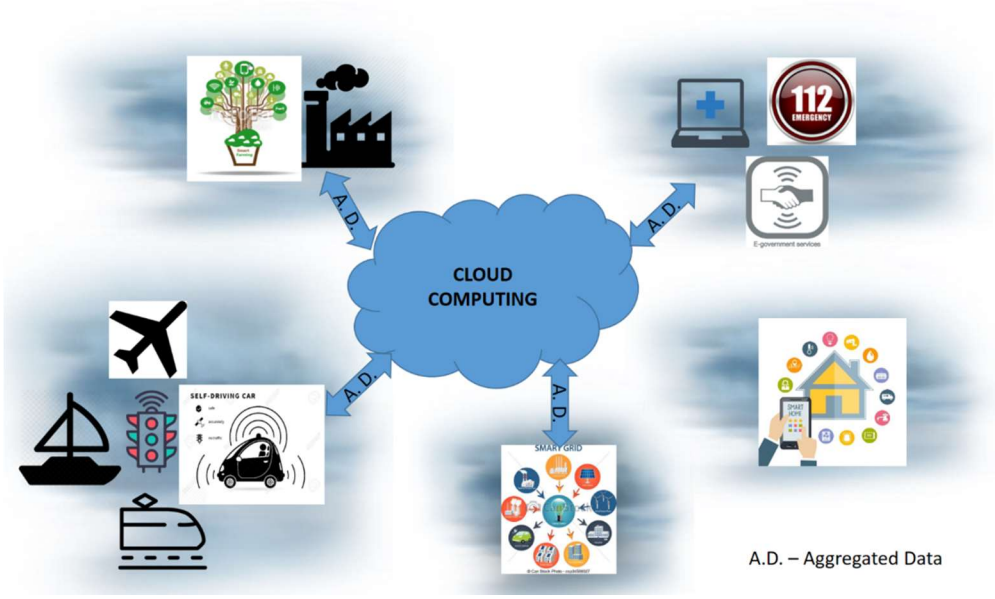


Fig. 3 Fog computing vs Cloud computing design proposal
Source: authors.

As an example, we can imagine following simplified situation; Train is approaching to a railway crossing point with a road. Traffic control sensorial network recognizes this and initiate respective measures to block vehicles from the crossing point by closing the ramps. Till this happened, a lot of computing would be calculated in the system (actual train speed vs distance, cross point clearance checking, control signals for actuators, etc.). If we suppose that there are also autonomous vehicles on the road, traffic control must notify them about the restriction and relevant time out. Hence, autonomous vehicle control system inside a vehicle can calculate new optimized routes, acknowledge autonomous vehicles segment about this new calculation in order to avoid traffic congestion caused by identical multiply optimizing by more vehicles. This scenario does not need to forward any data beyond the fog cluster, however it can forward certain aggregated knowledge. This information can be useful also for other IoT appliances like Smart Home (pre-heating reconfiguration according to actual delay, etc.).

On the other hand, some accident can occur at the same scenario. Here will be the highest priority to forward an urgent message over the cloud to national infrastructure cluster in order to minimalize the emergency assets response time. In this case the cloud structure will be used only as a medium for transfer the message. But common cloud purpose is to collect upper level data, which are data describes the clusters, sometimes segment overall parameters (i.e. load, reliability, average response time, number of incidents, level of impact, etc.). The data is used as a source for analysis, modelling predictions, forecasting, simulation, etc. Hence, we can say that cloud should handle with prioritization. Because of a cloud represents a top data model, should be responsible also for archiving. Based on the purpose of the cloud structure, its operational range covers mostly application layer and business layer of the IoT model.

4 SCOPE OF ATTACKS APPLIED IN THE IoT

The other aspect which desirable influents security issues in IoT is human interaction level (HIL). HIL has been already categorized in the first paragraph of this paper as H2H, H2M an M2M [2]. In these three levels of interaction is encoded transformation of whole internet and following technologies. If we are supposing IoT as technology of the future, we will consider only M2M interaction (only rare interaction of humans to the processes is supposed) as relevant for our further assumptions. The third category of interaction represents a scenario, where IoT connected objects have implemented some kind of autonomous logic (usually artificial intelligence) to control not only themselves, but also interactions among them. Human intervention missing dramatically influent scope of cyber threats. It is caused by eliminating unpredictable human factor, because the machine's control is based on finite-state algorithms, therefore under certain circumstances, anomalies can be detected much easier and more over some kind of cyber-attacks cannot be applied even [2].

From [1] we can use prescription rule for evaluating differences of types of attacks denoted by impact matrix A. Impact matrix A is a rectangular 3rd dimension matrix concluded different objectives into

vertical line (property, hardware, society) as well as different impacts among objectives in horizontal line (property – information, monetary, credentials, …).

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \quad (1)$$

Members of the matrix have the following meaning:

a_{11} - Direct loss of information.
a_{12} - Direct loss of money.
a_{13} - Stealing credentials for further exploitation.
a_{21} - Harming end devices (computers, smart phones, medical devices, nuclear centrifuges, …).
a_{22} - Harming front devices (servers, edge firewalls, …).
a_{23} - Harming infrastructure (all between 2 and 3).
a_{31} - People or groups compromising (like politicians, parties with certain interests, …).
a_{32} - Operational and working outages.
a_{33} - Foot-printing clearance.

Finally, the most important of this part is transforming the knowledge about attack impacts within cyber space to members of the matrix. Each member of the matrix can be evaluated from 0 to 5 due to its level of impact in an attack. Zero means no impact (victim is not influenced by the particular threat), five means the highest impact (no other threats could have higher impact on the victim).

Based on our general cyber-threat analysis [1] and wireless specific cyber threat analysis [6] we retrieved which attacks can be applied in the IoT environment as we summarize in updated Table 1.

Table 1 Updated summary of the Cyber threads in cyber physical environment [1,6]

Attack typology	Applicability on IoT	M2M apply	Impact matrix	Symb.
SQLi attacks	Principle of SQLi attack is based on human interaction on web, where there is trapping a dummy link and behind it is malicious code. Therefore, this kind of attack is not possible apply in IoT.	N	$\begin{bmatrix} 4 & 2 & 4 \\ 3 & 0 & 0 \\ 1 & 2 & 5 \end{bmatrix}$	A
Defacement	The purpose of this attack is to change data on a web page against subscribers. In M2M communication it has no sense.	N	$\begin{bmatrix} 1 & 2 & 0 \\ 3 & 0 & 0 \\ 5 & 1 & 0 \end{bmatrix}$	B
Account Hijacking	Nowadays, this kind of attack has no substance for applying within machines, but if machines has accounts with valuable credentials, it can be considered.	Y	$\begin{bmatrix} 2 & 4 & 5 \\ 1 & 3 & 0 \\ 4 & 1 & 4 \end{bmatrix}$	C
Targeted attack	This is a group of attacks represent many methods of penetration into certain object, therefore it is fully qualified attack in IoT environment.	Y	$\begin{bmatrix} 4 & 4 & 3 \\ 4 & 0 & 0 \\ 2 & 1 & 4 \end{bmatrix}$	D
Malware	The main property of the malware is its intentional implementing by a user. If we suppose only indirect human to machine communication, we can conclude this attack as impossible.	N	$\begin{bmatrix} 4 & 1 & 4 \\ 5 & 4 & 0 \\ 1 & 0 & 4 \end{bmatrix}$	E
Property hijacking	It is usually based on sophisticated social engineering exploitation due to it is very improbable in M2M communication environment.	N	$\begin{bmatrix} 4 & 2 & 5 \\ 0 & 1 & 3 \\ 2 & 1 & 4 \end{bmatrix}$	F
Software vulnerability	M2M communication is fully rely on built in algorithms, hence this kind of attack is supposed.	Y	$\begin{bmatrix} 5 & 2 & 2 \\ 1 & 1 & 1 \\ 4 & 1 & 5 \end{bmatrix}$	G
Cross Site Scripting	Implementing of this technique is also fully depended on H2M interaction. Hence, it is not applicable in M2M communication.	N	$\begin{bmatrix} 4 & 3 & 5 \\ 2 & 3 & 3 \\ 4 & 1 & 5 \end{bmatrix}$	H
Unauthorized access	Is usually related to personal credentials and social engineering attacks. We do not suppose this attack as a threat to M2M communication.	N	$\begin{bmatrix} 2 & 2 & 4 \\ 1 & 1 & 1 \\ 3 & 1 & 0 \end{bmatrix}$	I
Watering hole	Is typical presentation of Web of Human attack with massive social engineering contribution. No technical opportunities can be offered by M2M communication even in future.	N	$\begin{bmatrix} 2 & 2 & 0 \\ 1 & 1 & 0 \\ 3 & 0 & 5 \end{bmatrix}$	J
Botnet	Botnet is a kind of autonomous or semi-autonomous malicious code, therefore it can be implemented as a bug in M2M communication with efficiently using all its advantages.	Y	$\begin{bmatrix} 3 & 3 & 4 \\ 2 & 2 & 0 \\ 3 & 1 & 3 \end{bmatrix}$	K
DNS cache poisoning	DNS attack is related with traditional internet. In IoT is no possible implementation.	N	$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 5 & 4 \\ 0 & 3 & 2 \end{bmatrix}$	L

Brute force attack	This attack is usually executed aside on acquired sequenced of data and should be fully applicable in M2M environment. However, it is depended on possibility of a user to reach M2M communication.	Y	$\begin{bmatrix} 2 & 1 & 2 \\ 4 & 4 & 1 \\ 0 & 2 & 1 \end{bmatrix}$	M
KVM attack	From nature of this attack, we will need to communicate with M2M via input/output devices what can be applied.	Y	$\begin{bmatrix} 4 & 5 & 5 \\ 5 & 3 & 2 \\ 3 & 0 & 5 \end{bmatrix}$	N
Directory traversal	This kind of attack is based on narrow interaction user and machine so in M2M is no applicable.	N	$\begin{bmatrix} 4 & 1 & 4 \\ 2 & 4 & 0 \\ 2 & 2 & 4 \end{bmatrix}$	O
Man in the Middle (MiM)	The attack is supposed especially when data comes from fog to cloud. Literally said, MiM can be practically installed on the edge of a fog.	Y	$\begin{bmatrix} 3 & 5 & 3 \\ 1 & 3 & 3 \\ 4 & 0 & 5 \end{bmatrix}$	P
BGP traffic redirection	If a fog uses BGP protocol, the attack can be fully qualified, however zeta-byte structures will require a brand new routing protocols suitable for heterogeneous networks.	Y	$\begin{bmatrix} 4 & 0 & 1 \\ 0 & 0 & 5 \\ 0 & 5 & 5 \end{bmatrix}$	R
NTP reflection	Time synchronization is feasible for communication within M2M, hence if even another protocol for central synchronization is used, it will be very probable attempting of its manipulation.	Y	$\begin{bmatrix} 4 & 0 & 0 \\ 0 & 0 & 3 \\ 1 & 2 & 4 \end{bmatrix}$	S
Data interception	In consideration of objects high mobility, they will be critically depended on mobile communication. Therefore, this kind of attack is substantially important.	Y	$\begin{bmatrix} 5 & 4 & 4 \\ 1 & 1 & 1 \\ 3 & 2 & 4 \end{bmatrix}$	T
DoS wireless	In spite of mean less typical DDoS attack aimed on data structure, this type of attack is targeting to transporting medium itself. There is only limited protection possible against it.	Y	$\begin{bmatrix} 2 & 1 & 0 \\ 3 & 3 & 5 \\ 2 & 5 & 3 \end{bmatrix}$	U
Rouge device	Rouge device is added by an unconscious user and create a security hole for an attacker.	Y	$\begin{bmatrix} 2 & 3 & 4 \\ 4 & 4 & 1 \\ 2 & 0 & 5 \end{bmatrix}$	V
Evil twin device	An attacker adds this kind of device intentionally. Some IoT systems cannot be physically protected, hence this attack is very likely.	Y	$\begin{bmatrix} 2 & 2 & 5 \\ 2 & 2 & 1 \\ 3 & 1 & 4 \end{bmatrix}$	W

5 ATTACK VECTOR

As we have already remarked, the IoT can be applied in a spread spectrum of environments as well as surrounded conditions. Just concrete situation can specify which possible threats should be considered. For instance, enclosed automation in a factory, where is spectacular physical protection provided can be hardly applied an evil twin attack, however rouge device attack is not mitigated by established physical security. On the other hand in traffic control systems where IoT devices are distributed in public area is impossible to provide physical protection within all premises. Therefore, there is evil twin attack very likely. This leads us to introduce Attack vector for individual situation. Each individual attack matrix [1, 9] is labelled by letter from A to W. Vector is then denoted as a sequence of individual attack matrixes each multiply by coefficient, which can be 0 or 1.

$A_V = \{c_1A, c_2B, c_3C, c_4D, c_5E, c_6F, c_7G, c_8H, c_9I, c_{10}J, c_{11}K, c_{12}L, c_{13}M, c_{14}N, c_{15}O, c_{16}P, c_{17}R, c_{18}S, c_{19}T, c_{20}U, c_{21}V, c_{22}W\}$, (1)

where c_x {0.1}.

For A, B and L matrixes there is default $c_x = 0$.

Hence, we get simplified vector denoted as IoT maximal attack vector:

$A_V = \{c_3C, c_4D, c_5E, c_6F, c_7G, c_8H, c_9I, c_{10}J, c_{11}K, c_{13}M, c_{14}N, c_{15}O, c_{16}P, c_{17}R, c_{18}S, c_{19}T, c_{20}U, c_{21}V, c_{22}W\}$. (2)

If we consider above-mentioned examples, attack vector for traffic control environment will be following:

A_v(traffic control) = {0A,0B,0C,1D,1E,0F,1G,0H,1I,1J,1K,0L,1M,1N,0O,1P,1R,1S,1T,0U,0V,1W} = {1D,1E,1G,1I,1J,1K,1M,1N,1P,1R,1S,1T,1W}.

After reverse substitution the acronyms by original matrixes, we can see complex notation as follows:

Table 2 Example of attack vector

Targeted attack	Malware	Software vulnerability	Unauthorised access	Watering hole	Botnet
$\begin{bmatrix}4&4&3\\4&0&0\\2&1&4\end{bmatrix}$	$\begin{bmatrix}4&1&4\\5&4&0\\1&0&4\end{bmatrix}$	$\begin{bmatrix}5&2&2\\1&1&1\\4&1&5\end{bmatrix}$	$\begin{bmatrix}2&2&4\\1&1&1\\3&1&0\end{bmatrix}$	$\begin{bmatrix}2&2&0\\1&1&0\\3&0&5\end{bmatrix}$	$\begin{bmatrix}3&3&4\\2&2&0\\3&1&3\end{bmatrix}$

B-F attack	KVM attack	Man in the middle	BGP traffic redirect.	NTP reflection	Data Interce-ption	Evil twin device
$\begin{bmatrix}2&1&2\\4&4&1\\0&2&1\end{bmatrix}$	$\begin{bmatrix}4&5&5\\5&3&2\\3&0&5\end{bmatrix}$	$\begin{bmatrix}3&5&3\\1&3&3\\4&0&5\end{bmatrix}$	$\begin{bmatrix}4&0&1\\0&0&5\\0&5&5\end{bmatrix}$	$\begin{bmatrix}4&0&0\\0&0&3\\1&2&4\end{bmatrix}$	$\begin{bmatrix}5&4&4\\1&1&1\\3&2&4\end{bmatrix}$	$\begin{bmatrix}2&2&5\\2&2&1\\3&1&4\end{bmatrix}$

The vector can tell us something about security but only from static point of view. It means that it can be useful information for a certain phase of the product life. In addition, it does not reflect upper-level aspects of the environment, especially social factors (trust, national economy, dynamic security influence, etc). Therefore, we can use the vector as only initialization vector and we have to combine it with other metric reflecting dynamicity and complexity of the environment, where the subject is applied.

To reflect the above-mentioned changes, we implement superior coincident set of rules to reflect security measures of whole product-life (in product life we suppose design, installation and life cycle of a product). The coincident set of rules can be implemented by a matrix denoted as following:

Table 3 Coincident product-life security matrix

Mode/Attack vector	A	B	C	…	V	W
In Design mode	0	1	1		0	1
In Installation mode	0	0	1		1	1
In Process mode	0	0	0		0	0
In Service mode	0	0	1		1	1

Based on our general experience with automation, there are following modes with different vulnerability spectrum:

1. Design mode. It is a specific mode during developing and design cycle of the product. In this phase, it is required to establish resources for further security implementation. Therefore, it is critical to exactly figure out how the system will be working as well as interacting with surrounding environment. Undersized resources in this phase usually leads to serious troubles in Process mode.
2. Installation mode. During installation, there are some unique and specific issues, which require temporary implementation of some security measures. It is mainly caused by wider social environment threat (many different companies are involved to the installation process) as well as missing overall integrity (subsystems are insulated from early installation phase). This gives a unique opportunity to implement such kinds of attacks required physical reachability of the system. Its high importance is emphasised by our very last experience from China, where during building up a turnkey pharmaceutical factory in Nantog one of the contributed subcontractors (PM group) did no respect BOSCH fully qualified design. In spite of correct designing all critical processes respective to Good Manufacturing Processes as well as Good Engineering Processes, PM group (a third party incorporated to the project) suggested to the end customer to change Ethernet communication to WI-FI. They suppose only benefits (less caballing, possible moving the devices, etc.), however no cyber-security protection rules has been applying [6]. Moreover, they connected the WI-FI to the global Internet with explanation that production can be controlled in more convenient way from home-office. Of course, the end customer was very happy with this solution, however he is not aware of tremendous risk of such solution. Applied security suit in wireless communication is very primitive respective to shallow knowledge of the contributed companies as well as non-respecting experts' recommendations. There is not only an enterprise solution missing (each session-user has different password within the domain) [6], but also the common password was chosen to be remembered easily with explanation it can be changed later on. This is a paramount example how tricky non-qualified personal can be, especially in China. We have also positive experience from our installation in the USA, where cyber-security was keeping at the first place [6].

The poor security in installation phase can allow to easily penetrate to the resources of the network and theirs exploitation can be effectively used in the next phase of the live cycle. In the process mode, a possible hacker would have an

exact knowledge about network topology, IP address plan, processes, sensors, actuators, recipes, etc. After he successfully guess the password (it is possible by using cloud computing [6]) can easily change concrete parameters in prescribed recipes what could lead to different drugs production with possible lethal impact to human beings.

3. Process mode security is closely related with Installation mode security. Once data integrity is guaranteed and only process – respective personal is allowed to enter the area, some security threats from previous phase are mitigated by enhanced and solid security measures.
4. Service mode is only temporary mode (between-production) for maintenance, but necessary mode in any product life-cycle. From cyber-security aspect, this mode could use very similar resources as installation mode. Therefore, there are also risks similar to installation phase. The risk can be partially mitigated by efficiently lesson-learned implementation.

As we can see the attack vector is changing over the product life cycle. While in Installation and Service mode can be implemented a malicious hardware as well as access to the resources by a malicious person, this risk is mitigated in Operating mode by its nature, where the resources are limited by respective authorization to the system.

6 CONCLUSION AND FURTHER CHALLENGES

To measure security in a heterogeneous cyber-physical space where IoT is applied is still a challenging problem. The complexity is boosted by its connection to physical platforms despite of traditional Internet where only pure cyber environment is becoming into consideration. The second identified complication is much wider non-cleric personal acting in IoT security. As our very last experience from China showing us, this could be the greatest challenge in IoT cyber protection for the future.

As a very fundamental point for security measures is to describe threats. For this purpose, we digested all previously researched and analyses into Attack vector (denoted as A_V). The A_V has only static function and cannot reflect dynamic influence of changing environment. Therefore, we are proposing the superior Coincident product-life security matrix to reflect the security vector throughout the product-life. There is still a big challenge to the future research to find out a suitable model, which can dynamically reflect different social status and environmental aspects of mostly heterogeneous networks. Some of the peer to peer communication concepts for traditional internet are described in [7] and could be useful as a source for our further research.

References

[1] OBERT, M., HARAKAĽ, M.: Contemporary Cybernetic Threats Analysis. In *Science & Military,* No 1, Volume 10, 2015. Liptovský Mikuláš : Armed Forces Academy of General Milan Rastislav Štefánik, 2015. ISSN 1336-8885.

[2] MISRA, S., MAHESWARAN, M., HASHMI, S.: *Security Challenges and Approaches in Internet of Things.* Springer Briefs in Electrical and Computer Engineering, 2017.

[3] ISTABRAQ, M. Al-Joboury, EMAD, H. Al-Hemiary: Internet of Things (IoT): Readme. In *Qalaai Zanist Journal*, Vol. 2, No. 1, April 2017.

[4] FLANNAGAN, M.: *Embracing Data & Analytics in the IoT with Our Partners.* 14. April 2015, CISCO.

[5] White Paper, Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are, CISCO, 2015.

[6] OBERT, M., HARAKAĽ, M.: *Low Level Profile Security Analysis in Wireless Environment.* Liptovský Mikuláš: Armed Forces Academy of General Milan Rastislav Štefánik, No 1, Vol. XX, 2017.

[7] KWONG, Y., KWOK, R.: *Peer to Peer Computing: Applications, Architecture, Protocols and Challenges,* CRC Press, 2011.

Eng. Martin OBERT (PhD. student)
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 06 Liptovský Mikuláš
Slovak Republic
E-mail: martin.obert2@gmail.com

Col. (ret.) Prof. Eng. Marcel HARAKAĽ, PhD.
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 06 Liptovský Mikuláš
Slovak Republic
E-mail: marcel.harakal@aos.sk

Eng. Martin Obert - was born in Trenčín, Slovakia in 1980. He received his Engineer degree in 2003 in Communication and Radio systems from the Military Academy in Liptovský Mikuláš. His research is aimed to security in wireless communication and its applications mainly in industry in the field of autonomous cybernetic systems.

Col. (ret.) Prof. Eng. Marcel Harakaľ, PhD. - He received the MSc. degree in electrical engineering from the Faculty of Electrical Engineering, Slovak Technical University in Bratislava in 1983. In 1997 he successfully finished his PhD. studies in artificial intelligence. From 1983 to 1989 he worked as a research engineer at the Military Research Institute in Liptovský Mikuláš. In 1989 he joined the Armed Forces and since then he has worked in various teaching and managerial positions at the Department of Informatics. In 2002 he habilitated as an Associate Professor in the Electronics and telecommunication field. In 2018 he became a Professor in Military Communication and Information systems. During his university career from 2004 to 2012 he led the Department of Informatics. Currently he is in the position of Vice Rector for Science of the Armed Forces Academy of General Milan Rastislav Štefánik, Liptovský Mikuláš, Slovakia.

His research interests include computer engineering, image processing, cyber security, and network operations.

2019 Communication and Information Technologies (KIT)
Hotel GRANIT - Vysoké Tatry / Tatranské Zruby
October 9, 2019 – October 11, 2019

Presentation of new sophisticated technologies and results of both theoretical as well as applied research in the area of communication and information technologies. The aims of the Conference are professional discussions and plenaries on communication and information technologies and their use in research, training and education, with focus on military applications.

Since 2017 the conference has been supported by the IEEE and the accepted papers will be published in the conference proceedings and submitted to IEEE Xplore. The papers from the last conference are indexed in Web of Science and Scopus as well.

Conference Contact:
Address: Armed Forces Academy of General M. R. Štefánik, Department of Informatics,
Demänová 393, 031 06 Liptovský Mikuláš, Slovak Republic
Phone: +421 960 423019
Fax: +421 44 5525639
E-mail: kit@aos.sk

CRITICAL INFRASTRUCTURE PROTECTION IN THE CONTEXT OF THE SECURITY NETWORKS

Daniel ROMAN

Abstract: Security is one of the reference elements of an entity, regardless of its nature and of how it is reported at the micro- or macro-dimensional level. Due to the complexity of the reference environment against which the state of security is defined in a contemporary context, this poses a major challenge to specialists in all areas: political, military, social, economic, information, infrastructure and environment. Therefore, identifying those viable solutions for preventing, counteracting or eliminating the effects of a crisis, depending on its nature, may only be possible by understanding the "operating mechanisms" of each area. Following the dynamics and describing the interaction relationships of the responsible social systems can be one of the methods of managing a potential complex crisis that may occur at a given time. In this article, we have intended to argumentatively support the need for an integrated approach to the security of the identified "pillar systems" by focusing on critical infrastructure protection and designing, planning and deploying military actions. For the first time, based on integrating the dynamics of the risks and the vulnerabilities of the social systems, we have argumentatively developed the concept of network interaction. By monitoring and analyzing the essential descriptive parameters of each security field, we can decipher their security states due to the identified network connections, and moreover, we can anticipate a potential crisis or the possible occurrence of a major negative event.

Keywords: security; critical infrastructures; military action; crisis; vulnerabilities; collaborative workflow; negative event.

1 THE COMPLEXITY OF THE INTEGRATED SECURITY ENVIRONMENT

The notion of security, in most definitions, essentially covers that state that expresses the existence or the performance of the activities of an entity in order to fulfill its established role or objectives without a direct or indirect influence factor of any kind being capable to affect or hinder it. Depending on the nature of the domain we make reference to, the state of security is described in detail and is reflected in the absence of danger. Understanding the terms that refer to the state of security is paramount in all attempts to express, define, or describe the position of an entity related on a micro- or macro-dimensional level. Knowing the parameters that describe the dynamics of the evolution of an entity, an analysis of the entity's state can be made, as well as a formulation of those solutions required for maintaining the systemic balance. The problem arises when, due to being ignorant of the transformations of the existence of the subject entity, extreme values of the descriptive parameters are generated or new connections appear influencing other entities in the same or in different domains. In this sense, we can consider that decoding the reality with respect to a certain entity is the starting point in constructing the influence connections between one or more entities based on certain types of functional networks created due to mutual influences.

Regarding the introduction of the concept of a "network of influences", the state of security of an entity exceeds the area of its own descriptive parameters and transits in another area of interaction with other identified or unidentifiable entities. Because of this, it is noticeable that new network connections are born and there are a number of role changes of the elements becoming network nodes. In other words, even if mathematically argued relationships between different entities are developed, the concept of integration into a particular network or into multiple networks shows that the nature of the relationships between the entities and the context of mutual influences is not a simple well designed puzzle or just one way of assembling it, but rather a very complex system in which the components fit in so many configurations, almost impossible to define [1]. By launching the hypothesis by which any socio-technical system is capable of developing its own personality and implicitly of adapting to its own environment, it results that at the level of the network it is possible to have functioning laws based on self-organization.

Through the intuitive application of the concept of network and the transposition of the components of a socio-technical system, such as a political, military, social, economic, informational or environmental one, a series of infrastructures with different roles and distinct geometry is constructed.

Due to the relationships established between the network elements of the socio-technical systems and due to their role in society, the infrastructures were classified according to their role in: ordinary infrastructure, special infrastructures and critical infrastructures [2]. From the point of view of network geometry, infrastructures are born and grow differently, depending on the degree of association and belonging to that network of all its constituent elements. Figure 1 shows that the newly connected elements (the white rings) join the network by establishing connections with the most connected network elements (the black rings). Depending on the role they perform, each network element modifies the geometry of the network according to the connections made, and extends it to the area of greatest interest or importance. Translating each element into its own network and according to the connections it has to other elements from other

networks involves making new connections between two or more networks. Thus, connections are made between two or more networks/domains of interest and there are a number of advantages and drawbacks which will be addressed later on.

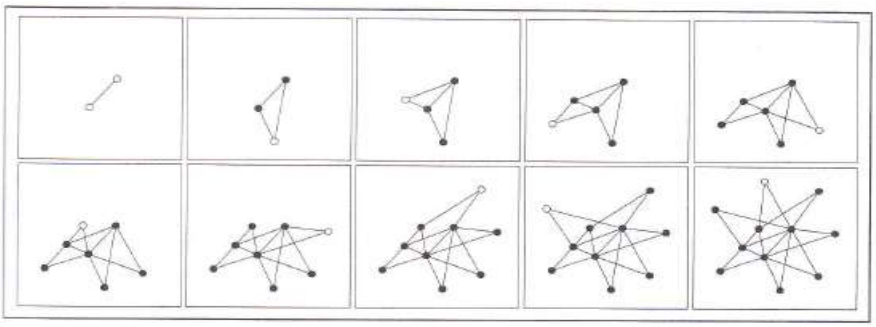


Fig. 1 Variants of design and self-organization of networks
Source: Albert Laszlo Barabasi.

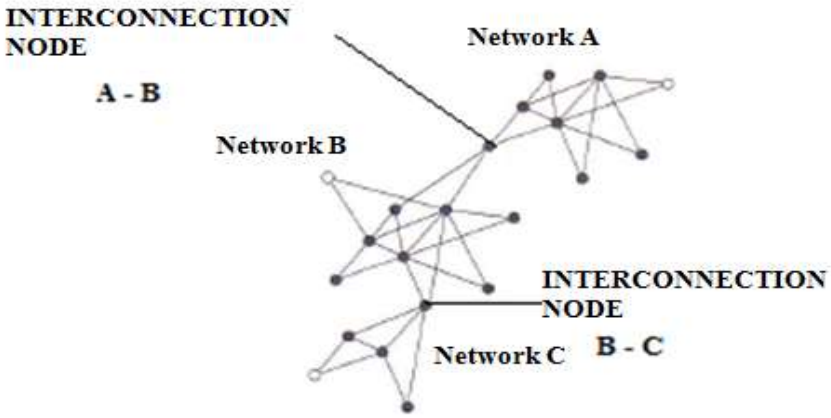


Fig. 2 Variants of connections between two or more networks/areas of interest
Source: Directive 114/2008, 345/77.

The more the network connection element is "more connected" to its own network, the stronger the connection between networks is. This way of explaining the connections between infrastructures or areas of interest can be helpful in understanding the "mechanism" of occurrence of a crisis or a major negative event at a given time. Identifying solutions to surmount a potential crisis or to help the entity concerned survive the major impact negative event involves "locating the entity in the network of influences." The network of influences is given by the nature of the connections between the entities that interact directly or indirectly. We will refer to two areas, namely the critical infrastructure protection and the area of military action. As defined in EU Directive 114/2008, a critical infrastructure is "an element, a system or a component thereof located within the territory of the Member States that is essential for the maintenance of vital societal functions, health, safety, security, social or economic well-being of persons and whose disruption or destruction would have a significant impact on a Member State as a result of the inability to maintain those functions". The military component is the essential factor of a nation or an alliance that guarantees security against the military action of a potential aggressor [3]. Due to the destructive power resulting from the military action (material damage and loss of life), it is necessary to reposition the critical infrastructure protection at the conceptual level. This implies achieving an integrated vision of the two areas of interest: the military and the critical infrastructures. This integrated approach, as previously formulated, relocates the security components and defines the multitude of connections between the network nodes and their importance, an aspect which will be highlighted in the case study on the cyber attacks in the capital of Estonia, Tallinn.

2 CRITICAL INFRASTRUCTURES IN MILITARY ACTIONS, EFFECTS AND CONSEQUENCES

The complex situation in the spring of 2007 in the capital of Estonia, Tallinn, can be considered as one of the major reference to which the security environment needs to be redefined. Although at that time the cyber attacks could not be considered hostile military action, their effects and especially their consequences have shown that the security environment can no longer be described as the property of only one security entity. The coincidence of the cyber attacks with the deterioration of the Russian-Estonian political-diplomatic relations amid ethnic-social dissatisfaction regarding the transfer of certain symbols of high significance to the Russian minority in the Estonian national territory is the starting point of a potential crisis of a certain extent. By this extent we mean the degree to which the problem of cyber attacks escalates.

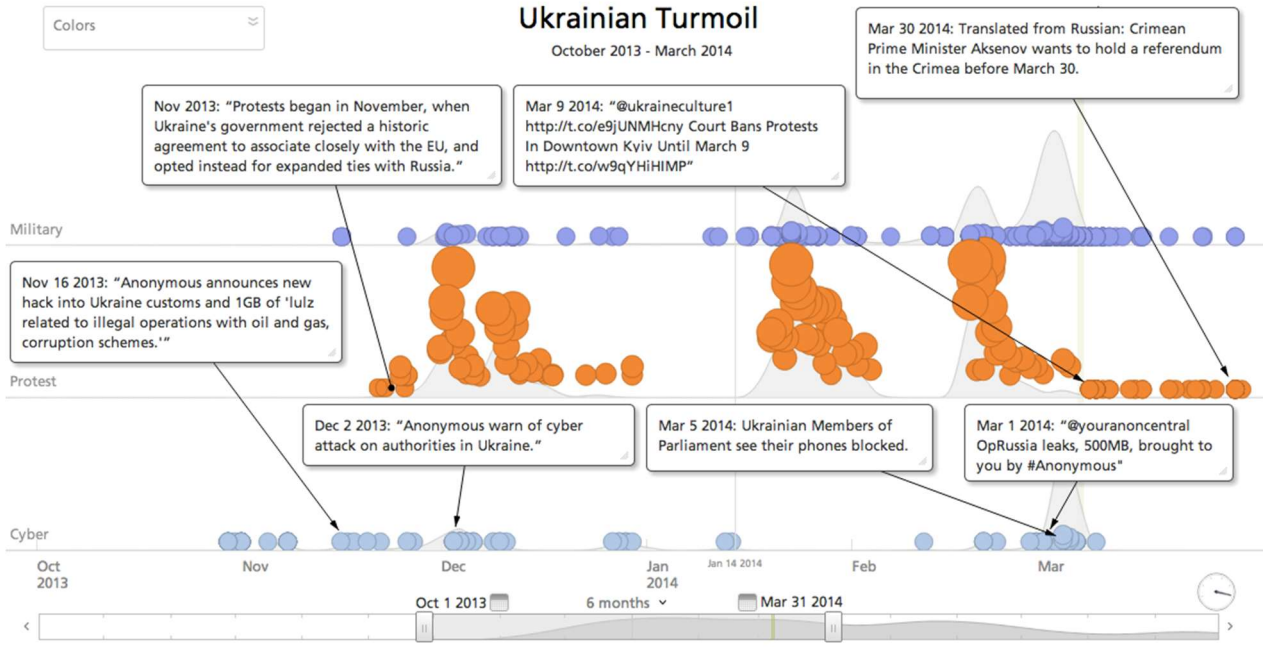


Fig. 3 Chronologic representation of complex incidents that precede a cyber attack
Source: [4].

Paralyzing the Estonian state institutions and causing important damage to critical infrastructure components due to cyber attacks in NATO's vision was "an operational security issue" handled as seriously as possible. In hypothetical terms, if the effects of the cyber attacks were to seriously affect the existence and the functionality of the attacked Estonian critical infrastructures, by the degree of their damage, namely material damage and/or loss of human lives, the state of necessity would have been for sure declared, the combat capacity would have gradually increased and the military structures would have engaged the aggressor. Without tackling technical details, the cyber attacks on the institutions in Tallinn in 2007, due to the lack of NATO and EU legal bases, could not have been regarded as clear military action. However, the involvement of the security factors: political, economic, military, social, information and infrastructure, clearly shows the nature of their relationships and their behavior in managing the incident through a certain shape and geometry specific to a security network or multiple networks.

The concept of network action of the security factors for managing an event with a negative impact on one or more states can be the key to anticipating the occurrence of attacks of a specific nature aimed at destabilizing the state of security. The combination of the two components: the critical infrastructure protection and the defense specific for the military field, in our view, must be intersected and positioned "operationally convergent". One of the strongest arguments is given by the number of victims and the volume of material damage that can be attributed to attacking a critical infrastructure and by the conduct of military operations or exercises that could get out of control. The explosion of an atomic-power plant due to its failure to operate under nominal technical parameters due to cyber attacks or terrorist actions may have consequences similar to military attacks such as the explosion of a nuclear rocket. Hence, defining hybrid war remains one of the most difficult

tasks assigned to military experts. In April 2016 another nuclear power plant from Germany was the target of ingenious cyber attacks that could have had catastrophic consequences. The computer viruses "W32.Ramnit" and "Conficker" were identified in the Gundremmingen B unit in Germany, aiming to corrupt the computer data of the equipment responsible for handling the nuclear fuel bundles [5]. The mode of action of a computer aggressor in this case is described as a remote action on a computer system when it is connected to the Internet. The consequences of such an attack, apart from major material damage and loss of human lives following a nuclear explosion occurring at the atomic power plant can be anticipated and described on the basis of the relationships established according to the model of a coherent network of security factors.

Under another determination report, a state's critical infrastructure may be damaged by the outburst of a military conflict. The supply of drinking water for the population or the supply of water needed for industrial or agricultural activities can be seriously affected by military operations, as was the case in the military conflict in Ukraine. Air transport, viewed as part of a designated critical infrastructure in a state, may be affected as a result of military conflicts. We mention the destruction of a civilian aircraft in Flight MH-17 of Malaysia Airline by the military missile type SA-11 in the aviation catastrophe in the Donetsk region on July 17, 2014 resulted in the death of 298 people [6]. A first observation is on the degree of involvement of the institutions responsible for the security, which determines a certain geometry of the network of influences. In other words, overlapping the effects of the actions or inactions of the security factors, regardless of how the network connections are made, assigns different values to network nodes depending on the context of the affected domain. The implications of the Russian Federation's military action near NATO borders concluded on November 24, 2015 with engaging a military aircraft Suhoi Su-24 in Turkey's airspace [7]. Although it did not result in huge material damage or significant loss of human lives, the consequences of such an incident had a major impact on the political and military security pillars, with direct and indirect influences on the economic and energy fields.

Another aspect, particularly important for the typology of the network of security factors influences is the military conflict in Syria. In this case, the situation becomes even more complex due to the number of actors involved in the conflict, as well as the particularly serious consequences on all areas: political, military, economic, social, information, infrastructure and environmental. Assigning a theater of military operations includes all aspects related to the infrastructure of the operation area. The critical infrastructures of the theater of military operations are one of the fundamental elements of conducting combat. The geographic region of a military conflict, defined at political level, may be delimited to execute or support military operations in one or more areas of joint operations. Due to the important geographic extent, the military operations (the situation in Syria) can take place in several combat environments, which can lead to successive and different threats both within and outside the conflict territory [8]. One of the major dangers of a military conflict like the one in Syria, beyond the possibility of the military conflict expanding beyond the geographical boundaries, is to create imbalances at the wider level of the conflict area. The phenomenon of the population migrating outside the military conflict area may affect the parameters of the designated critical infrastructures in the territory of the countries affected by migration, or may generate social incidents of an ethnic or religious nature, as well as imbalances at State or Union level in some states. In other words, a military conflict can directly or indirectly generate effects of an economic, social, political or other nature, both on the territory of the state undergoing a conflict and on the territory of other states, irrespective of the distance to the epicenter of the war. The consequences, based on causes and effects, in a specific area of military operations, depending on their nature and subject matter, may be extended. Following the integration of the concept of network of influences on the designated critical infrastructures such as terrorist attacks inside states not involved in military conflicts but politically supporting these conflicts is one of the key arguments for an integrated approach to critical infrastructure protection concerning the conduct or the support of military action.

3 NEW HORIZONS ON THE CRITICAL INFRASTRUCTURE PROTECTION IN MILITARY ACTION

The reality of contemporary society, characterized by a profound complexity of problems in all security areas, combined with access to state-of-the-art technologies, is one of the challenges defense specialists have to face. Cyber attacks have become increasingly sophisticated in terms of technology, which calls for resorting to specific measures but also for establishing specialized rapid reaction structures for the emergency situations in the cyberspace. For preventive purposes, NATO and EU institutions have moved on to adopt those technical measures and to create those specialized structures capable of building and maintaining the state of security and intervention in the event of a crisis or occurrence of an event having a major negative impact.

In this respect, specific to critical infrastructure protection, according to EU Directive 114/2008, a security mechanism has been set up, which, through the operator security liaison officer, implements the critical infrastructure operator's security plan [9]. Following the above mentioned examples, we can admit that a certain degree of amplification of

vulnerabilities of the designated critical infrastructures is directly proportional to the level of connection of the subject within the network of influences. We have overlooked the fact that the vulnerabilities of an atomic power plant or a military operator exponentially increase with the level of their or their systems' connectivity in cyberspace. In other words, the network of influences is not just a conceptual network; it can be physically not just conceptually identified at a given moment in cyberspace. Another aspect is the operational technical knowledge of the "security pillar" domains that cannot be limited to just a certain segment of infrastructures. The level of connectivity can generate cascading effects, and a seemingly insignificant cyber attack on a particular structure can lead to major catastrophic effects for the other connected or unconnected infrastructures.

One of the current security trends regarding those infrastructures considered critical is the technical isolation of the main responsible systems in the cyber space for commanding and controlling vital systems of the critical infrastructures and eliminating all external connection possibilities. The installation of antivirus software and the physical protection against unauthorized access to electronic systems is still one of the most common security measures. The scenarios of the security incidents demonstrate that a number of innovative cyber attacks and a certain technological complexity can still be generated. Therefore, the competent security forces have initiated specific legislative procedures on working in the cyberspace. In order to cope with the increased evolution of cyberspace threats, the US has adopted the concept of Active Cyber Defense (ACD) in cyber defense strategy. Active cyber defense has already become a very controversial topic. The controversial aspect is given by the Responsive Cyber Defense (RCD), defined as "cybernetic infrastructure protection against an ongoing cyber attack through measures directed against the cybernetic infrastructure from which the attack originated or against an infrastructure as a third party thereof" [10]. Apparently similar, the two concepts are totally different in terms of area and specific mode of action. RCD addresses a cyber attack in progress and does not involve preemptive or retaliatory actions. While defining a policy in the narrow sense of the RCD, this implies the application of offensive, punctual cyber-measures in clearly defined situations [11].

Regarding "the position" of defending against or countering the threat such as a cyber attack or a terrorist attack, at least two strategies can be distinguished: the reactive and the proactive strategies. In line with the position of the subject in question(reactive or proactive) in a possible network of influences, he will manifest different behavior to the external factors (of aggression). Depending on the ability of the subject to adapt to the environment, it is assumed that he will be able to cope with any unforeseen hazard. Due to the implementation of the concept of network and the assimilation of the states of security specific to critical infrastructures in military operations, we notice the existence of more than just one security level. The systemic approach, to which we have referred, connects the elements of several distinct domains. The degree of connectivity of the elements and the nature of the connections between them form the direction of threat manifestation

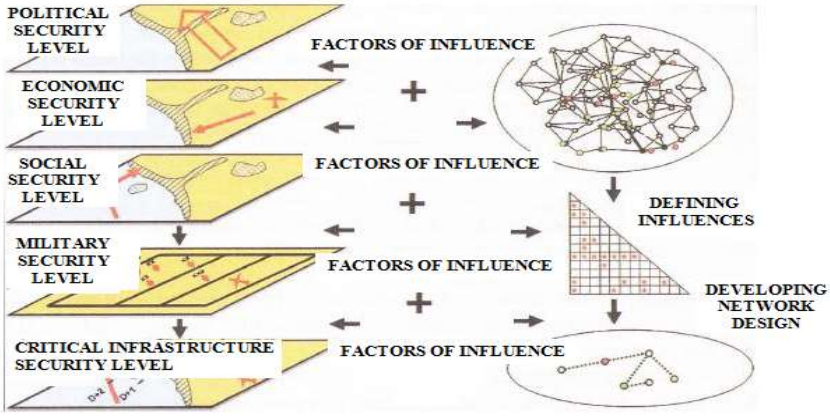


Fig. 4 Representation of the security levels and the network geometry according to influences
Source: [4].

The conceptual creation of networks based on the influences between the nodes connected to a particular connection scheme may outline a particular state of crisis and, implicitly, the possibility of a proactive attitude of counteracting the crisis, regardless of its nature. From an international perspective, two or more states interconnected at one or more "security pillars" can be affected by the same crisis differently, depending on the "geometry of the network of mutual influences." The same can be said

in the case of a negative event with a major impact on the critical infrastructure on the territory of a state having direct or indirect causes, as a result of incidents occurred on the territory of the neighboring state or of another state. The military conflict in Syria has produced or is about to cause serious damage to critical infrastructures across the territory of other states in multiple ways: from social, economic, infrastructure, cultural, etc. point of view, both in the short term and especially in the medium and long term, with particularly difficult, unavoidable consequences.

4 INSTEAD OF CONCLUSION

Decoding the reality of how a crisis develops or how a negative event with a major impact on a state or several states occurs is the fundamental aim of researches into the concept of a "network of security pillars". Understanding thoroughly how the security systems or the critical infrastructures on the territory of a state or states work helps us identify their vulnerabilities. The vulnerabilities of each system in the concept of a "network of influences," as we have argued in the contents of this article, can be interpreted as a "crack in an amorphous body" where the body can be that "system of systems." Therefore, the vulnerabilities of a subsystem may represent in different percentages depending on the situation or the degree of connection of this system with the other systems, different threats on the macro system that all the networked subsystems create.

Another observation resulting from the systemic interpretation of the network of influence focuses on the performance of the critical infrastructure managers and on their ability to conduct a collaborative workflow. The specific manner of working towards mitigating or removing the vulnerabilities of a security system cannot guarantee the security of the entire security macro-system, be it at the level of a single state or the level of several states. For this, we suggest a possible working solution for the responsibility factors, in the sense of mutual awareness or sharing the information resulting from overcoming dangerous situations they had been exposed to in the past. This may be possible extending the concept of a network of influences based on the collaborative workflow typology. In other words, we can anticipate and better defend against an aggressor threatening a state-entity if within the collaborative workflow the strengths or weaknesses and lessons learned from an earlier confrontation of the aggressor with the collaborative partner of the state-entity have been disseminated. This can be done by building those common databases that are available to the parties included in the collaborative workflow network, as previously mentioned.

The conduct of the mutual awareness activities as well as the systemic interaction of each security pillar on the territory of one or more states is the starting point for decoding the connections of the network of influences and implicitly the implementation of a proactive behavior of identifying and countering a crisis. In this respect, we support the idea of the specialists in all areas of security collaborating, focusing their efforts on understanding the causes of the vulnerabilities and identifying the similarities of their manifestations. Critical infrastructure protection in the context of the security networks is a way of preventing and counteracting a crisis or of preventing the occurrence of a major negative event, and this subject can be elaborated in a much more thorough research by specialists in the field of security and not only.

We conclude by urging each owner or decision maker of a critical infrastructure to initiate and develop vulnerability scenarios based on potential threats in a network of mutual influences, and to identify solutions in a joint context consistent with the collaborative workflow principle, involving security or other systems

References

[1] BARABASI, A. L.: *Linked noua ştiinţă a reţelelor*. Timişoara : BrumaR Publishing House, 2017. p.12.

[2] *Official Journal of the European Union*, Directive 114/2008, L 345/77, RO.

[3] MARTIN, I.: *Raţionament şi argumentare în planificarea operaţiilor*. Bucharest : "Carol I" National Defense University Publishing House, 2015.

[4] Available at: https://www.recordedfuture.com/russia-ukraine-cyber-front/, accessed on 15.06.2018.

[5] Available at: https://www.reuters.com/article/us-nuclearpower-cyber-germany/german-nuclear-plant-infected-with-computer-viruses-operator-says-idUSKCN0XN2OS, accessed on 30.08.2018.

[6] Available at: https://www.independent.co.uk/travel/news-and-advice/mh17-anniversary-malaysia-airlines-plane-crash-russia-ukraine-conspiracy-theories-a8450501.html, accessed on 10.09.2018.

[7] Available at: https://cyberleninka.ru/article/n/the-sukhoi- su-24-incident-between-russia-and-turkey, accessed on 28.08.2018.

[8] Available at: https://www.worldvision.org/refugees-news-stories/syrian-refugee-crisis-facts, accessed on 10.06.2018.

[9] Available at: https://www.sri.ro/upload/Studiu%20-%20Protectia%20Infrastructurilor%20Critice.pdf, accessed on 10.09.2018.

[10] Available at: http://intelligence.sri.ro/cyber-noul-domeniu-operational-nato/, accessed on 08.09.2018.

Other Sources

[1] ALEXANDRESCU, G., VĂDUVA, G.: *Infrastructuri critice. Pericole, ameninţări la adresa acestora.* Bucharest : Sisteme de protecţie, "Carol I" National Defense University Publishing House, 2006.
[2] National Defense Strategy for 2015-2019, document approved by decision of the Supreme Council of National Defence no. 128 of 10 December 2015.
[3] Communication of the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, Bruxelles, 2009. Available at: http://ec.europa.eu/ transparency/regdoc/rep/1/2009/RO/1-2009- 149 -RO-F1-1.Pdf.
[4] Directive 2008/114/CE of the Council of 8 December 2008 regarding the identification and designation of European critical infrastructures and the assessment of the requirement to improve their protection, Bruxelles, 2008. Available at: http://ccpic.mai.gov.ro/docs/directiva114_RO. pdf?uri=OJ:L:2008:345:0075:0082:RO:PDF.
[5] DRACK, M.. Ludvik von Bertalanffy's early system approach. In *Systems Research and Behavioral Science,* Volume 26, Issue 5, September/October 2009, p. 566. Available at: http://journals.isss.org/index.php/proceedings52 nd/article/viewFile/1032/322.
[6] STEPHEN, P. R.: *Organizational Theory: Structure, Design, and Applications.* New Jersey : Prentice Hall, 1990.

LTC Assoc. Prof. Daniel ROMAN, PhD.
"Carol I" National Defence University
Panduri Street, No. 68-72, sector 5
Bucharest
Romania
E-mail: danutroman2@yahoo.com

LTC **Daniel ROMAN** is an Associate Professor within the Land Forces Department of the Faculty of Command and Staff, at "Carol I" National Defense University in Bucharest.

RISK ASSESSMENT FOR CRITICAL INFRASTRUCTURE IN THE CONDITIONS OF UKRAINE

Serhii IVANIUTA

Abstract: In the article the character of changes in natural and man-made threats for critical infrastructure in the conditions of Ukraine are investigated. Risk assessment for critical infrastructure from emergency situations in Ukraine with regard to the European Union approach is provided. Priorities for risk reduction of emergencies of natural and man-made origin for critical infrastructure protection in Ukraine are recommended.

Keywords: critical infrastructure; risk; threats; likelihood; emergency situations; consequences, priorities.

1 INTRODUCTION

The operation of numerous mining, chemical, energy companies, a large number of industrial and urban agglomerations and the high population density in them predetermine the increase of emergencies situations (ES) with large negative consequences due to the threat of damage and destruction of critical infrastructure objects (CI). Among such facilities, a certain threat comes from the spatially distributed railways, oil and gas pipelines, bridges, main electricity grids, which safe operation are of primary importance for the socio-economic development of Ukraine.

The critical infrastructure of Ukraine is systems and resources, physical or virtual, which are providing functions and services whose violation may lead to significant negative consequences for the life of the society, socio-economic development of the country and the provision of national security [1].

In accordance with the Code of Civil Protection of Ukraine, an emergency situation is the situation in a separate territory characterized by violation of normal living conditions of the population, caused by a disaster, an accident, a fire, a natural disaster, an epidemic, an epizootic or other dangerous event that has led (may lead) to a threat to life or health of the population, a large number of deaths and injuries, causing significant material damage as well as the impossibility of inhabiting the population in such territory [2].

The threat is considered as a dangerous phenomenon, substance, human activity or condition, which may lead to social and economic losses, loss of life, injury or other health consequences of the population, loss of property, livelihoods and services, environmental damage [3].

In the publication, the risk is considered as a combination of the negative effects of the event or the threat and the likelihood of its occurrence associated with it [4].

2 ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

The study of the main trends and nature of changes in emergencies of natural and man-made origin in the world convinces that there is a growing risk of their occurrence [5]. The current programs and reports of the UN and the World Bank on the consequences of natural disasters and man-made disasters in recent years show a significant increase in economic losses from them [5; 6]. The main approaches to assessing the risk of emergencies of different origins are researched in Ukraine [7; 8] and the world [9; 10].

The analysis showed an increase in the threat of reducing the level of safety of numerous critical infrastructure objects in Ukraine as a result of overtime exploitation of structures, equipment and engineering networks which operating on the verge of exhaustion of their resource and forming serious risks of emergencies of natural and man-made nature for the safety of critical infrastructure operation [11, 12].

In addition, in the conditions of the military conflict in the Donbass, due to the destruction of many industrial and residential buildings as a result of hostilities, there is an increase in the risks of the emergence of man-made industrial origin. Military destruction and damage to many critical infrastructure objects, which can include water treatment plants, chemical plants and agricultural enterprises, poses a serious threat to the population and the environment.

Research in the area of prevention and counteraction to threats of different genesis suggests that the state system of protection of population from natural and man-made ES requires the introduction of a risk-based approach for the effective prevention and reduction of the risk of disasters of various origins for critical infrastructure objects [13; 14].

It should also be considered that the negative nature of changes in environmental and man-made threats that occurs due to pollution of river basins and underground waters, the destruction of landscapes and objects of the nature reserve fund, significantly reduces the level of safety of life of the population in the zone of military conflict in the eastern Ukraine, as well in other territories of Donetsk and Luhansk oblasts, ecologically connected with it.

Significant threat of emergencies of natural and man-made origin comes from the presence in the territory of Luhansk and Donetsk regions of a large number of flooded and semi-flooded mines, which have a permanent hydraulic connection with the

existing mines. The unsatisfactory ecological state of coal mining regions, especially Donbass, is complicated by the high concentration of metallurgical and chemical enterprises, which increases the technogenic load on the environment and creates real threats to the health of the population.

The goal of the article is to analyze the changes of actual threats of natural and man-made nature for critical infrastructure in Ukraine, and on this basis to conduct risk assessments for critical infrastructure with the methodology used in the European Union.

3 PRESENTATION OF THE MAIN RESEARCH MATERIAL

During 2016, there were 149 emergencies in Ukraine, of which 89 were of a natural origin, 56 were man-made (Table 1). As a result of these events, 171 people died and 1856 people were injured.

Table 1 Characteristics of natural and man-made emergency situations in Ukraine in 2015-2016

Emergency situations			Threats for population			
Type	Amount of ES		Died		Injured	
	2015	2016	2015	2016	2015	2016
Emergency situations of man-made origin						
Accidents or catastrophes in transport	14	11	53	33	74	128
Fires, explosions	40	36	103	116	59	35
Including in buildings or constructions of residential purposes	*30*	*29*	*85*	*100*	*6*	*11*
The presence of harmful and radioactive substances exceeding The maximum permissible concentrations in the environment	1		0	0	0	0
Sudden destruction of buildings and structures	2	4	0	3	0	2
Crashes in life support systems	5	4	0	0	0	0
Accidents in oil and gas industrial complex systems	1	1	0	0	0	0
Total	***63***	***56***	***156***	***152***	***133***	***165***
Emergency situations of a natural origin						
Geological ES	2	1	0	0	0	0
Meteorological ES	2	6	0	4	7	13
Hydrological ES of surface waters	1		0	0	0	0
related to fires in natural ecological systems	13	4	0	0	0	1
Medical-biological ES	59	78	22	15	690	1677
Total	***77***	***89***	***22***	***19***	***697***	***1691***

Source: [15].

Despite the fact that in comparison with 2015, there was a certain decrease in the number of emergencies of an industrial nature for all types, in 2016 there was an increase of 17 % in the number of deaths in the emergencies associated with fires (explosions) in buildings and structures for residential use, as well as an increase of 72 % of the number of victims as a result of ES in road transport.

In spite of a certain decrease in the number of emergencies of the state level in 2016, the level of risks of natural and man-made disasters and the risks of losses from them remains rather high for most regions of Ukraine. Thus, the largest number of emergencies (14) during 2016 was recorded in the Odessa region. In the Volyn, Mykolaiv and Poltava regions there were 10 ES, in Dnipropetrovsk, Zhytomyr and Chernihiv regions - 8, respectively, in Sumy, Chernivtsi regions and in Kyiv, 7 emergencies were registered.

Among the main reasons for the emergence of natural and man-made disasters in Ukraine in 2016 are non-compliance with the rules of fire safety; ignoring requirements of the rules of the traffic; violation of sanitary and hygienic norms; reduction of control over the implementation of anti-epidemic measures; outdated fixed assets and the state of emergency of a large part of the utilities networks; abnormal manifestations of atmospheric processes [15].

In the first quarter of 2017, 48 ES were registered in Ukraine, 14 of which were man-made and 33 were natural and one of social character [16]. During these events, 47 people died and 261 injured. Compared to the same period in 2016, the total number of ES in 2017 increased by 71.4 %, while the number of ES of anthropogenic nature remained unchanged, and the number of ES of a natural origin increased more than twice, which is explained by an increase in the proportion of medical and biological emergencies.

Separately, it should be emphasized on cases of increased risk of emergence of man-made origin in the zone of anti-terrorist operation (ATO) due to the destruction of many industrial and residential buildings as a result of hostilities. Damage to critical

infrastructure objects, including water treatment plants, chemical plants and agricultural enterprises, caused by an armed conflict in eastern Ukraine, poses a serious threat to the population and the environment not only in Donetsk and Lugansk regions, but also throughout Ukraine. Therefore, the protection of infrastructure in the territory of a military conflict is extremely important. The OSCE has repeatedly urged the conflicting parties in the Donbass to make every effort to protect the vital objects of the civilian infrastructure of the region, since damage to any of them could lead to an ecological catastrophe, which would significantly aggravate the situation on both sides of the collision [17].

According to the OSCE Special Monitoring Mission, which operates in the area of the anti-terrorist operation, Donetsk filtration station during the year 2017 at least 9 times suffered significant damage. This led to her stoppage [18]. In general, due to the shelling of militants, this station, which provides 600,000 people with water on both sides of the line of demarcation, did not work for 45 days. According to the OSCE, more than 1 million people may be left without water because of numerous damages to infrastructure as a result of hostilities in the Donbass.

It is worth noting the growth of cybernetic threats for critical infrastructure of the state caused by hacker attacks, which can lead to failures of important information infrastructure. So, on June 27, 2017, Ukrainian institutions became victims of a large-scale cyberattack carried out with the help of the virus Petya. A. Hacker attacks were aimed at objects of critical information infrastructure of energy generating and power supply companies, transport facilities, a number of banking institutions, telecommunication companies. The reports of defeats of the information systems of commercial companies came from the Auchan network, the DHL postal service, commercial banks and telecom operators [19]. The virus struck numerous state resources, in particular the system of the Ministry of Infrastructure, the State Fiscal Service of Ukraine, the electricity distribution networks of Ukrenergo, etc.

Given the scale of cross-border impact of emergencies of various origins, international cooperation in disaster risk reduction is extremely relevant to Ukraine. The importance and the need to coordinate efforts to reduce the risk of emergency at the international, regional and local levels in recent years was paid in several multilateral framework programs and declarations. Among these important "Yokohama Strategy and Plan of Action for a safer world: Guidelines for disaster management, preparedness and mitigation", which was adopted in 1994 and today is the basic document of the United Nations in the field of disaster risk reduction and mitigating their negative consequences [21].

In general, this approach involves performing at the state level the relevant tasks, the most important of which is the inclusion of disaster risk reduction measures in the plans and programs of socio-economic development [23]. The ultimate goal is to prevent the emergence of new ones and to reduce the known disaster risks by implementing complex and inclusive economic, structural, legal, social, health, cultural, cultural, educational, environmental, technological, political and institutional measures that prevent and reduce the propensity to influence dangerous factors and vulnerability to disasters, increase readiness for response and recovery, and thus strengthen the potential of counteraction to the state.

4 RISK ASSESSMENT FOR CRITICAL INFRASTRUCTURE

In general, risk assessment includes several steps:

- identification of risks as a process of their recognition and description,
- risk analysis, which involves understanding the nature of the risk and determining its level,
- risk assessment, which involves comparing the results of the risk analysis with the criteria for determining whether the risk is acceptable.

If the problem of preventing and preparedness for a particular type of threat is addressed, the risk can be quantified as a function of the likelihood of occurrence of a threat, exposure (the total cost of all elements exposed to risk) and vulnerability [24].

At the same time, in the EU countries, in order to carry out a National Risk Assessment for critical infrastructure, it is recommended to use a risk matrix with a dimension of 5 x 5 as a means of visualizing the evaluation results (Figure 1).

Risk assessment should be based on three different categories of exposure and consider the negative consequences for human (population), economy (and environment), as well as political and social consequences. At the same time, for the first two categories of influence, the negative consequences are determined quantitatively as the number of dead (injured) persons or economic losses in UAH (Euro). Consequences for the third category of influence, considering social and political interconnections, are determined by qualitative indicators.

In the European Union, each country has to carry out risk assessments for each category of consequences and, accordingly, build three different risk matrices when conducting risk assessments for critical infrastructure. Among the various threats of different origins for critical infrastructure security (CI), the following are the most important [24]:

- natural: floods, extreme weather events, forest fires, earthquakes, epidemics and pandemics, epizootics,

• man-made:
  a) inadvertent: industrial accidents, nuclear / radiological accidents, transport accidents, loss of critical infrastructure,
  b) malicious: cyberattacks, terrorist attacks.

Particular attention is needed to the interconnections and interdependence between threats of natural origin when the emergence of some dangerous phenomena leads to the formation of new through the mechanism of cascading effects (Table 2).

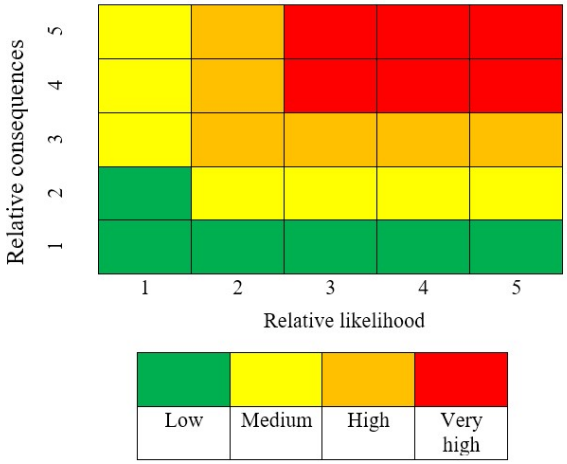


Fig. 1 Sample of the risk matrix
Source: [24].

Table 2 Interconnections and interdependencies between threats

Threat	Related Threats
Hazardous weather phenomena	Floods, landslides, forest fires, pollution, loss of critical infrastructure, traffic accidents
Earthquakes	Landslides, tsunami
Landslides, volcanoes	Transport accidents
Nuclear, chemical and transport accidents, loss of critical infrastructure	Pollution, terrorist and cybernetic attacks
Loss of critical infrastructure	Floods, pollution, loss of critical infrastructure, pandemics
Pollution	Pandemic

Source: [24].

The awareness of cascading effects of modern threats is quite complicated due to the interconnection of infrastructure objects and the environment surrounding it. Failure to reach agreement of stakeholders and political leadership in predicting and mitigating the negative effects of new threats, primarily of natural origin, can lead to serious violations of the critical infrastructure in the near future.

The risk assessment of the death from the ES of natural and man-made origin is carried out in accordance with available data from the State Service of Emergency Situations of Ukraine regarding the threats of different origin, therefore a risk matrix is constructed. At the same time, according to statistical data, the likelihood of emergence of dangerous situations and the likelihood of death from them is calculated, and on this basis a corresponding dependence is formed that was done to address the purpose of this publication (Figure 2). The likelihood of the ES was determined as the ratio of the number of ES of the corresponding type to the total number of ES that occurred during the year.

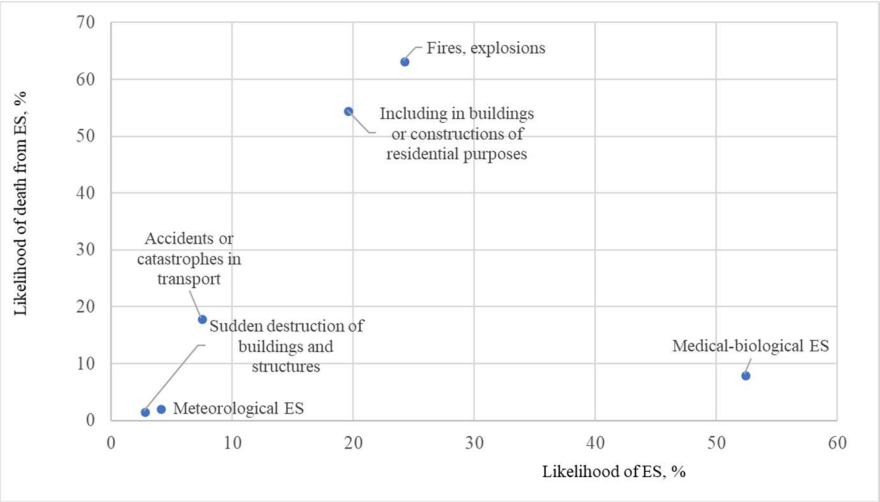
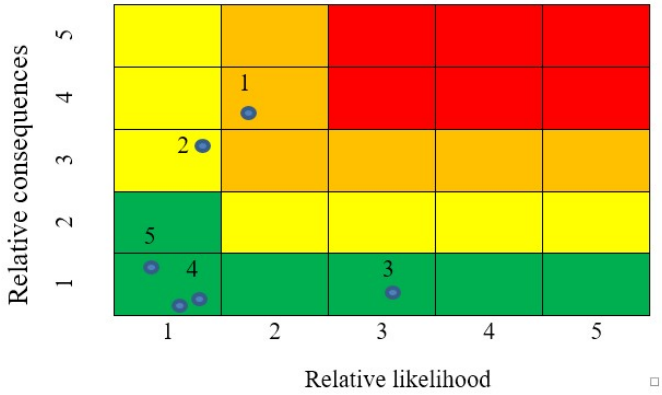


Fig. 2 Dependence between likelihoods of and the death from ES in 2016
Source: author's calculations.

The results of the assessment indicate that the greatest likelihood of occurrence of emergency situations with human victims in Ukraine is typical for medical-biological emergency, fires, explosions in buildings and structures, accidents and transport accidents. At the same time, the greatest likelihood of death is characterized by dangerous situations arising as a result of fires, explosions, including in buildings and structures, as well as accidents and catastrophes in transport.

Considering the obtained results of estimating the likelihood of occurrence of ES and death from them, the risk matrix is then constructed according to the model used in the EU (Figure 3).



Notes:
1 – ES as a result of fires, explosions;
2 – ES due to fires, explosions in buildings or constructions of residential purposes;
3 – medical and biological emergency;
4 – meteorological ES;
5 – ES due to accidents or disasters in transport

Fig. 3 Risk matrix of death from the ES in 2016
Source: author's calculations.

Analyzing the results obtained, we can note: an increased risk of death is characteristic of emergency situations, which occurred during fires, explosions. The average level of risk is due to fires, explosions in buildings or buildings of residential purposes. Other types of ES, which are considered in this study, including medical-biological, meteorological, emergency situations, which occurred as a result of the sudden destruction of buildings and structures, are characterized by low risk of death.

From the point of view of making managerial decisions on reducing the victims from the ES of different origin, it is obvious that the primary attention should be directed specifically to counteracting and reducing the risks of the occurrence of fires and explosions, including at objects of critical infrastructure. In turn, management and, to a certain extent, risk reduction involves a process of risk mitigation under different scenarios, such as:

- avoiding risk, the completion or rejection of the activity causing the risk,
- taking risk in order to take advantage of certain opportunities,
- exclusion of a source of risk,
- change of likelihood,
- change of consequences,
- distribution of risk to the other party by contracting or financing risks,
- preservation of existing risk level based on a coherent solution.

In the conditions of complex interconnections and mutual influences of the main factors of the formation of the ES, an effective process of reducing the risk will involve the combined implementation of several of these scenarios, which can be worked out based on the use of expert assessment methods.

At the same time, it should be borne in mind that the risk matrix (Figure 2) in determining the economic losses and losses for the environment from the ES will be significantly different from that discussed above (Figure 3), since for Ukraine the greatest economic losses are characterized by threats of natural origin, in first of all those that are related to meteorological emergency and dangerous exogenous geological processes.

5 CONCLUSIONS

Nowadays in Ukraine there are tendencies for further decrease of the level of safety and reduction of the duration of work of objects of critical infrastructure that arise as a result of overtime operation of buildings, structures, equipment and engineering networks operating on the brink of exhaustion of their resource and forming the serious threats of emergencies of natural and anthropogenic character for the safety of the operation of critical infrastructure objects.

In the conditions of the hybrid war in the east of Ukraine there is an increase in the risks of the emergence of man-made industrial origin in the ATO zone due to the destruction of many industrial and residential buildings as a result of hostilities. The damage caused by the military conflict in eastern Ukraine to critical infrastructure objects, in particular water treatment plants, chemical plants and agricultural enterprises, poses a serious threat to the population and the environment of the region.

A significant risk of emergencies of natural and man-made origin on the territory of the ATO generates the presence of a large number of flooded and semi-flooded mines in the Luhansk and Donetsk regions, which have a permanent hydraulic connection with the existing mines. The unsatisfactory ecological condition in coal mining areas of the Donbas is intensified due to the concentration of enterprises in the metallurgical and chemical industries, which increases the technogenic load on the environment and creates real threats to the formation of an emerging man-made state with massive negative consequences for the population.

The development and implementation of measures to reduce the risks of ES of different origins on critical infrastructure objects is hampered by the lack of a national body responsible for coordinating existing state security and crisis response systems in the area of critical infrastructure protection. To date, the state has no single methodology for assessing threats and risks to critical infrastructure, which also complicates the development of measures to prevent and minimize the negative consequences of the ES, which are possible on the territory of Ukraine, on critical infrastructure objects.

6 SUGGESTIONS

At the moment one of the most significant step forward is the development and submission to the Parliament of Ukraine of a draft law "On the Protection of Critical Infrastructure", which should address all aspects of the establishment of a state system for the protection of critical infrastructure, including the body responsible for coordinating critical infrastructure protection activities.

Among them priority should be given to defining the functions and powers of central executive authorities in the area of critical infrastructure protection, rights, responsibilities and responsibilities of owners and operators of critical infrastructure objects, the introduction of criteria for assigning objects to critical infrastructure on a critical scale, the order of their certification and categorization.

At the same time priority should be given to the formation of criteria for assigning objects, including potentially dangerous, to critical infrastructure, assessing threats to critical infrastructure, developing plans to ensure the sustainability of the functioning of critical infrastructure and the formation of a nationwide system of interaction in accordance with the competence of ministries.

Prospects for further exploration in this area are related to conducting a risks assessment of natural and man-made disasters for critical infrastructure objects of Ukraine, their categorization by types and levels of risk, and also the development of well-grounded measures to prevent the emergencies with large negative consequences for the CI.

Such risk assessment will require the availability of operational and objective data on monitoring of actual natural and man-made threats, especially regarding economic losses from their implementation. In this regard, the restoration of the proper functioning of the Government Information and Analytical System for emergencies and the improvement of the system of early detection of threats and reduction of the risks of emergencies of natural and man-made origin for CI are important.

This system will be able to provide an effective interagency information interaction and support for the adoption of management decisions to prevent the emergence of different origins based on the use of modern methods of spatial analysis and mathematical modeling of emergencies based on a comprehensive processing of operational, analytical, reference, expert and statistical data from different information sources.

References

[1] *Green Paper on critical infrastructure protection in Ukraine: Mater.* International expert. Meetings. D. S. Biryukov, S. I. Kondratov; edited by O. M. Sukhodolya - K.: NISS, 2016. 176 pp.

[2] *Code of Civil Protection of Ukraine.* [Electronic resource]. Available at: http://zakon3.rada.gov.ua/laws/show/5403-17. Accessed 17 Aug 2018.

[3] UNISDR. (2009, May). 2009 UNISDR Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction. [Electronic resource]. Available at: http://www.unisdr.org/files/7817 UNISDRTerminologyEnglish.pdf. Accessed 19 Aug 2018.

[4] ISO31000:2009 – Risk management. Principles and guidelines. International Organization for Standardization, 2009.

[5] 2011 Global Assessment Report on Disaster Risk Reduction. Revealing Risk, Redefining Development. [Electronic resource]. Available at: www.preventionweb.net/gar. Accessed 10 Aug 2018.

[6] World Bank. 2010. *Natural hazards, unnatural disasters: The economics of effective prevention.* Washington : World Bank and United Nations. Gupta, 2011. 587 p.

[7] BYCHENOK, M. M., IVANUTA, S. P., YAKOVLEV, Y.O.: *On complex assessment of life-threatening risks in potentially hazardous regions.* Ecology and Resources: Sb. sciences Works of the Institute of National Security Problems. K.: IPNB, 2007. No. 17. P. 33-42.

[8] LESCHINSKY, O. L., SHKOLNY, O.V.: *Economic risk and methods of its measurement*. K.: Delta, 2005. 112 p.

[9] BERNSTEIN, P. L. *Against the Gods: the Remarkable Story of Risk.* John Wiley & Sons, 1996. 383 p.

[10] MORGAN, M. G., HENRION, M. *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. Cambridge : Cambridge University Press, 1990. 344 p.

[11] KACHINSKY, A. B.: *Security, Threats and Risks: Scientific Concepts and Mathematical Methods.* K.: IPNB, NASBU, 2004. 472 p.

[12] BECK, U.: *World Risk Society.* Cambridge : Polity Press, 1998. 425 p.

[13] Assimilation potential of the geological environment of Ukraine and its estimation. S.O. Long, V. V. Ivanchenko and others. National Academy of Sciences of Ukraine, Institute of Telecommunications and Global Inform. space - K.: Nika-Center, 2016. 176 p.

[14] IVANYUTA, S. P., KACHINSKY, A. B.: *Ecological and natural-technogenic safety of Ukraine: a regional dimension of threats and risks.* Monograph. National. in-t of strategic research. K.: NISS, 2012. 308 p.

[15] Information and analytical information on the emergence of the National Assembly in Ukraine during 2016. [Electronic resource]. Available at: http://www.dsns.gov.ua/ua/Dovidka-za-kvartal/ 57279.html. Accessed 7 Aug 2018.

[16] Information and analytical information on the emergence of the National Assembly in Ukraine during the first quarter of 2017. [Electronic resource]. Available at: http://www.dsns.gov.ua/ua/Dovidka-za-kvartal/61431.html. Accessed 10 Aug 2018.

[17] The OSCE called for the protection of important infrastructure in the Donbass. [Electronic resource]. Available at: http://www.theinsider.ua/politics/593595f08e98b/. Accessed 11 Jul 2018.

[18] This year Donetsk Fltr Station shelled at least 9 times & not operational 45 days [Electronic resource]. Available at: https://twitter. com/OSCE_SMM/status/876430361366073344?ref_src=twsrc%5Etfw&ref. Accessed 10 Jul 2018.

[19] Petya virus cyberattack. [Electronic resource]. Available at: http://www.dw.com/uk. Accessed 11 Jul 2018.

[20] S/RES/2341 (2017) – Protection of critical infrastructure. [Electronic resource]. Available at: http://www.un.org/en/ga/search/view.doc.asp?symbol=S/RES/2341%282017%29&referer=/english/&Lang=E. Accessed 8 Jul 2018.

[21] International Decade for Natural Disasters Reduction. Yokohama Strategy and Plan of Action for a safer world. In *World conference*

on natural disaster reduction, Yokohama, Japan, 1994.
[22] UNISDR (United Nations, International Strategy for Disaster Reduction). Hyogo framework for action 2005–2015: building the resilience of nations and communities to disasters. In *World conference on disaster reduction.* Kobe, Japan, January 2005.
[23] Sendai Framework for Disaster Risk Reduction 2015–2030. [Electronic resource]. Available at: http://www.unisdr.org.
[24] Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. Luxembourg: Publications Office of the European Union, 2015. 40 p.

Serhii Ivaniuta is a deputy head of energy and technogenic security department at National Institute for Strategic Studies in Ukraine. He is a Doctor of engineering science and Senior research fellow with 18 years of experience. He participated in various National and international research related to critical infrastructure protection and environmental security issues. Currently his research is focused on risk accessment for critical infrastructure and development of critical infrastructure protection system in Ukraine.

Serhii IVANIUTA
Doctor of Engineering Sciences
Senior Research Fellow
National Institute for Strategic Studies
Chokolivskiy blvd., 13, Kyiv
Ukraine 03186
E-mail: ivanyuta@niss.gov.ua

THE EFFECTS OF TWO DIFFERENT PHYSICAL TRAINING PROGRAMS ON MOVEMENT PERFORMANCE OF PROFESSIONAL SOLDIERS

Roman MARKOVIČ

Abstract: The level of physical fitness is checked annually for each professional soldier by an annual exercise performance test. At work, we investigated the impact of two different physical fitness programs on the performance of professional soldiers in the annual physical fitness tests. In the overall assessment of the annual physical fitness tests, Group 1 improved from 147 points on the input measurement to the final 183 points in the output measurement, improved by 36 points (12 % increase in movement performance). Group 2 improved by 15 points from 155 to 170 points (5 % increase in movement performance). Based on the results, we can state that the proposed comprehensive motion training program is an effective and appropriate means of developing the movement performance of professional soldiers and we recommend that it be put into practice.

Keywords: movement program; professional soldier; movement performance; movement abilities; physical fitness tests.

1 INTRODUCTION

The army increasingly emphasizes the importance of physical training, whose job is to ensure the optimum level of movement performance of the professional soldiers.

According to Harman et al. (2008), the soldier has to engage in a lot of physically demanding activities in the field of combat, such as long-range field shifts, short-lived activities such as spying through the battlefield and overcoming various obstacles in the rural and urban terrain. The speed at which these activities can be performed may affect the combat effectiveness and survival of soldiers. Therefore, it is important to look for the best training programs within the time constraints of the army and thus prepare the soldiers to fight.

Each army must, therefore, guard the level of physical fitness and readiness of its soldiers. Its verification uses the established performance standards that must be met by soldiers in order to carry out their profession. The soldier of the Slovak Republic must annually pass annual physical fitness tests, where he has to complete three disciplines (sit-ups per 1 minute/pull ups, 10 x 10 m shuttle run/ 60 m dash, 12 minutes running / 300 m swimming) with which it is then spotted. Based on the age category, he is awarded a final rating of 1-3 completed and 4 failed. Each country has set its own testing standards, which has been further described by Stilwell (2015), Malmberg (2011). Few studies have been conducted to examine the improvement of exercise performance through physical training programs, Heinrich et al. (2012), Harman et al. (2008) investigated the effectiveness of the US Army's Physical Motion and Weight-Based Training (WBT) in US Army soldiers, they found that self-weight training (SPT) is a more effective means of developing exercise performance as a weight-training exercise (WBT). In the past, authors have been updating and streamlining the training system for professional soldiers of the Slovak armed forces Pápay et al. (2010), Pápay, Litva (2012), Litva (2005). Abroad on the optimization, effectiveness and usability of motion programs in the armed forces Santilla, et al., (2015), Roos et al. (2015), Groeller (2015), Harman et al. (2008), Knapik et al. (2009), Heinrich et al. (2012), the findings of all these authors were used to create a complex motion program that we applied during the experiment. In the creation of the content of a complex motion program in the field of physical development, we have provided many valuable insights on Stilwell (2005), Lauren, Clark (2013), Peřič, Dovalil (2010), Zatsiorsky, Kraemer (2014), Vanderka (2013) 2004), Dufour (2015), Wade (2015), Dívald (2010), Šimonek (2009, 2013), Bursová (2005). We have provided valuable insights on the impact of stressors on the human organism and on its performance in combat activities, Lindholm, Lundgren (2009), Wilmore-Costill (2008), Macek, Radvansky (2011), McAardle et al. (2006), Driskell, Salas (2009).

2 AIM

The aim of this work is to investigate the influence of two different physical education programs on increasing the movement performance of professional soldiers and their results in the annual physical fitness test.

3 HYPOTHESIS

H 1: We assume that Group 1 (Complex Motion Program) will be a more effective means of developing the selected motion skills of the professional soldiers as a current system of physical training (Group 2).

H 2: In Group 1 we expect higher point increments in the overall assessment of the annual review of the movement performance of the professional soldiers than after the current physical training system (Group 2).

H 3: Effect of experimental factor Group 1, we expect statistically significant changes in the level of the dynamic and endurance force of the abdominal, skeletal and muscular muscles, as measured by the test, sit-ups per 1 minute.

H 4: We assume that under the influence of the complex motion program there will be a positive influence of the speed capabilities in the experimental set, where we expect statistically significant changes in the level of the running speed with the changes of direction, as measured by the 10 x 10-meter shuttle run test.

H 5: In Group 1, we expect statistically significant changes in the level of runner endurance, as measured by the 20 m endurance shuttle test (Beep test).

H 6: We assume that with the impact of a complex motion program in a 10-week mesocycle, the professional soldiers will have a positive influence and statistically significant changes in the level of force capability as measured by the pull-ups test.

4 METHODOLOGY

In the research, we used a two-group crossed pedagogical experiment where we will work with two unbalanced groups of individuals in three phases of the experiment (Chráska, 2007). The experiment was carried out at the Academy of the Armed Forces in Liptovsky Mikulas (hereinafter AAF LM), with two-year students (1st and 2nd year). The entire course of the cross-over experiment approaches Tables 1, 2.

Table 1 Characteristics of the research groups in individual phases.

Group	Phase	Date	Probands	Age AVG	Testing		Experimental factor	Participation
					input	output		
1	1	2.10.2017-11.12.2017	students 2nd year	20,67	50 students	42 students	Complex movement program of physical training 5 x 20 min weekly	69%
							Physical education 2 x 90 min weekly	85%
2	1	2.10.2017-11.12.2017	students 1st year	19,71	53 students	37 students	Morning physical exercices 5 x 20 min weekly	84%
							Physical education 2 x 90 min weekly	88%
1,2	2	12.12.2017 - 2.3.2018	Without experimental intervention Physical education 2 x 90 min weekly					
1	3	5.3.2018 - 14.5.2018	students 1st year	20,25	37 students	34 students	Complex movement program of physical training 5 x 20 min weekly	87%
							Physical education 2 x 90 min weekly	76%
2	3	5.3.2018 - 14.5.2018	students 2nd year	21,23	42 students	40 students	Morning physical exercices 5 x 20 min weekly	83%
							Physical education 2 x 90 min weekly	86%

Table 2 Summary characteristics of the research groups in individual phases

Group		Probands	Age AVG	Testing		Experimental factor	Participation
				input	output		
1		students 1st, 2nd year	20,5	103 students	74 students	Complex movement program of physical training 5 x 20 min weekly	78%
						Physical education 2 x 90 min weekly	81%
2						Morning physical exercices 5 x 20 min weekly in the	84%
						Physical education 2 x 90 min weekly	87%

Research in group 1 was realized in the gym no. 1 AAF LM. At the beginning of the observation period, the conditions for the course and organization of a complex physical program of physical training were determined by the author of the research. In Group 2 morning physical exercises took place at AAF LM premises as instructor training. The input and output testing were carried out in the gym no. 1 AAF LM, under the supervision of the author of the research and one member of the AAF LM Department of Physical Education and Sports, which was present in all measurements.

Group 1 exercise in a 10-week mesocycle 5x weekly 20 minutes exercises of a complex motion program from physical training, the main essence of which is based on the development of coordination and conditioning skills, not only through athletic, gymnastics, combat exercises, but also through the gradual increase of adaptation of the human organism to the action of stressors (hunger, apnea, cold, pain, lack of time, lack of sleep). The 10-week mesocycle was divided into 5 microcycles, which were primarily focused on the development of mobility, then on the development of maximum strength, proprioceptive ability, power-speed development, and ultimately strength-endurance skills. Group 1 has completed a 90-minute physical education weekly focused on the military-run, an obstacle track, close combat, military-practice climbing, and swimming.

Group 2 performed 5-week 20-minute morning physical exercises on the basis of a military program (5 minutes of warm-up, 5 x 400 meters run in the aerobic zone and 5 x 10 push-ups and 10 squats) for 10 weeks. 2 x per week 90 minutes of physical education performed on the basis of accredited study programs for individual study departments in a similar form to group 1. We used the following input and output tests to determine the level of general movement performance and the impact of complex movement program on physical training:

- sit-ups per 1 minute (Vestník MO SR č.100, 2015, Eurofit, 2002),
- pull-ups (Vestník MO SR č.100, 2015),
- 10 x 10 m shuttle run (Vestník MO SR č.100, 2015),
- beep test 20 m (Eurofit, 2002).

The 12-minute run values were obtained based on the performance calculations in the 20 m endurance boat run, using "Beep Test VO2max Calculator" by Wood (2008). The reference groups were characterized in numerical and graphical form. In numerical form, we used the basic statistical characteristics of the central position (average, median) and variability (standard deviation, maximum, minimum, integer quotient). Normality of distribution was reviewed by Shapiro - Wilk test. Differences between significance levels (average and median) were characterized by the difference (d), statistical significance and magnitude of the effect. Changes in motor performance and somatic variables independent groups were assessed by paired t-test to assess the significance level equivalence in order to demonstrate the statistical, factual, practical and clinical significance of the tests, using the Effect Size coefficient based on their estimate (Cohen's coefficient of action "d"). To reject the zero hypothesis about the equivalence of significance levels, we determined the significance level $p \leq 0.01$. Numerical processing of empirical data was evaluated by table and statistical program, MS Excel. When comparing the results of the movement performance, we used a table with norms for the evaluation of the movement performance of professional soldiers (Vestník MO SR č.100, 2015 and Vestník MO SR č.54, 2016). When processing research data, we followed the procedures recommended by Hendl (2004).

5 RESULTS

The aim of the research was to find out the influence of two different physical training programs on increasing the movement performance of the professional soldiers and their results in the annual physical fitness test. On the basis of the overall results achieved in the individual tests, we can conclude that in the overall assessment of the annual physical fitness test of the professional soldiers, both programs have achieved a significant improvement in their motion performance. In the overall assessment of the annual physical fitness test, Group 1 improved from 147 points on the input measurement to the final score of 183 points in the output measurement (pull ups - 10 x 10 m shuttle run - 12-minute run), the respondents improved by 36 points (12 % increase in movement performance). In the discipline evaluation (sit-ups per 1 minute - 10 x 10 m shuttle run - 12-minute run), the improvement was 150 points to 177 points on the final test, the improvement was 27 points. Group 2 improved by 15 points from 155 to 170 points (5 % increase in exercise performance) for both tested variants.

An important point is that Group 1 achieved stronger improvements in each of the tested disciplines compared to Group 2 and in the overall assessment of the annual physical fitness test, we have seen more than double the improvement of the group performing the complex motion program, which is confirmed by **H2.**

Based on the results from Table 4 we can state that we have demonstrated on the basis of the mathematical difference "d" the improvement of the movement performance in all disciplines tested in both groups. In Group 1, we recorded more significant increases in movement performance than group 2, we confirming **H1**.

In Group 1 we have seen significant improvements in all disciplines to 1 % of the level of statistical significance ($p \leq 0.01$). Group 1 achieved significant improvements with a mean effect in the discipline pull-ups ($p \leq 0.01$, $r=0.42$-0.70) and sit-ups per 1 minute ($p \leq 0.01$, $r=0.52$) which is confirmed by the **H6** and **H3** shown in Table 4. Due to the complex motion program occurred changes at the run speed with changes in direction and at run endurance level significant improvements with a high effect ($p \leq 0.01$, $r \geq 0.71$) in the 10x10m shuttle run and the endurance shuttle run to 20m confirmed by **H4** and **H5**.

In Group 2 we also saw significant improvements in all tested disciplines, while effect size in sit-ups per 1 minute, 10x10m shuttle run and in pull-ups was small. The mean effect ($p \leq 0.01$, $r = 0.42$-0.70) was measured only in endurance shuttle run at 20m. The group performing a complex motion program has achieved greater points in the overall assessment of the annual examination of the movement performance of the professional soldiers than after the current physical training system (Group 2).

Table 3 Evaluation of annual examination from the motor performance

Evaluation of annual examination from the motor performance of professional soldiers															
GROUP	Testing	Age AVG	Age category	Sit ups per 1 minute	points	Pull ups	points	10x10m shuttle run	points	12 minute run	points	ALL POINTS	RATING	Mathematic diference "d"	%
1	input	20	1	54	59			26,1	57	2320	34	150	4	27	9
	output			57	64			25,4	65	2590	48	177	2		
2	input			55	60			26	58	2370	37	155	4	15	5
	output			57	64			25,6	62	2500	44	170	2		
1	input					9	56	26,1	57	2320	34	147	4	36	12
	output					12	70	25,4	65	2590	48	183	2		
2	input					10	62	26	58	2370	37	157	4	15	5
	output					11	66	25,6	62	2500	44	172	2		

Table 4 Descriptive statistic

Table 4 Descriptive statistic		Basic statistical characteristic					Differencies (mathematic difference "d", percentual deviation, statistic significance, factual significance, effect size)					
TEST	Testing	Number of	Mean	Standard deviation	Min.	Max.	d (x1-x2)	%	paired t-test	p-value p≤0.01	ES Cohenov "d"	Effect size
GROUP 1												
Sit ups per 1 minute [reps]	input	74	54,30	6,00	39,00	70,00	-3,11	-5,41	20,98	YES	-0,52	medium effect
	output	74	57,41	6,04	44,00	72,00						
10 x 10 m shuttle run [sec]	input	74	26,09	0,94	23,84	28,18	0,67	2,64	16,27	YES	0,73	**big effect**
	output	74	25,42	0,91	23,30	27,20						
Pull ups [reps]	input	74	9,45	4,02	2,00	20,00	-2,39	-19,41	28,14	YES	-0,53	medium effect
	output	74	11,84	4,62	3,00	23,00						
Beep test 20 m [reps]	input	74	65,89	15,08	30,00	105,00	-15,01	-18,56	19,35	YES	-1,13	**big effect**
	output	74	80,91	11,28	56,00	114,00						
GROUP 2												
Sit ups per 1 minute [reps]	input	74	54,59	6,50	31,00	72,00	-2,09	-3,69	6,56	YES	-0,34	small effect
	output	74	56,69	5,67	40,00	72,00						
10 x 10 m shuttle run [sec]	input	74	26,02	1,20	23,65	28,90	0,45	1,77	5,91	YES	0,40	small effect
	output	74	25,57	1,06	23,06	28,17						
Pull ups [reps]	input	74	9,99	4,17	0,00	19,00	-1,14	-10,25	7,72	YES	-0,27	small effect
	output	74	11,14	4,43	1,00	23,00						
Beep test 20 m [reps]	input	74	67,76	12,53	39,00	100,00	-7,62	-10,11	7,70	YES	-0,66	medium effect
	output	74	75,38	10,57	40,00	101,00						

6 CONCLUSION

Based on the results of our research, we recommend for an increase of level movement performance professional soldiers to apply for Program no. 1 (complex motion program). An important point is the fact that for Group 1, which performed a complex motion program for 10 weeks, all hypotheses and improvements in each of the tested subjects were significantly confirmed from the hypotheses assumed compared to Group 2 was twice as effective. This suggests that the proposed complex motion training program is a more effective and appropriate means of developing motion performance for professional soldiers than the current physical training system. From the results, we can further state that the current system of physical training is a suitable means of maintaining the same physical performance and can therefore only be applied to professional soldiers who want to maintain approximately the same level of physical fitness (1 for "excellent" or 2 for " good"). For professional soldiers who do not have enough physical performance (score 4 - "nonconforming" or 3 - "conforming"), we need to achieve a more pronounced performance improvement of at least 30 points in order to increase the performance by at least one mark and thus ensure the ability to perform professional soldier services. The research results confirmed that if we need to increase the movement performance, it is appropriate to apply a complex motion program to professional soldiers for 10 weeks, which confirmed 36 points increase, which is a good improvement.

We also compared program no. 1 and program no. 2 with similar studies by Heinrich et al. (2012), Harman et al. (2008) that investigated the effectiveness of the standard motion program (SPT) and weight-based training (WBT) in US Army soldiers. They found that self-weight training (SPT) is a more effective means of developing movement performance than a Weightlifting exercise (WBT). When comparing the results we found similarity with the results of the program no. 2 with the US Army's Standard Motion Program (SPT). Complex motion program No. 1 was, however, more effective than both US Army programs. Therefore, we recommend that this movement program is put into practice and used as an effective means of training professional soldiers under AAF and within the armed forces. We will propose a complex motion program to supplement the legislation in the field of professional

training of professional soldiers, which would contribute to an increase in the physical fitness and movement performance of professional soldiers of the Armed Forces of the Slovak Republic.

References

[1] BURSOVÁ, M.: *Kompenzační cvičení*. Praha : Grada publishing, 2005. ISBN 80-247-0948-1.

[2] DÍVALD, L.: *Kontrolovaný tréning*. Poprad : Popradská tlačiareň, 2010. ISBN 978-80-970358-1-5.

[3] DRISKELL, J., SALAS, E.: *Stress and human performance.* New Jersey : Psychology Press, 2009. 314 s. ISBN 0-8058-1182-6.

[4] DUFOUR, M.: *Pohybové schopnosti v tréninku: RYCHLOST.* Praha : Mladá fronta, 2015. ISBN 978-80-204-3461-6.

[5] GROELLER, H., BURLEY, S., ORCHARD, P., SAMPSON, J., BILLING, D., LINNANE, D. 2015. How effective is initial military-specific training in the development of physical performance of soldiers? In *The Journal of Strength & Conditioning Research,* November 2015, Volume 29, Issue 11, p S158–S162. doi: 10.1519/JSC.0000000000001066.

[6] HARMAN, E., GUTEKUNST, D., FRYKMAN, P., NINDL, B., ALEMANY, J., MELLO, R., SHARP, M.: Effects of Two Different Eight-Week Training Programs on Military Physical Performance. In *The Journal of Strength & Conditioning Research:* March 2008, Volume 22, Issue 2, p 524-534 doi: 10.1519/ JSC.0b013e31816347b6.

[7] HEINRICH, K., SPENCER,V., WALKER, N., POSTON, N.: Mission Essential Fitness: Comparison of Functional Circuit Training to Traditional Army Physical Training for Active Duty Military. In *Military Medicine*, Volume 177, Issue 10, 1 October 2012, Pages 1125–1130. Available at: https://doi.org/10.7205/ MILMED-D-12-00143.

[8] HENDL, J.: *Přehled statistických metod zpracování dat.* Praha : Portal, 2004. 584 strán. ISBN 80-7178-820-1.

[9] CHRÁSKA, M.: *Metody pedagogického výzkumu.* 1. vydanie. Praha : Grada, 2007. 262 s. ISBN 978-80-247-1369-4.

[10] KNAPIK, J. J., RIEGER, W., PALKOSKA, F., VAN CAMP, S., DARAKJY, S.: United States Army physical readiness training: rationale and evaluation of the physical training doctrine. In *The Journal of Strength & Conditioning Research:* July 2009, Volume 23, Issue 4, p 1353-1362. doi: 10.1519/JSC.0b013e318194df7.

[11] LAUREN, M., CLARK, J.: *Telo ako posilovňa.* Bratislava : TIMY PARTNERS spol. s. r. o., 2013. ISBN 978-80-89311-37-8.

[12] LITVA, D.: The influence of endurance ability on the physical development, functional Skills and motional efficiency in the special units of ground forces in the army of Slovak. In *International Congress on Soldiers´ Physical Performance* : 2005, Jyväskylä, Finland : University of Jyväskylä, 2005. S. 136. ISBN 951-25-1593-8.

[13] LINDHOLM, P., LUNDGREN, CE.: The physiology and pathophysiology of human breath-hold diving. In *Journal of Applied Physiology* 106: 284–292, 2009. First published October 30, 2008. doi:10.1152/ japplphysiol.90991.2008.

[14] MÁČEK-RADVANSKÝ, J.: *Fyziológie a klinické aspekty pohybové aktivity.* Praha : Galen, 2011. ISBN: 978-80-7262-695-3.

[15] MALMBERG, J.: Physical Fitness Tests in the Nordic Armed Forces. Oslo : The Norwegian Defence University College, 2011. ISSN 1891-8751.

[16] McAARDLE, V., KATCH, F., KATCH, V.: *Excercise Physiology. Energy, Nutrition & Human Performance.* Baltimore : Lippincott Wiliams & Wilkins, 2006. 1068 s. ISBN: 978-0-7817-4990-9.

[17] MORAVEC, R., KAMPMILLER, T., SEDLÁČEK, J. a kol.: EUROFIT: Telesný rozvoj a pohybová výkonnosť školskej populácie na Slovensku. Bratislava : Slovenská vedecká spoločnosť pre telesnú výchovu a šport, 2002. Druhé vydanie. ISBN 80-89075-11-8.

[18] PÁPAY, J. a kol.: *Optimalizácia pohybových režimov vojakov profesionálov.* Záverečná správa AGA-03-08 / Ján Pápay [et al.]. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2010. 54 s.

[19] PÁPAY, J., LITVA, D.: *Optimalizácia pohybových režimov vojakov- monitorovanie výcviku z hľadiska telesného zaťaženia*. Záverečná správa VV6 - 2011 / Ján Pápay, Dušan Litva, 1. vyd. Liptovský Mikuláš : Akadémia ozbrojených síl gen. Milana Rastislava Štefánika, 2012.

[20] PERIČ, T., DOVALIL, J.: *Sportovní tréning.* Praha : Grada publishing, 2010. ISBN 978-80-247-2118-7.

[21] ROOS, L., HOFSTETTER, M-C., MÄDER, U., WYSS, T.: Training methods and training instructors' qualification are related to recruits' fitness development during basic military training. In *The Journal of Strength & Conditioning Research,* November 2015, Volume 29, Issue 11, p S178–S186. doi: 10.1519/JSC.0000000000001106.

[22] SANTTILA, M., PIHLAINEN, K., VISKARI, J., KYRÖLÄINEN, H.: Optimal physical training during military basic training period. In *The Journal of Strength & Conditioning*

Research: November 2015, Volume 29, Issue p S154–S157. doi: 10.1519/JSC.0000000000001035.
[23] STILWELL, A.: *Cesta k vojenské zdatnosti – nároky výcviku v ozbrojených silách.* Praha : Mladá fronta, 2015. ISBN 978-80-204-3906-2.
[24] STILWELL, A.: *Přiručka speciálních jednotek psychická a fyzická odolnost.* Praha : Naše vojsko, 2005. ISBN 978-80-206-0906-9.
[25] ŠIMONEK, J.: *Modelový program rozvoja rovnováhových schopností.* Bratislava : Ševt a. s. 2013. ISBN 978-80-558-0239-8.
[26] ŠIMONEK, J.: *Model rozvoja koordinačných schopností v dlhodobej športovej príprave v športových hrách.* Bratislava : Peter Mačura – PEEM, 2009. ISBN 978-80-8113-018-2.
[27] TSATSOULINE, P.: *Nahý bojovník.* Šamorín : Vydavateľstvo Zelený kocúr, 2004. ISBN 978-80-89761-04-3.
[28] VANDERKA, M.: *Silový tréning pre výkon.* 1. vyd. Bratislava : Slovenská vedecká spoločnosť pre telesnú výchovu a šport, 2013. 270 s. ISBN 978-80-89075-40-9.
[29] VESTNÍK Ministerstva obrany Slovenskej republiky č. 100. Bratislava : Ministerstvo obrany Slovenskej republiky, 2015.
[30] VESTNÍK Ministerstva obrany Slovenskej republiky č. 54. Bratislava : Ministerstvo obrany Slovenskej republiky, 2016.
[31] Vojenský predpis o telesnej výchove a športe v rezorte ministerstva obrany Tel 1-1. Bratislava : Ministerstvo obrany Slovenskej republiky, 2001.
[32] WADE, P.: *Explozívna kalistenika*. Šamorín : Vydavateľstvo Zelený kocúr, 2015. ISBN 978-80-89761-21-0.
[33] WILMORE, J., COSTILL, D., KENNEY, W.: *Physiology of Sport and Excercise.* Champaign (USA): Human Kinetics, 2008, 574 s. ISBN 13-978-0-7360-5583-3.
[34] WOOD, R.: *Beep Test VO2max Calculator.* Topend Sports Website, 2008. Available at: https://www.topendsports.com/testing/ beepcalc. htm, Accessed 28. 09. 2018.
[35] ZATSIORSKY, V. M., KRAEMER, W. J.: *Silový trenink.* Praxe a věda. Praha : Mladá fronta, 2014. ISBN 978-80-204-3261-2.

Mgr. Roman MARKOVIČ
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: roman.markovic@aos.sk

Mgr. Roman Markovič, was born in 1989 in Kežmarok, Slovak Republic. He graduated (Mgr.) in 2012 on the Univerzity of Matej Bel in Banská Bystrica. He work at the Armed Forces Academy in Liptovský Mikuláš as assistant at the Department of Physical Education and Sport. He is a PhD. student at the Constantine the Philosopher University in Nitra, Slovak Republic

THE TERRITORIAL DEFENCE FORCES AS THE FIFTH TYPE OF THE ARMED FORCES OF THE REPUBLIC OF POLAND

(Genesis and political background of their formation as well as attitude to them among society)

Katarzyna DOJWA-TURCZYNSKA

Abstract: In 2015, political alternation at a central level took place in Poland. Conservative right-wing party Law and Justice (Polish: PiS) emerged as the winner of the parliamentary elections. A range a changes followed. One of them was establishment of the fifth type of the Armed Forced of the Republic of Poland - the Territorial Defence Forces. They are designed to aid the regular army in situations of military crises and threats.

Keywords: government; ruling; Armed Forced of the Republic of Poland; Territorial Defence Forces; public opinion.

1 INTRODUCTION

2015 saw a change of power in Poland. For the first time in history, by decision of the voters, a single party, conservative right-wing Law and Justice (PiS), took power. The first leader of the party was Lech Kaczyński, the President of the Republic of Poland who died in a plane crash near Smoleńsk in Russia (10 April 2010). The political block led by his brother, Jarosław Kaczyński, gained a strong mandate from the voters and formed an autonomous government with the ambition to implement changes in Poland. The central group in the previous government coalition was Civic Platform (Polish: PO). PiS and PO have differed and still differ with respect to the ideology and values, views on the issues of threats to the country, and perception of Poland's political alliances. The parties understood the issues of the country's security and perceived the meaning of Russia's territorial proximity in different ways. They differed in their orientation in the international policy and interpretation of Poland's membership of the European Union and NATO. These values were translated into a range of specific measures taken by the government formed as a result of the 2015 elections and had a functional implication in the area of a national security policy. A different view on the role, strength and size of the Polish army resulted in establishment of the fifth type of the Armed Forced of the Republic of Poland - the Territorial Defence Forces.

2 HISTORICAL SOLUTIONS CONNECTED WITH TERRITORIAL DEFENCE IN POLAND

In the Polish history, solutions connected with what today is called a territorial army have a rich tradition [1, p. 401]. As early as in the times of the first rulers, the Piasts, the army was made up of two components. The first was the ruler's squad - an equivalent of operational forces and professional soldiers. The second component was an army established to defend a certain territory, drawn mostly from the peasantry (or from townsfolk in towns), who were non-professional soldiers. With time (from the 11th century), the centre of gravity of the defence shifted from the duke's/king's squad to warrior knights, who settled down on a given territory and fulfilled defending functions in a situation of a conflict. Casimir III the Great's military reforms bound the "military" and "civil" components: the *pospolite ruszenie* (mass mobilisation of armed forces) was reorganised and the peasantry was obliged to defend their territory in the event of an attack [2]. The *pospolite ruszenie* functioned from the 13th to the 17th century, supporting the regular army, conducting partisan operations and defending known territories. On the day preceding the partitioning of Poland, it was written in Art. 11 of the Constitution of 3 May 1791 that "The nation has an obligation to itself to defend itself in case of aggression and to keep itself whole. Thus, all citizens are defenders of the whole and national freedoms. The army is nothing other (…)" [2, p. 322]. That declaration is vital due to the fact that Poland was a forerunner in Europe in creation of basic laws and shortly afterwards the country ceased to exist.

Territorial armies, or bottom-up initiatives of Poles under the command of experienced officers or skilful strategists turned out to play an important role over the 123 years of life under a foreign country's rule. Except for the November Uprising (1830-1831), Poles' attempts to regain independence (1846, 1848, 1863-1865) relied on irregular units of militia [2, p. 323]. Various formations of land forces, militia and partisan units were established as part of such efforts [1, p. 402]. After Poland's regaining of independence in 1918, the issue of territorial defence was raised relatively late, i.e. in the second half of the 1930s. The Territorial Defence was created based on the principle of territorial mobilisation and was drawn from people who had not been conscripted. By the year 1939, 11 brigades and semi-brigades consisting of around 50 thousand soldiers and 1600 officers were created [2, pp. 325-325]. Although those units were not designed to carry out autonomous operations, and their task was mainly to carry out short-lasting defensive actions on a given territory, their soldiers "demonstrated huge sacrifice and courage, despite significant equipment shortages" [1, 402].

After WWII, in 1959, Committee for the Defence of the Country (Polish: Komitet Obrony Kraju) was established and dissolved later as part of the reforms of armed forces after 1989. A decade from the political transformation of the 1990s, an attempt was made to create territorial defence. However, due to reduction of the Armed Forced of the Republic of Poland and financial problems, it was established in an incomplete form and ultimately - as a result of the 2008 programme of Armed Forces professionalisation - ceased to operate in its then current form [2, p. 325-328].

During the transformation period, both politicians and people from the military circles proposed concepts of a territorial army that would combined citizens' volunteer participation and patriotic posture with security challenges facing the country. As Ewa Maj pointed out, "Questions about the sense of creating a Territorial Defence system continuously appeared in discussions on the defence of Poland in 1989-2015" [3, p. 300], however for many years these postulates and assumptions, originating mainly from the political right, were hardly materialised. Among those who had long stressed the importance of a non-professional territorial army was politician Antonii Macierewicz [3, p. 303], who became Minister of National Defence in 2015. The starting point for the formation of the territorial army was diagnosis and political analysis of Poland's geopolitical situation. The Law and Justice party had a negative view of Civic Platform's policy - e.g. it criticised the reduction of the country's defence capability by abandoning the concept of building the U.S. anti-missile shield in Poland [4] and the effects of the programme to professionalise the armed forces (2008-2010). The programme foresaw a shift from conscription service to a professional army so as to improve the army's effectiveness and capability to react to various military and non-military threats [5, p. 169]. This perspective might have been correct when the Polish army conducted operations in Iraq and Afghanistan, but in the light of the 2014 Crimean Crisis not so much so... Poland's relations with Russia became tense from 10 April 2010 onwards according to the Law and Justice, whereas according to the then ruling political elites - after annexation of the Crimea. Although the solutions adopted during NATO summit in Warsaw [6] were favourable for Poland's defence, a decision was taken as part of the internal policy to strengthen the Armed Forced of the Republic of Poland, not only by increasing the defence budget, but also by creating its fifth type - a territorial army.

3 POLITICAL CLIMATE OF THE CHANGE OF POWER IN POLAND IN 2015

It is not clear what led to the alternation of power in Poland in 2015. Certainly, one of the reasons was that people were "tired" of the political elites that had ruled nonstop for eight years and the fact they held the whole power in the country (especially after 2010). A factor that affected public opinion was the exposure, despite a virtual monopoly of the mass media, of a scandal involving people in power and their camp. In June 2014, the so-called eavesdropping scandal broke out - stenographic records of illegally eavesdropped conversations of leading Civic Platform politicians, members of the government and heads of state institutions as well as businessmen were published by the "Wprost" weekly. The recordings not only exposed materialistic motivation behind the political activity of those in power and their attitude to the society and state, but they also indicated political nepotism, corrupt activities and disrespect for public funds. In terms of security institutions, the scandal is associated not only with the fact that security forces allowed conversations of people fulfilling key functions in the state (apart from the Minister of Internal Affairs, also the then Head of Central Anti-Corruption Bureau) to be recorded, but also with a spectacularly inept entry of the Internal Security Agency into the editorial office of the "Wprost" weekly and attempts to seize the evidence. The whole "raid" on a newspaper's editorial office in a democratic state was covered live by some media: both commercial TV and the relatively weak but active at that time opposition media. Not long afterwards, Civic Platform's leader Donald Tusk resigned from his position as Prime Minister of the Republic of Poland to take the position of President of the European Council as of 1 December 2014. His leaving Polish politics weakened his party, as he enjoyed great public trust. The developments on the political scene that undermined Civic Platform and the decreasing popularity of this party coincided with the 2015 migration crisis. Only at the very beginning was the attitude to refugees/migrants among Poles relatively positive. As time passed, concerns started to dominate in the Polish society [7]. It had a major practical consequence for politics, when the then Prime Minister Ewa Kopacz broke the arrangements with the The Visegrád Group and announced at Brussels willingness to accept people referred to as refugees as part of relocation [8]. In the light of terrorist attacks (24 May 2014 – Brussels; 7-9 January 2015 – Paris, 14 February 2015 – Copenhagen) [9] the issue of refugees started to be associated in social perception with a threat to the country's inhabitants. The year 2015 became a watershed in the Polish politics: in spring 2015 (24 May 2015), the incumbent President of the Republic of Poland, who had been connected with the ruling party, was replaced by a candidate recommended by Law and Justice. In autumn (25 October 2015), the Law and Justice party gained 37.58% of valid votes [10], which allowed the party led by Jarosław Kaczyński to form a government together with its electoral allies.

4 POLITICAL DECLARATIONS OF CHANGES IN MILITARY SECURITY

The parliamentary elections held in autumn 2015 resulted in Civic Platform becoming the opposition party, while the President of the Republic of Poland entrusted the mission of forming the government to Beata Szydło. In her speech, the Prime Minister referenced the plans of the new cabinet, which were based on election promises. The issue of security was strongly articulated. One of the first words of her speech were as follows: (…)

(…) I am standing in front of you in an exceptional situation. A few days ago, a terrorist attack was carried out in France. A lot of people died, and many are still fighting for their life. A drama of innocent people took place before our eyes. (...) Poles, like other Europeans, want security today. Therefore we will act in solidarity with European countries to fight terrorism. At the same time, our priority will be to ensure security to citizens of our country. I will stress it once again. For the government of the Republic of Poland, the security of Polish men and women is paramount [11].

It is important to remind here that on 13 November 2015 coordinated terrorist attacks took place in Paris for which Islamic State claimed responsibility. The terrorists held hostages at the Bataclan concert hall. Overall, 130 people were killed in the attacks with over 350 wounded [9].

The issue of broadly understood security (social, energy security, etc.) was clearly highlighted in the speech. The Prime Minister spoke about ensuring military security to the country, understood as strengthening and developing the Armed Forced of the Republic of Poland, and announced investments in the army that would also facilitate the development of the Polish economy. The aim was to strengthen the eastern flank of NATO.

5 THE INSTITUTIONAL PATH TO CREATION OF TERRITORIAL DEFENCE FORCES

The Minister of National Defence in B. Szydło's cabinet became Antonii Macierewicz, a person who was present in the Polish politics after 1989 on the right side. He had already held public office (was among other things Minister of Internal Affairs), is associated with dissolution of Military Information Services (was Minister of National Defence) and with efforts to explain the causes of the so-called Smolensk catastrophe.

On 28 October 2016, after almost a year of preparations, "Government bill amending the act on universal duty to defend the Republic of Poland and certain other acts" was submitted to the Sejm of the Republic of Poland [12]. The explanatory statement of the bill reads: "Due to the change of Poland's geopolitical and geostrategic situation, we once again face the question of security of the Republic of Poland, especially its military security." Therefore, it was proposed to create Territorial Defence Forces, which would provide a "quick, cheap and effective" way to ensure military security to the country [13]. Relatively soon (2 November 2016), the first reading of the bill took place and decision was taken to continue the procedure. The second reading took place on 15 November 2016, and a day later (16 November 2016), there was the third reading of the bill and voting. 296 of the deputies were in favour of the bill, while 170 voted against it [14]. It was backed up by all the present deputies from the Law and Justice party and the anti-establishment Kukiz15 club, independent deputies and members of the Free and Solidary (Polish: Wolni i Solidarni) party. No one from other opposition parties supported the bill, few abstained, while the vast majority of deputies from Civic Platform, Modern political party (Polish: Nowoczesna) and the Polish People's Party (Polish: Polskie Stronnictwo Ludowe) were against it. Ultimately, on 2 December 2016, the act was submitted to the President of the Republic of Poland, who signed it on 20 December 2016 [12]. The act came into force on 1 January 2017.

6 TERRITORIAL DEFENCE FORCE IN LIGHT OF NORMATIVE SOLUTIONS

The amendment of the act on universal duty to defend the Republic of Poland [15], established Territorial Defence Forces as another type of military service next to Land Forces, Air Force and Navy (Art. 3 paragraph 3), incorporating its command into the existing normative solutions (Art. 3 paragraph 4a). The commander of the Territorial Defence Forces was guaranteed a relatively strong position by the act. He is competent to command military units and organisations of the Territorial Defence Forces (Art. 11c, paragraph 1), and performs the relatively broad tasks specified in the act (Art. 11c, paragraph 2) with the help of the Command of the Territorial Defence Forces (Art. 11c, paragraph 3). The recruitment of soldiers into the Territorial Defence Forces is on a volunteer basis, and the service lasts from one year to six years (Art. 98i and 98j). The soldiers serve (art. 98i paragraph 3) in military units, in organisations of the military type and as the command (Art. 98i paragraph 2). To be able to join the service, a candidate has to meet the following conditions: hold Polish citizenship and be of age, have a physical and psychical capability to do an active military service, have no criminal record of intentional offence and have a certain level of education. In addition, a person applying for the Territorial Defence Forces cannot be assigned to alternative civilian service or do any other active military service, cannot have any emergency assignment, and cannot have any other

military service obligations in a situation of mobilisation or war (Art. 98k, paragraph 3). The act also specified preferences as to the applicants. Precedence in recruitment will be given to people: living in a certain territory, former professional soldiers, members of defence organisations and students from schools that implement defence-oriented programmes or security education programs (Art. 98k, paragraph 5).

Territorial Defence Force soldiers serve on a rotation or availability basis (Art. 98m). Service on a rotation basis means that a soldier serves in a military unit at certain dates, at least once a month for two non-working days or on other days as required by the Armed Forces, at dates agreed with the commander. Availability means that a soldier stays outside of a unit but is ready to turn up in the unit. In the case of those starting their military service "adventure," i.e. those who have not yet done an active military service and have not taken military oaths, the service in the first period is on a rotation basis and lasts 16 days. During this service, basic training and taking of the oath take place (Art. 98m, paragraph 5). Serving in the Territorial Defence Forces can make it easier for an individual to become a professional soldier, as the act contains a provision saying that people who have served in the military for three years can be conscripted into a candidate or regular service on terms applying to reserve soldiers. It is also important to mention that Territorial Defence Force soldiers have the precedence over other candidates (Art. 98n, paragraph 2).

The concept of the Territorial Defence Forces was based on the idea to incorporate new personnel into active service and thus increase its size, but it was also a response to a certain social demand. It constituted a response to modern threats and challenges to security, and was an attempt to address the specific geopolitical position of Poland, and as such its formation started with the so-called eastern wall. It was assumed that at a time of peace, the tasks of the soldiers would be to provide assistance in emergencies and disasters. The effectiveness and efficiency of the Territorial Defence Forces is to be based on its local character. Residents of a given *locus* are given precedence during recruitment, and the territorial structure of the fifth type of the armed forces of the Republic of Poland is to be adapted to the three-level administrative division of the country (with the exception of the basic level of local government - gmina). The Territorial Defence Forces are to function at the central level (command), provincial level (Territorial Defence Force brigades in each province, 2 in the Mazovia region) and poviat level (in provincial cities - battalions, in poviats - 100-strong companies of various type) [1, pp. 402-403].

7 FUNCTIONAL ASSUMPTIONS CONCERNING THE TERRITORIAL DEFENCE FORCES

The fundamental task of every state is to ensure security. State, as a political organisation of a society, should ensure its residents internal and external security. This mission is fulfilled by state authority through a range of security institutions, which at present poses a particularly difficult challenge. The emerging new armed race, antagonisms and conflicts in various parts of the world - these are only few of the problems. The 21th century brings additional threats, which are a result of the emergence of new instruments, previously unknown tools and means of fighting. Terrorism is being reborn in a new form and is directly affecting European societies. Some countries start to fear so-called hybrid warfare [16, pp. 28-29].

In this context, the Territorial Defence Forces are seen as a proposal to ensure security to Poland and its residents. Their establishment should enhance defensive security of the Republic of Poland and ensure inviolability of the country's borders. They will be mainly used in situations when the professional armed forces, due to their size and deployment, will not be able to stop the aggressor on their own and it will be necessary to wait for the allies' assistance. The Territorial Defence Forces allow two components to be combined: professional armed forces and operational forces on the one hand and a non-professional but trained army that knows a given area. Another important factor is inclusion in the country's defence of a social group previously uninterested in service or military, as well as the capability to deter a potential aggressor [1, pp. 406-407]. Knowledge of and connection with an area are important, not only in a situation of an armed conflict and attack on Poland. They are also of rudimentary importance at a time of peace and performance of non-military tasks by the Territorial Defence Forces' soldiers. The Territorial Defence Forces are planned to be mainly used to support the authorities and society in various emergencies caused by e.g. natural disasters or technical failures, and in various campaigns (rescue, humanitarian, cleaning operations) [1, p. 409]. A specific purpose of using the Territorial Defence Forces' soldiers is to promote certain postures in society (patriotic, defensive),

8 PUBLIC OPINION

Democracy is not only about alternation of power and exercising it in compliance with the law, but also about ruling that finds public acceptance. Although the actual power of citizens is manifested relatively rarely, i.e. during elections and referendums, how the public assesses the individual actions taken by politicians is important for social legitimacy of power. It is especially important in the case of the

Territorial Defence Forces, i.e. forces that have a bottom-up character. A useful tool for monitoring current social sentiment is a poll carried out by specialised centres.

The first poll that asked Poles about their attitudes to the Territorial Defence Forces was research conducted on 21-22 November 2016 [17], i.e. when the legislative works were in progress. The biggest share of those polled (43 %) declared support for the creation of these forces. Almost one fourth of the respondents (24 %) was against the idea. As much as one third of the respondents (33%) did not have an opinion on that issue, and every fifth (19%) respondent has never heard of the forces [18].

Another public opinion poll concerning the fifth type of the Polish army was carried out on 2-9 February 2017 [19]. The question about the forces was similar, the differences lying in the responses from among which the respondents could choose. The poll showed that the "Territorial Defence Forces are gaining far more supporters (49 %) than opponents (25 %) (…)" although they were not commonly known or approved. One sixth (16 %) of the respondents had an indifferent attitude to them, whereas almost one in ten (9 %) respondents did not have an opinion on that issue. Support for the Territorial Defence Forces was mostly expressed by people who were satisfied with the result of the last elections and trusted the then minister of national defence. A positive correlation was also noted between satisfaction with the formation of the Territorial Defence Forces and political party preferences (71 % of Law and Justice supporters expressed positive opinions about the formation of the Territorial Defence Forces). Shortly after the second, the third poll appeared (2-3 March 2017), showing even greater social approval of the idea of creating Territorial Defence Forces. To the question "Are the Territorial Defence Forces needed in Poland?" 58 % of the respondents responded positively, 36 % were against their formation, and only 6 % indicated the response "I don't know" [20].

On 15-17 September 2017 [21], a Polish nationwide poll was conducted asking those who were familiar with the concept of the Territorial Defence Forces two questions. The first question was about the respondents' attitude to the formation of the Territorial Defence Forces. In the question about the assessment of the formation of these forces, 43 % of the respondents assessed them positively (of those, 33 % chose the response "rather positively," whereas 10 % - "definitely positively"). The share of the opponents to the formation of the Territorial Defence Forces was noticeably lower and accounted for 23 % of the respondents (of those, 13 % selected the response "rather negatively," while 10 % assessed the decision "definitely negatively"). The second question asked the respondents whether that type of armed forces could, in their opinions, turn out crucial in a situation of a war. The respondents' responses were similar. Again, positive attitudes towards the newly-created forces dominated. The response that the Territorial Defence Forces may play an important role in the case of an armed conflict was selected by 45 % of the respondents, with 26 % expressing the opposite opinion.

Despite the fact that the polls were conducted in different periods, different research techniques were used, and the questions were formulated in different ways, it can be concluded that the supporters of the formation of the fifth type of armed forces outnumbered their opponents. The factors affecting the attitude to the Territorial Defence Forces included approval of the government and support for the governing party as well as age (the Territorial Defence Forces are mostly supported by young people) and place of living (rural areas and small towns, and so-called Eastern Poland). Both from the perspective of legitimisation of the activities taken by those in power and recruitment into the Territorial Defence Forces, this is a relatively good result.

9 CONCLUSION

After a few months, rather than years, of the existence of the Territorial Defence Forces, it is hard to assess its significance for Poland's military security - it was not the aim of this paper for that matter. The fact is that the idea of territorial forces was implemented as a political action based on a political and social diagnosis. The political diagnosis focused on identifying threats to the country and the imperative of enhancing Poland's security, whereas the social diagnosis was based on growing concerns about the national security following the annexation of the Crimea and a war Donbass (2014) [22], concerns about the internal security in the face of the migration crisis (2015) and pro-defensive attitudes among the society [23]. The politicians' diagnosis seemed to be confirmed by the sentiment of a significant portion of the society - as showed by the above-presented polls and the research commissioned by the Ministry of National Defence [24].

Currently, there is a fierce conflict on the Polish political scene between those in power and the opposition. As was mentioned earlier, it has continued for years and is based on differing axiological models. This conflict also surfaced during creation of the Territorial Defence Forces. The opponents criticised the idea and vision, the legitimacy and purpose, and were concerned about politicisation of the forces, which was reflected in public opinion [25]. It was pointed out that only a professional army can ensure security to a country, as it possesses a real combat power, is well-trained and armed with heavy equipment, which the Territorial Defence Forces lack. There were concerns about the soldiers' poor training and being armed with light

armament, which could lead to significant losses. The criticism concerned the relative autonomy of the Territorial Defence Forces and the fact that they were subordinate to the operational forces' command. Moreover, given their dispersion, difficulties in training or commanding them as part of battalions or brigades were stressed. The opponents criticised not only the effectiveness of the Territorial Defence Forces, but also the fact that the system, being built from scratch, is cost-intensive and, given the personnel shortages, may drain the command and expert personnel of the regular army [1, 410-411]. Undoubtedly, one can add to these arguments issues connected with the actual building of the units and difficulties that arise in different areas.

Currently, positive attitudes towards the Territorial Defence Forces dominate in the society. However, their actual presence among the types of the Armed Forces of the Republic of Poland will be decided by politicians, and only time will show whether the decision to form these forces was right.

References

[1] POLCIKIEWICZ, Z.: Wojska Obrony Terytorialnej w systemie bezpieczeństwa narodowego Polski. In *Acta Sciencifica Acedemiae Ostroviencis*, 2016, nr 1, pp. 399-413. ISSN 2300-1739.

[2] SOKÓŁ, W.: Wojska obrony terytorialnej w historii Polski (wybrane problemy). In *Bezpieczeństwo. Teoria i praktyka.* Kwartalnik Krakowskiej Akademii im. A. Frycza Modrzewskiego. LASOŃ, M., KALISZ, M.(*ed.)*: Wojska Obrony Terytorialnej w Polsce i na świecie w drugiej dekadzie XXI wieku, 2017, nr 3(XXVIII), p. 316-330, e-ISSN 2451-0718.

[3] MAJ, E.: Obrona terytorialna i wojska obrony terytorialnej w myśli politycznej Polski współczesnej. In *Bezpieczeństwo. Teoria i praktyka.* Kwartalnik Krakowskiej Akademii im. A. Frycza Modrzewskiego, LASOŃ, M. i KALISZ, M.(ed.): Wojska Obrony Terytorialnej w Polsce i na świecie w drugiej dekadzie XXI wieku, 2017, nr 3(XXVIII), p. 297-315, e-ISSN 2451-0718.

[4] TURCZYŃSKI, P.: *Amerykańskie koncepcje tarczy antyrakietowej w Polsce.* Warszawa : Wyd. Poltext, 2012. ISBN 978-83-7561-178-6.

[5] SWATOWSKA, A.: Próba analizy wpływu programu Profesjonalizacji Sił Zbrojnych Rzeczypospolitej Polskiej na lata 2008-2010 oraz jego wpływ na obronność państwa. In *Obronność.* Zeszyty naukowe, 2014, 1(9), pp. 168-177. ISSN 2299-2316.

[6] TURCZYŃSKI, P. (ed.): *Bezpieczeństwo europejskie po Szczycie NATO w Warszawie.* Kraków : Wyd. Libron-Filip Lohner, 2017. ISBN 978-83-65705-51-8.

[7] DOJWA-TURCZYŃSKA, K.: Stosunek Polaków do migrantów. Refleksje socjologiczne w świetle wybranych badań empirycznych. In *Rocznik Europeistyczny*, 2016, Vol. 2, pp. 61-82. ISSN 2450-274X.

[8] Klamka zapadła: rząd Ewy Kopacz zgodził się na przyjęcie islamskich imigrantów od 2016 roku. Na początek będzie ich 5 tysięcy, 23.09.2015, [online]. Wgospodarce. pl, 2015. [cit.: 2018-06-30]. Available at: http:// wgospodarce.pl/informacje/21156-klamka-zapadla-rzad-ewy-kopacz-zgodzil-sie-na-przyjecie-islamskich-imigrantow-od-2016-roku-na-poczatek-bedzie-ich-5-tysiecy.

[9] Najważniejsze zamachy terrorystyczne w Europie w ostatnich latach. Dokumentacja, 5.06.2017, [online]. Gazetaprawna. pl, 2017. [cit.: 2018-06-28]. Available at: http://www. gazetaprawna.pl/artykuly/1048402,zamachy-terrorystyczne-w-europie-w-ostatnich-latach.html

[10] Obwieszczenie Państwowej Komisji Wyborczej z dnia 27 października 2015 o wynikach wyborów do Sejmu Rzeczypospolitej Polskiej przeprowadzonych w dniu 25 Października 2015 R.. Warszawa : PKW, 2015.

[11] Exposé premier Beaty Szydło – stenogram. Warszawa : Sejm RP, 18.11.2015 [cit.: 2018-06-30]. Available at: https://www.premier. gov.pl/expose-premier-beaty-szydlo-stenogram.html.

[12] Przebieg procesu legislacyjnego, Warszawa: Sejm RP, [cit.: 2018-06-27]. Available at: http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?id=CD612509DEA7D1C9C125805A005337F7.

[13] Druk 996, [cit.: 2018-06-27]. Available at: http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=966.

[14] Głosowanie nr 60 na 30. posiedzeniu Sejmu dnia 16-11-2016 r., [cit.: 2018-06-27]. Available at: http://www.sejm.gov.pl/Sejm8.nsf/agent.xsp?symbol=glosowania&nrkadencji=8&nrposiedzenia=30&nrglosowania=60.

[15] Ustawa z dnia 16 listopada 2016 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Warszawa : Sejm PR, Dz. U. 2016 poz. 2138.

[16] MICHALAK, A.: Cele, zadania, struktura i funkcje Wojsk Obrony Terytorialnej, In: *Bezpieczeństwo. Teoria i praktyka".* Kwartalnik Krakowskiej Akademii im. A. Frycza Modrzewskiego, LASOŃ, M. i KALISZ, *M.(ed.)*: Wojska Obrony Terytorialnej w Polsce i na świecie w drugiej dekadzie XXI wieku, 2017, nr 3(XXVIII), pp. 27-36. e-ISSN 2451-0718.

[17] BARAN, V.: Polacy o Wojskach Obrony Terytorialnej: 43 proc. jest za ich utworzeniem, 24 proc. jest temu przeciwnych, 24.11.2016. [cit.: 2018-06-26]. Available at: https://wiadomosci.wp.pl/polacy-o-wojskach-obrony-terytorialnej-43-proc-jest-za-ich-utworzeniem-24-proc-jest-temu-przeciwnych-6061983968514689a.
[18] Nowy sondaż Polskiego Radia 24: Czy Polacy popierają utworzenie Wojsk Obrony Terytorialnej, 24.11.2016, [cit.: 2018-06-27]. Available at: http://www.polskieradio.pl/130/2351/Artykul/1695916,Nowy-sondaz-Polskiego-Radia-24-Czy-Polacy-popieraja-utworzenie-Wojsk-Obrony-Terytorialnej.
[19] Stosunek do Wojsk Obrony Terytorialnej. Warszawa : CBOS, Nr 27/2017, marzec 2017. ISSN 2353-5822.
[20] KOZUBAL, M.: Entuzjazm dla Wojsk Obrony Terytorialnej, 8.03.2017, [cit.: 2018-06-27]. Available at: http://www.rp.pl/Sluzby-mundurowe/303089886-Entuzjazm-dla-Wojsk-Obrony-Terytorialnej.html 20]
[21] Sondaż: *Kto jest zadowolony z utworzenia WOT?* 20.09.2017, [cit.: 2018-06-27]. Available at: http://www.rp.pl/Sluzby-mundurowe/170929905-Sondaz-Kto-jest-zadowolony-z-utworzenia-WOT.html
[22] DOJWA-TURCZYŃSKA, K.: Poles' Sense of Security - Selected Sociological Aspects. In *Science and Military*, No 1, Vol. 10, 2015, s. 49-55, ISSN 1336-8885.
[23] KOZUBAL, M.: *Sondaż: Polacy nie boją się wojny.* 7.11.2016, [cit.: 2018-06-25]. Available at: http://www.rp.pl/Spoleczenstwo/311069938-Sondaz-Polacy-nie-boja-sie-wojny.html.
[24] *Polacy za rozbudową armii. Wyniki sondażu CBOS*. 14.08.2017, [cit.: 2018-06-25]. Available at: https://www.defence24.pl/polacy-za-rozbudowa-armii-wyniki-sondazu-cbos.
[25] DOJWA-TURCZYŃSKA, K., WOLSKA-ZOGATA, I.: Wojska Obrony Terytorialnej w opiniach internautów. Wybrane zagadnienia, wystąpienie na Kongresie Bezpieczeństwa, Toruń 6-8.12.2016.

dr hab. Katarzyna DOJWA-TURCZYSKA, PhD.
University of Wroclaw
Str. Koszarowa 3
51-149 Wroclaw
Poland
E-mail: k_dojwa@uni.wroc.pl
katarzyna.dojwa-turczynska@uwr.edu.pl

dr hab. Katarzyna Dowa-Turczyńska, PhD. - with „habilitation"of Social Sciences in the field of sociology (specialisation: sociology of the army). She completed studies in the field of Political Science (1999) and Sociology (2000) at the Faculty of Social Sciences of the University of Wrocław, and later defended her doctoral dissertation at the Institute of Sociology (sociology of politics). Since 2006, she has been working in the Department of Sociology at the University of Wrocław; currently she is Head of the Section of Public Sphere Sociology. Main areas of interest: sociology of the army, sociology of security and sociology of politics, as well as the issues of image building and PR of public institutions.