SCIENCE & MILITARY

No 2 | Volume 14 | 2019

Dear readers,

...another year is over and it is time to look back on what we have done and present our plans for the future.

At present, a scientific journal is not only an irreplaceable information channel in scientific communication. Its social and scientific significance is reflected in knowledge application and further scientific research and development. Publishing papers in journals is an important part of scientific and research work as it has an enormous impact on acquisition and deepening of knowledge. One of its pragmatic reasons is promotion of ongoing scientific research. Publishing in scientific papers is an essential part of doctoral studies and a chance for senior researchers to enhance their prestige in the scientific world.

New trends in scientific publishing are connected with new models that are emerging in scientific communication and publishing. They are influenced especially by the digital science tools, open access to scientific information and the Open Science concept as such. The Open Access and Open Science concepts are also backed by the European Union. Most European publishers of scientific journals are planning to publish open access papers within the Horizon 2020 framework programme. Advances in information technologies also lead to development of new means of dissemination and long-term storage of scientific information, including, for example, institutional repositories for digital preservation of scientific knowledge or social networks as means of distributing scientific publications.

The editorial board of the Science & Military journal still has the same long-term plan, which is to continuously improve its quality and make it accessible to the wider scientific community. Identity and quality of our journal (like those of any journal) are determined and developed by the editorial board, authors, reviewers and last but not least you, dear readers.

In September 2019, the new Decree No. 244/2019 Coll. on the System of Academic Disciplines of the Slovak Republic came into effect. The systematization of the fields of study led to definition of a new academic discipline No. 24 called Defence and Military Science, which presents a complex field focused on military-related monitoring, research and education. In this regard, I would like to invite all the academic staff and doctoral students to publish the results of their research work in this field in the Science & Military journal.

Besides requirements regarding continuous improvement of the journal's quality in terms of its content and specialisation, we have set a demanding goal for the upcoming years, which is to increase the journal's impact factor by indexing Science & Military into the SCOPUS database and the journals indexed for the Current Contents Connect (ISI).

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 article titled **"An Overview of Hash Functions Based on Neural Networks"** was written by Ján Astaloš, Miloš Očkay and Radoslav Forgáč. The authors of this paper point out the use of neural networks for hashing. On the other hand, they draw the attenton to the lack of independent cryptoanalysis that would confirm the safety of the neural network approaches.*

*The second article among the reviewed articles, which was written by Pavol Lukášik and Miroslav Marko and titled **"Preventive Diagnostics of the Common Rail Fuel System Injectors",** deals with the current condition of the fuel system, its issues and recommendations for further operations. Fuel and electronic systems of the compression-ignition engines belong to the highest failure rates group and to the most economically demanding items in modern vehicles. From this viewpoint, they deserve a greater attention in order to prevent break downs, failures and their premature wear.*

*The following article titled **"Possibilities of Implementation of Friendly Units' Manoeuvre in the Common Operational Picture"** by Jan Nohel, Zdeněk Flasar and Petr Stodola describes the possibilities of the use of information sharing on the network of computer workstations when planning the manoeuvre routes of a group of cooperating units with the task to attack the same target in a military operation.*

*Another article titled **"Use of Data Mining for Network Behaviour Analysis of Selected Operating Systems"** was written by Július Baráth. The aim of this paper is to use data mining techniques to obtain characteristic behaviour patterns of operating systems with a focus on the communication observed by a remote observer. Network communication of selected operating systems is observed, and the list of contacted targets is recorded.*

*Among the articles in this issue, you can find the article written by Jakub Vilímek titled **"Small Unmanned Aerial Vehicles – Threats and Defence against Them"**. The article discusses current small UAVs (Unmanned Aerial Vehicles) threats and ways of defence against them. The goal of the article is to define vital questions, which have to be answered before designing any UAV protection system.*

*The author Marek Hargaš wrote the article **"Cooperation between the EU and the USA in their Policy Towards Russia"**. The article is focused on the legislative and institutional background of the mutual cooperation between the EU and the USA within their policy framework towards Russia.*

Dear readers, I believe that this year's editions of the Science & Military journal provided you with the topics you were interested in. Let me wish you and your dear ones a very Merry Christmas and success in achieving your personal and professional goals in the upcoming new year.

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

Reviewers

Assoc. Prof. Dipl. Eng. Ľubomír **DEDERA**, PhD.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš, SK
Assoc. Prof. Dipl. Eng. Peter **FIEDLER**, Ph.D.	Brno University of Technology, CZ
Lt. Col. Assoc. Prof. Dipl. Eng. Petr **HRŮZA**, Ph.D.	University of Defence Brno, CZ
Col. Prof. Klára SIPOS **KECSKEMÉTHY**, PhD.	National University of Public Service, Budapest, HU
Prof. PhDr. Ján **KOPER**, PhD.	Matej Bel University in Banská Bystrica, SK
Assoc. Prof. Dipl. Eng. Miroslav **KRÁTKÝ**, Ph.D.	University of Defence Brno, CZ
Prof. Dipl. Eng. Ján **KURTY**, PhD.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš, SK
Assoc. Prof. RNDr. Milan **LEHOTSKÝ**, CSc.	Catholic University in Ružomberok, SK
Assoc. Prof. Dipl. Eng. Ľuboš **MAGDOLEN**, PhD.	Slovak University of Technology in Bratislava, SK
Assoc. Prof. RNDr. Martin **STANEK**, PhD.	Comenius University in Bratislava, SK
Prof. Dip. Eng. Jozef **ŠTULRAJTER**, CSc.	Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš, SK

AN OVERVIEW OF HASH FUNCTIONS BASED ON NEURAL NETWORKS

Ján ASTALOŠ, Miloš OČKAY, Radoslav FORGÁČ

Abstract: Increasing availability of hardware solutions for calculation of hash functions and the evolution of quantum computers bring the demand for strong cryptographic hash functions, resistant to brute-force attacks. One of the possible approaches is to utilize the properties of neural networks to construct hash functions. The authors of this paper point out the use of neural networks for hashing. On the other hand, they draw the attention to the lack of independent cryptanalysis that would confirm the safety of the neural network approaches.

Keywords: Hash function; Neural network; Chaotic maps; Cryptanalysis; Cryptography; Digital signature.

1 INTRODUCTION

There are basically two main methods usually used for electronic data authentication: digital signature and hash-based message authentication code (HMAC) [18].

A digital signature creates fixed-length bit string (otherwise called digital fingerprint or hash) by using cryptographic hash function and subsequent digital signing of the hash using a cryptographic key. The digital signature is typically distributed along with the original file. To verify the file's authenticity, it is necessary to know the hash function, the verification function of the digital signature and the verification key. In order to verify the authenticity of the signer, digital signature uses asymmetric encryption with the private key and the public key pair. The private key is used to create the signature. The public key is used for the authentication. Hash and signature verification functions are usually made public. In practice, the public key is digitally signed by a trusted certification authority.

The hash-based message authentication code is calculated using a cryptographic hash function in combination with a secret key. Similarly to digital signature, HMAC can be used to verify the data integrity and authenticity. However, it does not offer the possibility to verify the sender's identity because it uses symmetric key. It is mainly used for the exchange of messages. The secret key needs to be delivered securely to the recipient of the message in advance.

Cryptographic hash functions are algorithms that calculate hash from data with arbitrary length [1]. Hash is usually smaller and therefore, there are certainly two different inputs that give the same output. This is called collision of hash function. The ideal cryptographic hash function should meet the following key features:

- It is deterministic, which means that it always gives the same output for the same input.
- Its calculation is fast enough for input data of any length.
- It is practically impossible to generate an input giving a specific output.
- Small change in the input data should change the output so much that it cannot be observed by any relation with the original output.
- It is not feasible to find two different inputs with the same output.

Hash functions used in cryptography are constantly evolving. The functions that have been considered safe for a long time (for example MD5 or SHA1) were proven to be insufficient. At the time of writing this paper the hash functions that are considered safe are for example:

- Secure Hashing Algorithm (SHA-2, SHA-3) [14].
- RACE Integrity Primitives Evaluation Message Digest (RIPEMD) [15].
- BLAKE2 [16].

In 2007, the National Institute of Standards and Technologies in the USA (NIST) announced the competition for a new hash function SHA-3, which would complement the older SHA-1 and SHA-2 functions. The winning algorithm is a subset of a group of cryptographic functions Keccak. It is based on the "sponge" principle. For the subject of this paper it is important to note that none of the 51 candidates was based on neural networks.

Increasing availability of hardware solutions to calculate hash functions (such as Application-Specific Integrated Circuit ASIC) also increases the need for strong cryptographic hash functions resistant to brute force attacks. Another threat to cryptographic hash functions are quantum computers. Although the sufficiently large quantum computer for breaking SHA-256 (SHA-2 with 256 bit output) is currently not available, in the relatively near future it could be constructed. This caused formation of a new cryptography branch dealing with cryptographic functions resistant to attack by quantum computers – post quantum cryptography. The cryptographic function is considered quantum safe, if the quantum algorithm that would reduce the computational complexity of the function calculation is not known.

2 NEURAL NETWORK BASED HASH FUNCTIONS

The features of neural networks like confusion, diffusion and compression were utilized in the design of encryption algorithms. Stream and block ciphers are good examples [5]. In addition, neural networks also exhibit the features of one-way functions. If a neuron has multiple inputs and only one output, it is fairly difficult to retrieve input data from the known output. Compression function is given by the fact that the number of neurons in output layer is smaller than the number of neurons in the input layer.

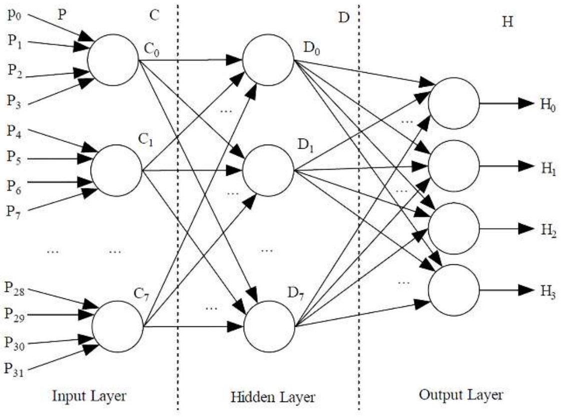


Fig. 1 Three layers neural network [5]

The first attempts to use neural networks for hash functions started in 1998 [2] with cellular networks. In 2002 there were experiments with using perceptron networks [3]. The origin of chaos based hash functions also belongs to the same period. The interesting feature of a deterministic chaotic system is that it can generate a sequence of pseudorandom numbers based on the input key, while the sequences generated with different input keys also differ. However, the same key always generates the identical sequence so it can be used to generate parameters of the neural network. Thus the chaotic systems and neural networks form a good pair for the construction of the strong hash functions [4].

Figure 2 shows the hash function based on a neural network with three layers and a chaotic map.

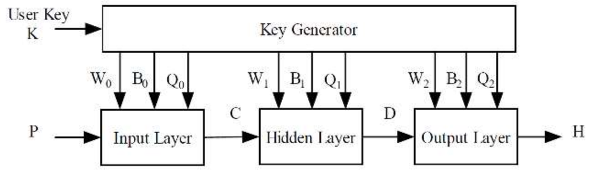


Fig. 2 Hash function proposed in [5]

Key generator creates weights W_i, biases of neurons B_i and control parameters for the chaotic map Q_i based on the encryption key. Chaotic map is used as a transfer function. The transfer function uses at least 50 iterations in an input and output layer. Extension to multi-block mode is shown in Figure 3.

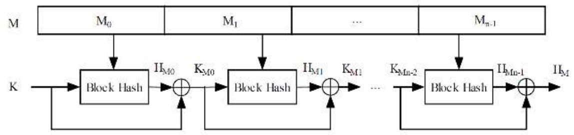


Fig. 3 Multi-block hash mode [5]

Transfer function iterations and the block pipeline prevent the effective parallelization. Figure 4 shows the algorithm modified for parallel processing.

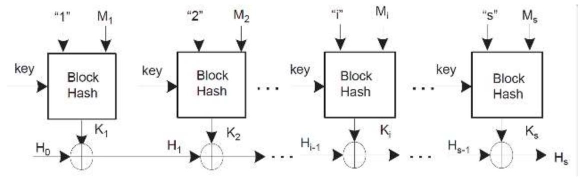


Fig. 4 Modified parallel algorithm [7]

The key feature is to separate the calculation of block hashes K_i and the combination of hashes to final hash H_S so that the computationally complex generation of block hashes can be done in parallel. In contrast with the three-layer neural network approach, the neural network in this example has only two layers. Piecewise linear chaotic map (PWLCM) is used as a transfer function.

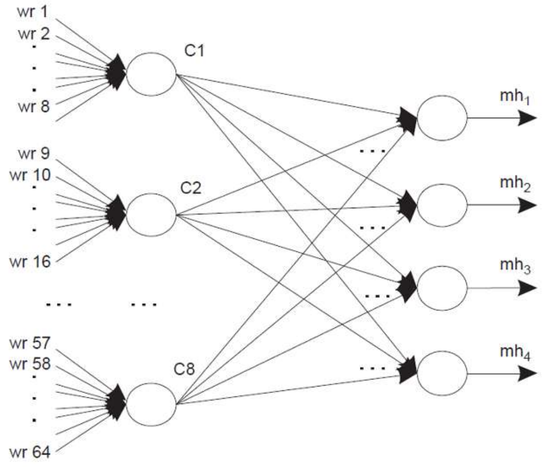


Fig. 5 Chaotic neural network structure of the block hash function [7]

Chaotic system can also be used to generate parameters of neural network [8] (Fig. 5). This approach uses 4D one-way coupled map lattices (OWCML) in conjunction with the chaotic tent map (CTM) (Fig. 6).

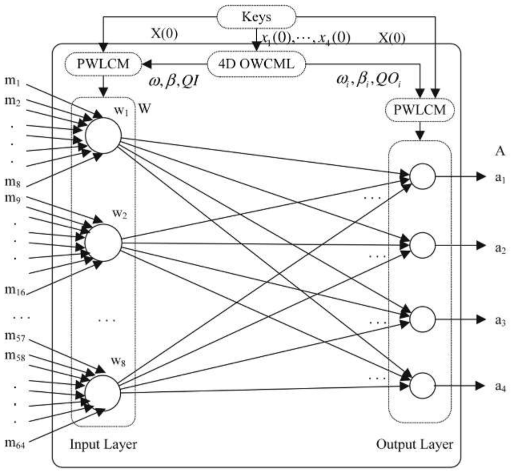


Fig. 6 OWCML in conjunction with CTM [8]

Another approach uses cellular neural network (CNN) [2]. In contrast with the multi-layer perceptron model, in this case the neurons form an interconnected cellular grid (Fig. 7). A possibility to use Field-programmable gate array (FPGA) for implementation is a primary advantage of this approach. Hash function in this case is based on Cartesian authentication code proposed by B. den Boer [17]. It has been implemented using CNN Universal Machine.

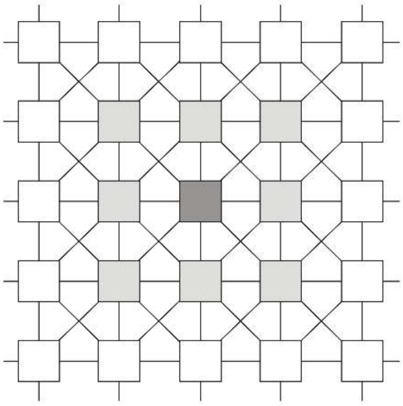


Fig. 7 Cellular neural network scheme [6, 8]

The combination of cellular neural networks and chaotic systems were also studied [6, 8]. Yang's solution is based on generating of chaotic sequence by iterating of cellular neural network by Runge-Kutta algorithm followed by iterating of chaotic sequence with the input message. According to the authors, chaotic sequence generated by basic chaotic systems may include loops and simple neural networks may not be robust enough against the attacks.

The combination of both approaches called Hyper-chaotic cellular neural network (HCCNN) (Fig. 8) shows a strong diffusion stability over solutions based solely on chaotic systems.

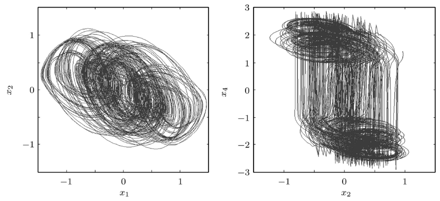


Fig. 8 Phase portraits of the HCCNN [6]

Parallel solution of hash function based on chaotic CNN is proposed in [12]. The input message is expanded by iterating the chaotic logistics map and then divided into 512-bit blocks, which are processed in parallel. The blocks are divided into 32-bit numbers, which are used as an input to a 4-dimensional chaotic "cat" map. By iterating the map, we get inputs into a 4-dimensional cellular neural network (4-D CNN), that displays chaotic dynamics (Fig. 9).

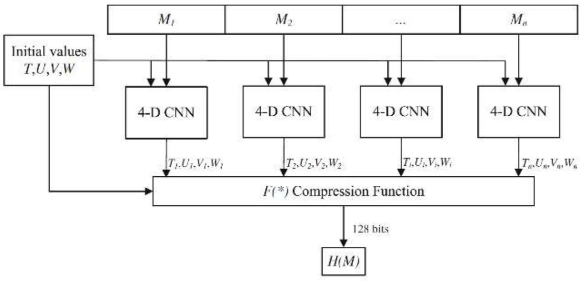


Fig. 9 Structure of the parallel Hash algorithm [12]

Another approach uses a recurrent neural network (RNN) [10]. Unlike the classic forward model, this solution utilizes RNN's ability to memorize the previous state of neurons as well as link the network output to the input. Neural network parameters (synapses weights, biases) form a secret key that must be safely transmitted to the recipient of the message (Fig. 10). This solution has only been experimentally verified on text messages. To use it for the verification of authenticity of image data, it will be necessary to perform its cryptanalysis.

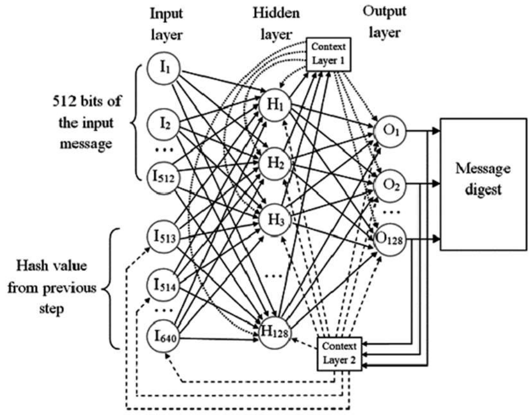
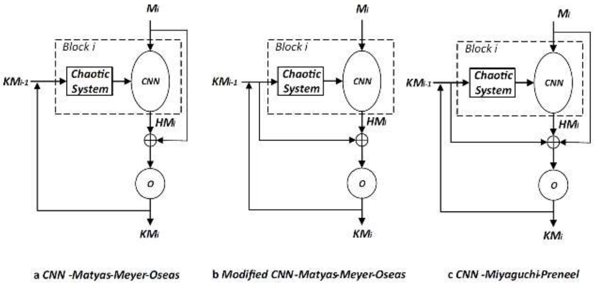


Fig. 10 The structure of the recurrent neural network for hash function generation [10]

Two hash functions based on chaotic neural networks using Merkle-Dåmgard (MD) construction (Fig. 11) with three output schemes (CNN-Matyas-Meyer-Oseas, Modified CNN-Matyas-Meyer-Oseas and CNN-Miyaguchi-Preneel) were proposed in [11].



a CNN -Matyas-Meyer-Oseas b Modified CNN-Matyas-Meyer-Oseas c CNN -Miyaguchi-Preneel

Fig. 11 The Merkle–Dåmgard compression functions proposed in [11]

The first function is created using a two-layer chaotic neural network and the second function is created using a single-layer network and non-linear functions (Fig.12).

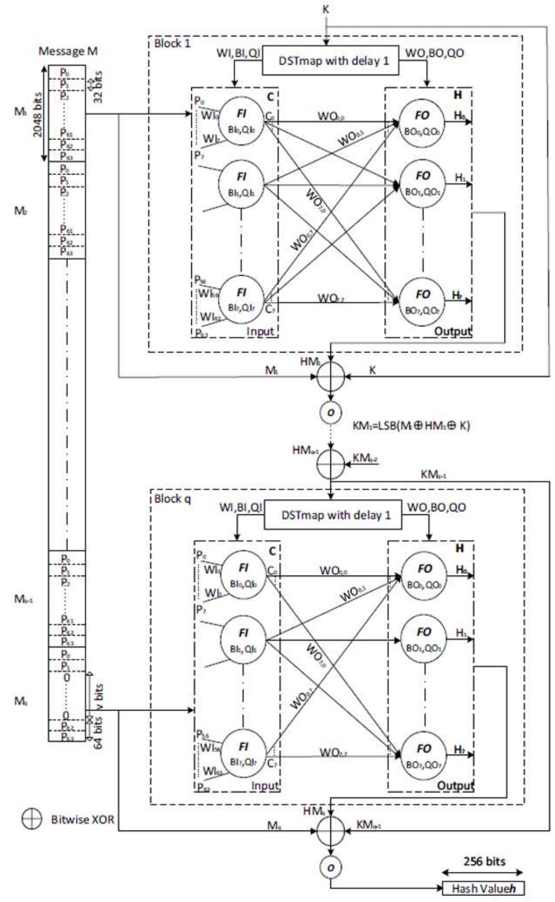


Fig. 12 Keyed hash function based on two-layer CNN with MP output scheme [11]

Neurons use a chaotic activation function based on the "Discrete Skew Tent" map (DSTmap) and the Discrete Piecewise Linear Chaotic Map (DPWLCmap) (Fig. 13).

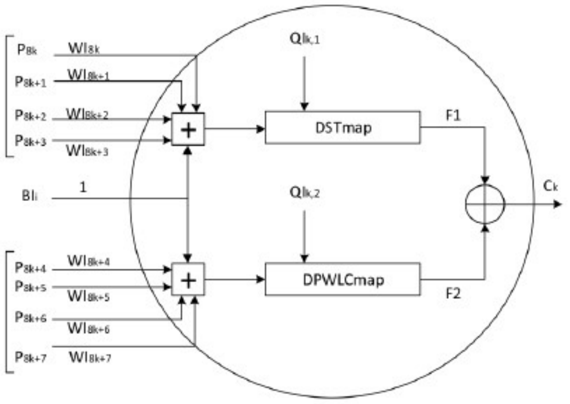


Fig. 13 Detailed structure of the neuron in an input layer of the two hash functions proposed in [11]

3 CRYPTANALYSIS OF HASH FUNCTIONS

Although the authors of hash functions often claim that their functions meet the requirements of cryptographic hash functions, in many cases it has been proven by cryptanalytic methods that this is not the case. The cryptanalysis of hash functions analyzes:

- Simplicity of calculation – how complex the calculation of the hash function is.
- Preimage resistance - the complexity of finding a message for a given hash.
- Second preimage resistance - the difficulty to find the second message with the same hash as the given message.
- Collision resistance - how difficult it is to find two different messages with the same hash.

Several works have been devoted to cryptanalysis of hash functions based on neural networks. For example, [9] analyzed the parallel hash function from [7], and there were identified three problems. The first problem is that the hash function only works if there is a number of blocks in a message greater than or equals to two. The authors propose to solve this problem by changing the calculation parameters for a chaotic map. The second problem is a large set of weak keys which need to be excluded. The third problem is poor resistance against the forgery attack. The authors proposed a modification that will increase the resistance of the original algorithm (Fig. 14).

The important parameter for comparing the cryptographic hash functions is their computational complexity. It is specified in computing cycles per byte (cpb) and it is usually different for different size of input data. It also depends on CPU type, compiler and compiler options used. Although the authors of hash functions sometimes compare their hash functions with other hash functions in the terms of computational complexity, if they don’t publish the source code and the conditions under which the measured values have been achieved, it is difficult to verify their results. Nevertheless, the published results [11] show that hash functions based on neural networks are generally more computationally complex than standard hash functions (e.g. SHA2-256).

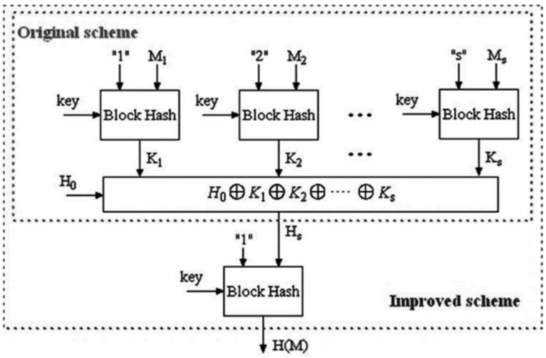


Fig. 14 Modified parallel hash function [9]

Another approach to improving the parallel hash function from [7] is using two-layer chaotic neural network with 4 neurons in its input and output layers (Fig. 15) as a hash mixer [13].

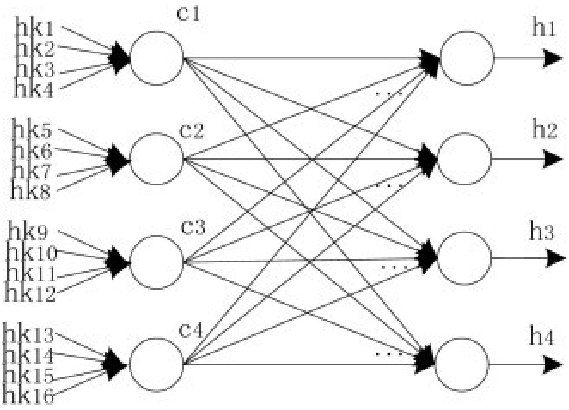


Fig. 15 Two-layer chaotic neural network used as hash mixer [13]

4 CONCLUSION

Cryptographic hash functions have been and still are the subject of an intensive research. The use of neural networks is mostly combined with the use of chaotic systems to increase the confusion of the resulting algorithm. In some cases, multiple chaotic systems are used at the same time to increase the complexity of the hash algorithms. Although the authors present their hash functions as safe, cryptanalysis in some cases revealed serious shortcomings. The source code unavailability also makes it difficult to verify the performance parameters presented by the authors.

Neural networks based cryptographic functions are an interesting research topic and new solutions will be surely proposed in the future. However, for real world deployment it is recommended to use only the hash functions that have undergone cryptanalysis and their implementation was a subject of security audits and intensive testing.

5 ACKNOWLEDGMENT

This work was supported by Slovak Scientific Grant Agency VEGA No. 2/0167/16.

References

[1] MENEZES, A. J., VANSTONE, S. A., VAN OORSCHOT, P. C.: *Handbook of applied cryptology.* Boca Raton : CRC Press, 1997. 810 p. ISBN 978-0429466335.

[2] CSAPODI, M., VANDEWALLE, J., ROSKA, T.: High speed calculation of cryptographic hash functions by CNN chips. In: *1998 Fifth IEEE International Workshop on Cellular Neural Networks and their Applications*. Proceedings (Cat. No. 98TH8359). London : IEEE, 1998. p. 186-191. ISBN 978-0780348684.

[3] YEE, L. P., SILVA, L. C. D.: Application of Multi-layer Perception Network as One-way Hash Function. In: *Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks 2.* IEEE, 2002. ISBN 0-7695-0619-4.

[4] XIAO, D., LIAO., XL.: A combined hash and encryption scheme by chaotic neural network. In: *International Symposium on Neural Networks.* Berlin, Heidelberg : Springer, 2004. p. 633-638.

[5] LIAN, S., SUN, J., WANG, Z.: *One-way hash function based on neural network.* New York : Cornell University, 2007.

[6] YANG, Q. T., GAO, T. G.: One-way hash function based on hyper-chaotic cellular neural network. In: *Chinese Physics B,* Volume 17 Number 7, OP Publishing Ltd, 2008.

[7] XIAO, D., LIAO, X., WANG, Y.: Parallel keyed hash function construction based on chaotic neural network. In: *Neurocomputing 2009*, Volume 72, Issue 10-12, 2288-2296 p.

[8] LI, Y., DENG, S., XIAO, D.: A novel Hash algorithm construction based on chaotic neural network. In: *Neural Computing and Applications.* Volume 20, ISSUE 1, 2011, 133-141 p.

[9] WANG, X., GUO, W., ZHANG, W., KHAN, M. K., ALGATHBAR, K.: Cryptanalysis and improvement on a parallel keyed hash function based on chaotic neural network. In:

Elecommunication Systems, Volume 52, Issue 2, 2011, 515-524 p.

[10] TURČANÍK, M.: Using recurrent neural network for hash function generation. In: *2017 International Conference on Applied Electronics,* Pilsen, 2017. ISBN 978-1-5090-5622-4.

[11] ABDOUN, N., EL ASSAD, S., DEFORGES, O., ASSAF, R., KHALIL, M.: Design and security analysis of two robust keyed hash functions based on chaotic neural networks. In: *Journal of Ambient Intelligence and Humanized Computing*, Springer Berlin Heidelberg, 2019. 1-25 p. ISSN 1868-5137.

[12] LI, Y., DENG, X., HUAQING, L., SHAOJIANG, D.: Parallel chaotic Hash function construction based on cellular neural network. In: *Neural Computing & Applic*, 2012, DOI 10.1007/s00521-011-0726-z.

[13] HUANG, Z.: *A more secure parallel keyed hash function based on chaotic neural network. Communications in Nonlinear Science and Numerical Simulation*. In: Volume 16, Issue 8, August 2011, 3245-3256 p.

[14] DAHAL, R. K., BHATTA, J., DHAMALAL, N. T.: *Performance Analysis of SHA-2 and SHA-3 Finalists.* In: *International Journal on Cryptography and Information Security (IJCIS),* Vol. 3, No. 3, September 2013. ISSN: 1839-8626.

[15] DOBBERTIN, H., BOSSELAERS, A., PRENEEL, B.: *RIPEMD-160Blake2*. September 2019. Available at: https://homes.esat.kuleuven.be/~bosselae/ripemd160.html

[16] AUMASSON, J. P.: *Blake 2*. September 2019. Available at: https://blake2.net

[17] BOER, D. B.: A simple and key-economical unconditional authentication scheme. In: *Journal of Computer Security 2,* 1993, 65-71 p. ISSN: 0926-227X.

[18] KRAWCZYK, H., BELLARE, H., M., CANETTI, R.: HMAC: *Keyed-Hashing for Message Authentication.* 2014. Available at: https://tools.ietf. org/pdf/rfc2104.pdf.

Dipl. Eng. Ján **ASTALOŠ**
Institute of Informatics
Slovak Academy of Sciences
Dúbravská cesta 9
845 07 Bratislava 45
Slovak Republic
E-mail: jan.astalos@savba.sk

Dipl. Eng. Miloš **OČKAY**, PhD.
Department of Informatics
Armed Forces Academy of general M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: milos.ockay@aos.sk

Dipl. Eng. Radoslav **FORGÁČ**, PhD.
Institute of Informatics
Slovak Academy of Sciences
Dúbravská cesta 9
845 07 Bratislava 45
Slovak Republic
E-mail: radoslav.forgac@savba.sk

Ján **ASTALOŠ** works as a researcher-developer at Institute of Informatics, Slovak Academy of Sciences. He received his MSc. degree in software engineering from the Faculty of Electrical Engineering and Informatics, Slovak Technical University in Bratislava in 1995. Main areas of his research are HPC, Grid and Cloud computing, adapting of computationally intensive applications to HPC including GPGPU accelerators and optimization of HPC applications.

Miloš **OČKAY** is an assistant professor at the Department of Informatics at the Armed Forces Academy in Liptovský Mikuláš. In 2003, he graduated (MSc.) at Military Academy in Liptovský Mikuláš as a civil student. He holds PhD. degree in the field of Informatics, received in 2012 from the Technical University of Košice. His scientific research focuses on parallel computing, computer graphics and steganography.

Radoslav **FORGÁČ** is a member of Department of parallel and distributed information processing at Institute of Informatics Slovak, Academy of Sciences. He holds PhD. degree in the field of Artificial Intelligence, received in 2006 from the Technical University of Košice. The focus of his research is aimed at neural networks for image and text processing. He is the author of the Optimized Model of Pulse Coupled Neural Network which was applied in the image recognition and recently also in the image steganography.

PREVENTIVE DIAGNOSTICS OF THE COMMON RAIL FUEL SYSTEM INJECTORS

Pavol LUKÁŠIK, Miroslav MARKO

Abstract: Fuel system and electronic systems of the compression-ignition engines belong to the highest failure rates group and to the most economically demanding items in modern vehicles. From this viewpoint they deserve a greater attention in order to prevent break downs, failures and their premature wear. Modern diagnostic tools provide us lots of essential information about current system condition via electronic control units. This issue also relates to company vehicle - Citroën Jumpy 2.0 HDi (Common Rail), which has been used for more than 12 years by Department of Mechanical Engineering (Armed Forces Academy of general Milan Rastislav Štefánik, Liptovský Mikuláš, Demänová). It is recommended to run the diagnostics of the fuel system and its regular monitoring in spite of low mileage (45 500 km). This article deals with actual condition of the fuel system, its issues and recommendations for further operation.

Keywords: Compression-ignition engine; Common Rail; Injector; Nozzle; Diagnostics; Fuel additive.

1 INTRODUCTION

Common Rail is a direct diesel injection system with high pressure fuel rail and electronically controlled valves for compression-ignition engine. The system was first introduced into production series in 1997. The system is thanks to its advantages being used by most of the manufacturers today [1].

The high-pressure fuel rail accumulates fuel under high pressure ratios. At the same time, it absorbs oscillation of the fuel pressure via stored fuel, which is caused by its transportation and the injection itself. The fuel rail is shared among all the cylinders and the fuel pressure is maintained at the constant level (± 2 %) despite high output demands. This way the pressure remains constant. The fuel injected into cylinder is dispersed better into small particles and therefore makes a more flammable mixture. The electronic valve control enables better management of the moment, duration of the valve open phase and it enables to split the amount of the fuel required for one cycle into a number of doses. Therefore, a higher efficiency and torque is achieved. A lower fuel consumption, sound level and emissions are a non-negligible advantage [1]. As a disadvantage we can mention a complex injection system. To achieve constant pressure in the system a specific power must be maintained, resulting in loss of overall engine efficiency. In case of damaged injection valve (jammed or clogged) there is a chance of constant fuel leak into the combustion chamber. Additional securing of the system is not possible. Depending on the type of the "constant fuel leak fault", there is a chance of engine failure in short time. The injectors are prone to clog overtime. Therefore, the system is very susceptible to fuel purity and quality [1].

2 INJECTORS CARBONIZATION ISSUE

During the process of diesel combustion, a carbon deposits build up (carbonization) occurs in the surrounding of the injectors and in the openings itself in the combustion chamber. The deposits have a negative impact on engine efficiency resulting in lowered fuel flow, change of the fuel injection direction – emission deterioration, increased fuel consumption and damaging the engine. The carbon deposits build up can be relatively suppressed using the right detergent additives, that are added during the diesel production process or they can be bought on the market and added from time to time by user [2].

Certain portion of the deposits build up in the combustion chamber and the injectors have, except the impurities and operating factors (such as driving at low engine speeds and short distance vehicle runs), also biocomponents (fatty acid methyl esters – FAME), which are fuel manufacturers obliged to add into the diesel in order to reduce emissions in accordance to EU legislation. Content of the FAME biocomponents in the diesel can be at the level of up to 7 % in volumes. There are currently no announced major changes in the diesel quality. Tightening of some quality requirements may occur, especially those affecting injection system. Especially vehicles manufacturers in "Worldwide Fuel charter" require the tightening of the lowering impurities content, increased cetane number and lubricity requirements [3].

An example of damaged piston is shown in Figure 1 as a result of defective fuel dispersion caused by polluted injector nozzles. Polluted nozzles cause sharp uneven jet of the fuel shown in Figure 2, that may cause melting off of the piston material and consequently damaging the engine.

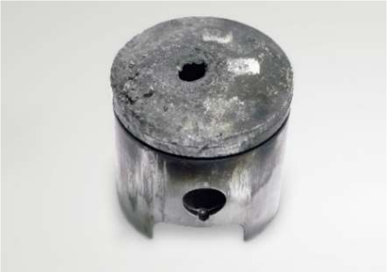


Fig. 1 Damaged piston (illustrative photograph) Source: [11].

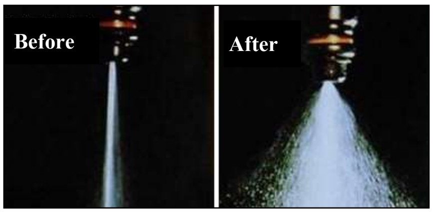


Fig. 2 Injector operation before and after the use of additive (illustrative photograph)
Source: [7].

Injection Common Rail fuel systems operate most of the time in the pressure range between 180 Mpa and 250 MPa. Generally, for compression-ignition engines (without the high-pressure fuel rail) with high range of engine operating speeds, the pressure of injections are correlated to the engine speeds – the higher engine speeds, the higher pressure of injection. It is a result of increased speed of the fuel flow through the injection nozzle. The fuel jet coming out of the injection nozzle reaches speeds of exceeding 400 m/s and disperses – the fuel jet disintegrates into numerous very small drops in form of a mist [4].

$$\overline{d}_{32} = \frac{\sum \pi \cdot n_i \cdot \frac{d_i^{\,3}}{6}}{\sum \pi \cdot n_i \cdot d_i^{\,2}}$$

$$\overline{d}_{32} = \frac{1}{6} \cdot \frac{\sum n_i \cdot d_i^{\,3}}{\sum n_i \cdot d_i^{\,2}} \qquad (1)$$

$\overline{d}_{32}$ – *middle size of drop parameter*
n_i – *engine speed*
d_i – *nozzle diameter*

In terms of creating a mixture, the $\overline{d}_{32}$ - middle size of drop parameter is the most significant parameter. This parameter is characterized by mathematical equation (1). This value depends most on the pressure of the injection and also on nozzle outlet hole diameter. Degree of dispersion – middle size of drop parameter $\overline{d}_{32}$ has a crucial role in adjustment of the fuel pre-injection. Clogging of the injector outlet holes therefore has a huge impact on the fuel dispersion starting with pre-injection up to the full injection dose during the operating cycle [4].

Fuel injection volume is characterized by mathematical equation (2) described by total duration of injection (in time) depending on the nozzle design, nozzle outlet hole area and indicated injection speed [5].

$$V_{pal} = \int_0^{\tau_d} \mu \cdot S_{Tr} \cdot w_{Tr} \cdot d_{\tau} \qquad (2)$$

V_{pal} – *fuel injection volume*
w_{Tr} – *injection speed*
S_{Tr} – *nozzle hole area*
τ_d – *duration of injection*
μ – *nozzle parameter*

It is apparent from the equation (2), that any flow restriction caused by carbon deposits has, except defective fuel dispersion, an impact on lowered fuel supply of the injector into the combustion chamber. In this case the insufficient fuel supply of the injector must be compensated by the other injectors. Such as forced fuel compensation by the Engine Control Unit (ECU) is undesirable in the long run in terms of uneven engine load, as well as in terms of its durability. The uneven fuel supply between injectors should not exceed 15 % while the engine is operating.

2.1 Experiment and fuel system additive testing

One of the most common avoidable issue among the injectors is burned carbon on the nozzle tip. Well established method of regaining operational condition of the injector is use of ultrasound technology with decarbonizing liquid. There is no mechanical damage of the nozzle thanks to this technology, therefore the nozzle tip is not scratched.

A chemical treatment is recommended first in case the injectors do not show a high rate of carbonization – an application of prescribed fuel system additive. We decided to test commercially available German brand additive P2101 CRDSC (Fig. 5). Two prescribed doses were added to the Citroën Jumpy fuel tank during the monitoring.

The vehicle (Fig. 4) made 1649 km during this period mostly on highway roads in Slovak and Czech Republic. From the first measurements it is slightly deteriorated (probably as a result of the additive cleaning processes), in comparison to the baseline condition. Gradually the results were better and the fuel supply differences between the injectors were compensated. (Fig. 6, 7).

However the last measurement showed a slight deterioration, which was attributed to the extremely demanding vehicle operation and overheating of the engine on purpose of purging at high engine speeds (more than 4000 rpm) during the last measurement on the Demänová – Liptovský Hrádok route (probably as a result of the additive cleaning processes).

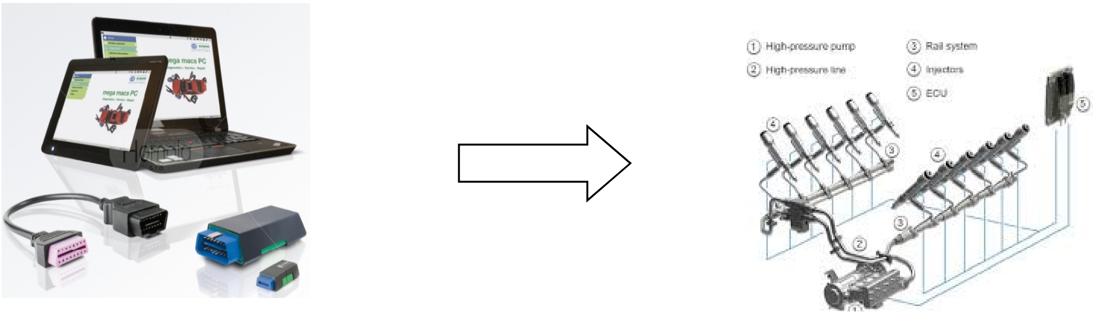
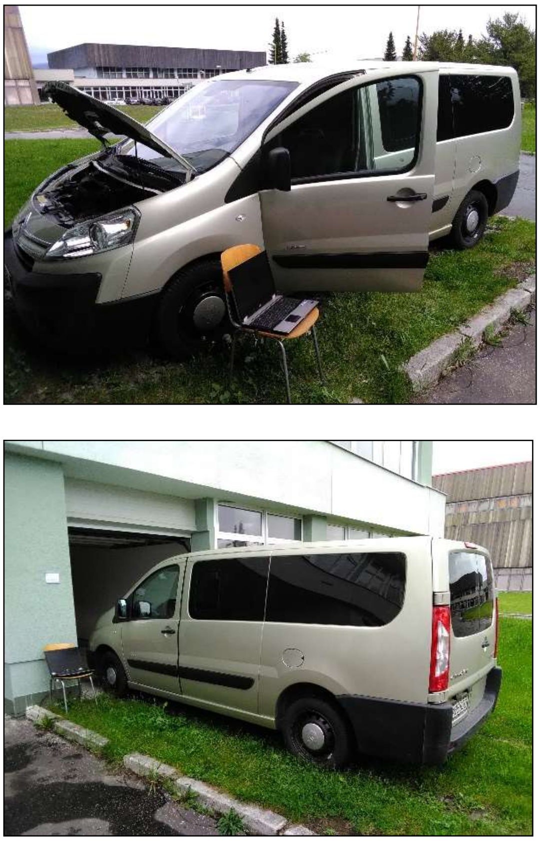


Fig. 3 Diagnostic kit Hella Gutmann Mega Macs PC
Source: [10].

Company car tested (Armed Forces Academy of General M. R. Štefánik, Department of Mechanical Engineering, Demänová): Citroën Jumpy 2.0 HDi



Engine 2.0 HDi specification:

- Power (kW): **88 kW**
- Horsepower: **120 hp**
- Horsepower: **118 bhp**
- Rev. at Max Power: **4000/min**
- Torque: **300 Nm**
- Torque (lb-ft): **221 lb-ft**
- Rev. at Max Torque: **2000/min**
- Displacement: **2 l**
- Displacement: **1997 cc**
- Number of Cylinders: **4**
- Number of Valves per Cylinder: **4**
- Bore: **85 mm**
- Stroke: **88 mm**
- Compression Ratio: **17.6 :1**
- Common Rail Diesel System

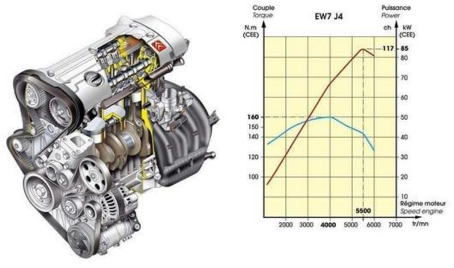


Fig. 4 Monitored vehicle Citroën Jumpy 2.0 HDi
Source: authors.

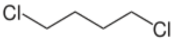
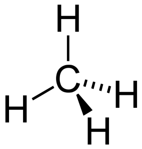
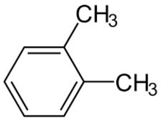
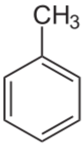
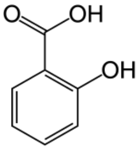
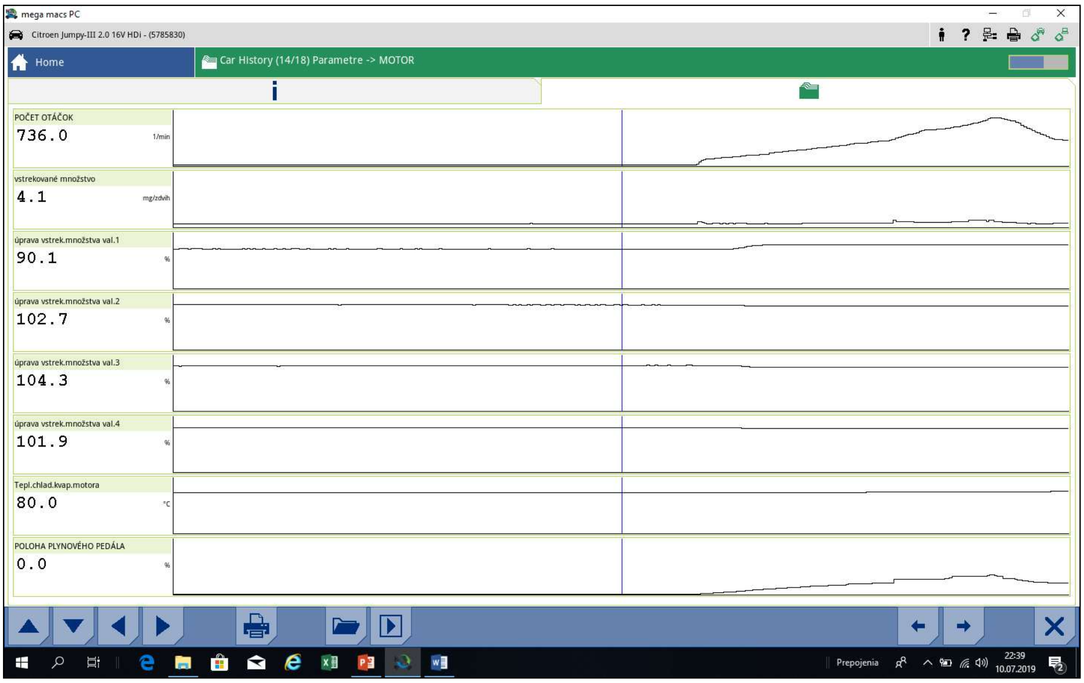
Diesel additive tested: P2101 CRDSC - Common Rail Diesel System Clean and Protect (the content of the individual constituents in the additive)		
	Chloroalkanes are UVCB substances (Substances of Unknown or Variable Composition) with varying chlorine contents (up to around 70 % by weight) and carbon chain lengths (between C10 and C13). They are yellowish oily liquids, runny or thick, without a distinct melting point, but undergo a process of thickening at temperatures below 35 °C.	
	N-alkanes in organic chemistry, an alkane, or paraffin (a historical name that also has other meanings), is an acyclic saturated hydrocarbon. In other words, an alkane consists of hydrogen and carbon atoms arranged in a tree structure in which all the carbon–carbon bonds are single.	
	Xylene is a clear, colorless and highly volatile mixture of xylene isomers with a characteristic odor. Its toxicity is much less compared to benzene. Xylene is flammable at room temperature; therefore, it constitutes a fire hazard. It is insoluble in water but mixes readily with many organic solvents.	
	Toluene is a clear, colorless, water-insoluble and highly volatile liquid with a characteristic sweet and pungent odor. It is an irritant to the eyes, skin, nose and lungs. Toluene is a dangerous fire hazard and can lead to flashback due to its heavy vapor. It is an aromatic hydrocarbon that is widely used as an industrial feedstock and as a solvent.	
	Phenols in organic chemistry, phenols, sometimes called phenolics, are a class of chemical compounds consisting of a hydroxyl group (— OH) bonded directly to an aromatic hydrocarbon group. Phenolic compounds are classified as simple phenols or polyphenols based on the number of phenol units in the molecule.	

Fig. 5 Tested additive P2101 CRDSC
Source: authors.

Table 1 Measured vehicle´s operation intervals and injector´s output after route

Monitored vehicle operation					**Quantity injected fuel**			
Date	Vehicle route	Initial state (km)	end state (km)	Total sum (km)	Injector No. 1 (%)	Injector No. 2 (%)	Injector No. 3 (%)	Injector No. 4 (%)
13.05.2019	AFA Demänová area	45 522	45 522	0	90.1	102.7	104.3	101.9
14.05.2019	AFA Demänová – Bratislava – AFA Demänová	45 522	46 124	602	90.9	104.3	103.5	101.1
23.05.2019	AFA Demänová – Nitra – AFA Demänová	46 124	46 508	384	87.0	106.6	103.5	102.7
29.05.2019	AFA Demänová – Brno – AFA Demänvá	46 508	47 127	619	87.9	105.9	103.0	103.2
18.06.2019	AFA Demänová – L. Mikuláš – AFA Demänová	47 127	47 140	13	94.9	105.0	100.3	98.8
27.06.2019	AFA Demänová – L. Hrádok – AFA Demänová	47 140	47 171	31	90.9	107.4	105.5	97.2

Source: authors.



mega macs PC

Citroen Jumpy-III 2.0 16V HDi - (5785830)

Home

Car History (14/18) Parametre -> MOTOR

POČET OTÁČOK 736.0 1/min

vstrekované množstvo 4.1 mg/zdvih

úprava vstrek.množstva val.1 90.1 %

úprava vstrek.množstva val.2 102.7 %

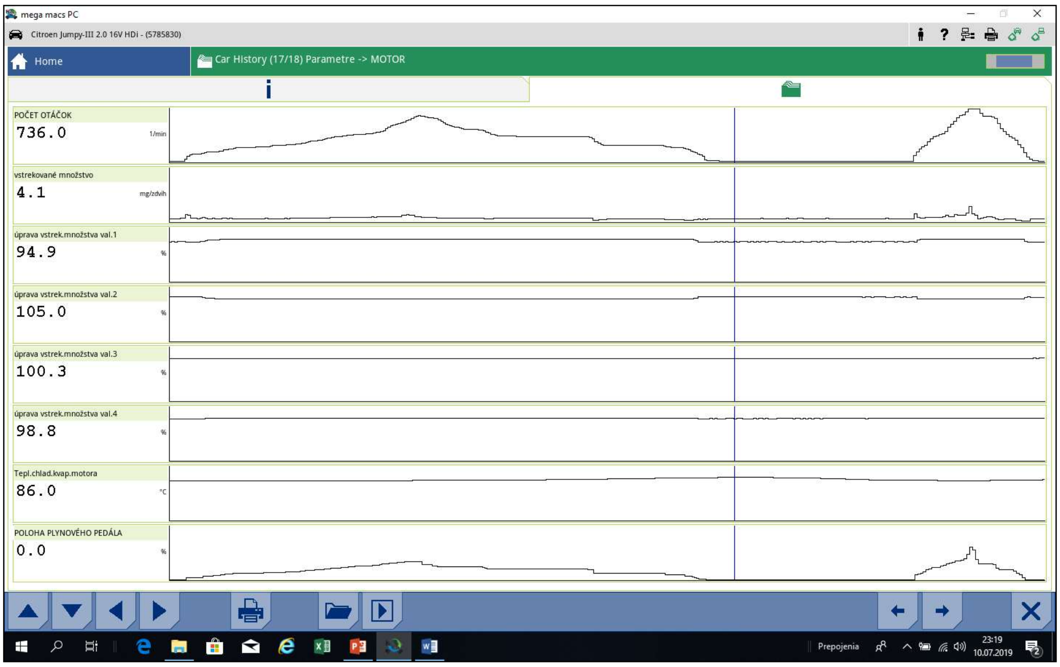
úprava vstrek.množstva val.3 104.3 %

úprava vstrek.množstva val.4 101.9 %

Tepl.chlad.kvap.motora 80.0 °C

POLOHA PLYNOVÉHO PEDÁLA 0.0 %

Fig. 6 Uneven fuel supply of the injectors at idling engine speed - before use of the cleaning additive P2101 CRDSC 13.05.2019 (total distance traveled: 45 522 km)
Source: authors.



mega macs PC

Citroen Jumpy-III 2.0 16V HDi - (5785830)

Home

Car History (17/18) Parametre -> MOTOR

POČET OTÁČOK 736.0 1/min

vstrekované množstvo 4.1 mg/zdvih

úprava vstrek.množstva val.1 94.9 %

úprava vstrek.množstva val.2 105.0 %

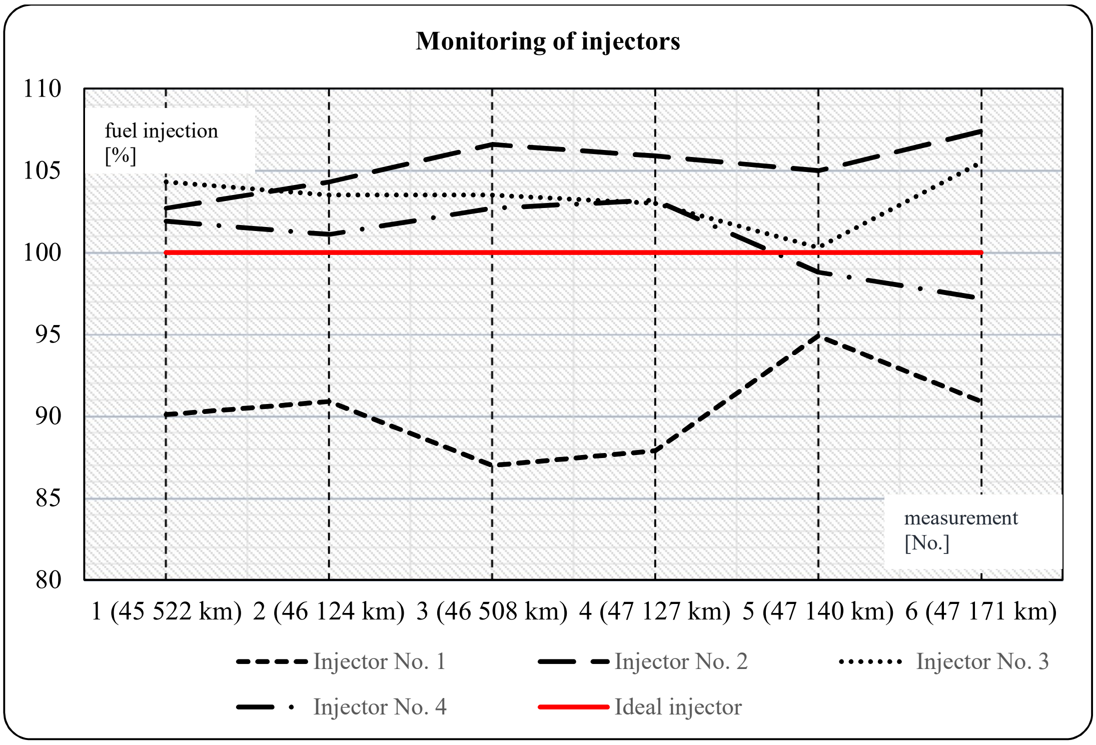
úprava vstrek.množstva val.3 100.3 %

úprava vstrek.množstva val.4 98.8 %

Tepl.chlad.kvap.motora 86.0 °C

POLOHA PLYNOVÉHO PEDÁLA 0.0 %

Fig. 7 Fuel supply of the injectors compensation at idling engine speeds after use of the cleaning additive P2101 CRDSC 18.06.2019 after 1618 km (total distance traveled: 47 140 km)
Source: authors.



Graph 1 Monitoring of the injectors output during the vehicle operation (graphical interpretation Tab. 1)
Source: authors.

The vehicle Citroën Jumpy 2.0 HDi did not show any signs of fuel system failure, nor any significant rough engine operation (vibrations, hesitation, knocking, excessive noise, etc.). Only a slight uneven engine operation was notable at idling engine speed as well as slight hesitation while vehicle acceleration through gears (0 – 1 – 2 – 3).

The highest uneven fuel distribution between the injectors was found while the fuel system was diagnosed at idling engine speed (736 rpm) – from 90 % up to 105 % level, which is close to 15 % threshold. The highest abnormality in a long term showed injector No. 1, which the fuel supply output was as low as 87 % (Tab 1). The higher engine speeds, the balanced fuel distribution was and at the 1500 rpm to 1600 rpm all injectors achieved the same fuel supply level of 100 %. It is important to point out the fact, that all measurements were performed in neutral gear and the engine was at operating temperature of at least 80° C (Graph 1).

3 CONCLUSION

It is only allowed to fuel company vehicles with base 51 cetane diesel – "Diesel Tempo Plus" and it is prohibited to fuel high-grade 55 cetane diesel – "EVO Diesel" in The Armed Forces of the Slovak Republic. Therefore, logistics of the Slovak Armed Forces should provide dosing of the cleaning additive into fuel systems of the vehicles equipped with Common Rail technology when performing major maintenance. The monitoring of the company vehicle demonstrated, that even an engine with total distance traveled of only 45 500 km (in 12 years) has marks of polluted fuel injectors. From a pragmatic view it is not beneficial to save on fuel – financial expenses for the cleaning additive (10 000 km) are 20 € while replacement of the injectors can climb up to 2 000 €.

True conclusions can be drawn only after a long-term monitoring (approx. 1 year or a distance traveled of at least 10 000 km), any conclusions drown right know are hasty. But we can conclude over this short period, that the chemical additive application into the fuel system was mainly a positive change of the fuel injectors output. Preventive diagnostics and additivities of the fuel system has shown as reasonable solution. Every user of the vehicle (especially with Common Rail system) should pay attention to its fuel system.

References

[1] GÁL, L.: *Elektronické možnosti zvyšovania výkonu vznetového spaľovacieho motora.* Bratislava : STU, 2011. FEI-5386-51388.

[2] MARKO. M., MARCHEVKA. M., BOLECH, V.: *Bull-13-4 - Bulletin č. 4 Skladovanie, preprava a vlastnosti vybraných druhov palív.* Trenčín : ÚLZ OS SR, 2015.

[3] TŘEBICKÝ, V.: *Paliva pro moderní motory.* Mazání v moderním průmyslovém podniku, 13.

Mezinárodní Česko – Slovenská konference 25. - 27. dubna 2018. Praha : Czech Mechanical Engineering Society, 2018. ISBN 978-80-02-027850.

[4] BEROUN. S.: *Vozidlové motory.* Studijní texty k předmětu „Motorová vozidla". Liberec : TU, 2002.

[5] TRNKA. J., URBAN. J.: *Spaľovacie motory.* Bratislava : Alfa, 1992. ISBN 80-05-01081-8.

[6] *Diagnostika CR vstrekovačov naftových motorov* [Electronic resource]. Available at: https: //www. engineering. sk/ strojarstvo-extra/ 3636-diagnostika-cr-vstrekovacov-naftovych-motorov.

[7] *Jazdi lacno s BOOGIE ENERGY PILL* [Electronic resource]. Available at: https://jazdilacno.webnode.sk/ako-to-funguje/ ozdravna-kura/.

[8] *Citroën JUMPY. Príručka na údržbu, obsluhu a záruky.* Creation 4D Concept Automobiles Citroën – RCS Paris 642050199, Imp. en U. E. 06/09, ENT-SQ-9006/2, 2006.

[9] Citroën JUMPY. *Návod na obsluhu*, Creátion 4D Concept Automobiles Citroën – RCS Paris 642050199 – Edition ALTAVIA/ PRODITY, Imp. en U. E. 06/09, G9VU – SQ – 2006.

[10] Hella – Gutmann Mega Macs PC, Stručná úvodní příručka, H-G Solutions GMBH 2015, QSMMPCV47CZ0215SO.

[11] MS Moto service [Electronic resource]. Available at: http: /twitter.com/ msmotorservice/status/680455858938114049

Dipl. Eng. Pavol **LUKÁŠIK**
Armed Forces Academy of General M. R. Štefánik
Department of Mechanical Engineering
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: pavol.lukasik@aos.sk

Dipl. Eng. Miroslav **MARKO**, PhD.
Armed Forces Academy of General M. R. Štefánik
Department of Mechanical Engineering
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: miroslav.marko@aos.sk

Pavol **LUKÁŠIK** - was born in Liptovský Mikuláš, Slovakia in 1980. He received his Master Degree (Dipl. Eng.) at the Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš in 2004. He started his dissertation studies in 2017, his research interests are focused on tribology and diagnostic. Currently he is working as an assistant professor at the Department of Mechanical Engineering, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš.

Miroslav **MARKO** - was born in Myjava, Slovakia in 1954. He received his Master Degree (Dipl. Eng.) at the VVŠ PV Vyškov in 1978. In 2004 he successfully finished his dissertation studies in tribology. From 1993 he is working as an assistant professor and special assistant at the Department of Mechanical Engineering, Armed Forces Academy of General M. R. Štefánik in Liptovský Mikuláš. He is member of board of Slovak Society for Tribology and Tribotechnics (SSTT).

POSSIBILITIES OF IMPLEMENTATION OF FRIENDLY UNITS´ MANEUVER IN THE COMMON OPERATIONAL PICTURE

Jan NOHEL, Zdeněk FLASAR, Petr STODOLA

Abstract: The article describes the possibilities of the use of information sharing on the network of computer workstations when planning the maneuver routes of a group of cooperating units with the task to attack the same target in a military operation. The key factor for gaining operational superiority over the enemy in this situation is a rapid and accurate processing of all relevant information about the overall battlefield situation. The appropriate solution to this problem is the use of the MCS CZ software, which calculates the optimal maneuver route of the unit based on intelligence information.

Keywords: Information; Situation awareness; Networking; Passability; Maneuver.

1 INTRODUCTION

Detailed and up-to-date situation awareness is a prerequisite for taking qualified decisions by each commander in a military operation. It represents a thought process, in which the commander is well versed in all available relevant information related to the tactical situation on the battlefield. The successful accomplishment of the units´ task is influenced particularly by the activity of the enemy, the terrain features, the effects of the civilian environment, as well as the activity of friendly units in the operation. The geographical factors of the movement in the terrain or the movement using the communication over land in a military operation is described in more detail in [1, 2]. We know the intention and activities of friendly units but we have to collect the information about the activity of the enemy, the influence of the area of operations and the local population. However, the key to the operational superiority over the enemy is the speed of appropriate response and the action of friendly units, depending on the change in the situation on the battlefield. The speed mentioned is based on gathering the real-time information. Then, the speed of information processing into a format for immediate use, and the subsequent speed of orientation and implementation of its outputs to the command and control process on the battlefield are equally important.

The Common Operational Picture (COP), which summarizes and characterizes all the important information from the area of operation on the terrain layout, is a fast orientation tool for the commander. The structure and the content of the COP and its importance for creating situation awareness on the battlefield are described in [3-5]. In a digitized battlefield environment, the COP has the form of a virtual image of a real battlefield processed and displayed on computer workstations. Its function is provided by the C4ISR systems (Command, Control, Communication and Computers, Intelligence, Surveillance and Reconnaissance). The data in the C4ISR systems can be processed in a raster form divided into thematic areas. Their cumulative effect on the activities of friendly forces and equipment can be expressed using the evaluation criteria and mathematical algorithms of map algebra. The mathematical combination of evaluation criteria related to the effects of individual information areas will generate a continuous effect of the tactical situation on the activities of friendly forces and equipment. On the basis of this analysis, it is then possible to effectively plan the maneuver of friendly units. Complications and the time delay can occur when coordinating a maneuver of a group of units that perform the tasks with the same goal. Modeling and simulating the movement of forces and equipment in the environment of the 21st century battlefield is further dealt with in [6]. The possibilities of information processing in the environment of networked computer workstations for the purpose of taking decisions are described in [7].

2 MANEUVER CONTROL SYSTEM CZ

The Maneuver Control System CZ (MCS CZ) has been developed at the Department of Intelligence Support at the University of Defense of the Czech Republic. It is based on the optimal movement route model, implemented in the TDSS (Tactical Decision Support System), which continuously evaluates the information layers of the effects of the ground surface, relief, weather, enemy activity and the possibilities to support friendly forces and equipment for the passability of the operation area, see Fig. 1. The result of the model calculations is the Cost surface, on the basis of which the MCS CZ creates routes for maneuvers, see [8].

Currently, the MCS CZ offers four types of maneuver to the user – commander. These are the envelopment and the attack by fire at the enemy, described in more detail in [9], and then the frontal attack and the turning movement. The maneuver element itself can be selected from the database of all the entities of friendly forces and equipment in the considered area of operation just as the target enemy element. All four offensive maneuvers are derived from the model of the optimal maneuver route. Their course is thus guided along a clear and safe route.

3 SHARED MANEUVER CALCULATIONS OF THE MCS CZ

The simulated presentations of the possibilities of using the MCS CZ are shown through a simulated attack of the first-line companies of a motorized battalion on the enemy units that take up the defense in the urban area. It has the form of a small town with a population of approximately 2,900 inhabitants. The reconnaissance devices of friendly forces have identified the position of three rifle platoons of the enemy infantry company. The battalion commander and his staff have conducted a shortened planning process using the MCS CZ, the result of which is the maneuver routes of the frontal attack of three first-line companies. The town will be attacked from three directions; the width of the battalion zone of attack will be 2 to 4 kilometers. The MCS CZ has calculated the spatial design of the passable route through the terrain, safe from the viewpoint of the enemy's operation and supplemented by the calculated time to cover it.

Time is an important coordinating factor when performing a multiple maneuver of the group of units. In order to successfully attack the enemy in an urban area, it is necessary to start the advance to the target area at the same time. The routes of all three first-line companies are calculated on the basis of the evaluation of the time demand to cover the area, affected by the weather, the activities of the enemy and the friendly forces and equipment. Therefore, the MCS CZ calculations provide a qualified estimate of the total time to cover the created route of maneuver to the objective. Thus, the battalion commander will be able to estimate the approach time of individual companies to the town and to adjust their maneuver and speed.

The nature of the terrain, in which the maneuver routes of all three companies have been calculated, is very similar. The relief is moderate, with an altitude of 500 to 650 meters above sea level. The ground surface has the character of fields and meadows, with irregular areas of coniferous and deciduous forest. On the maneuver route of the 1st company, there is approximately a 600-meter wide stretch of continuous forest that will have to be overcome. The length and time to cover individual routes are shown in Table 1.

In this case, the times to cover the three maneuver routes of all three companies differ in the range of 2 minutes and 43 seconds. Such a time difference can be adjusted by a mere acceleration or deceleration of individual companies in the simpler sections of the movement. By summarizing the maneuver routes of individual companies, the battalion commander will gain an overview of their passability in the terrain and the time for covering, shown in Fig. 2.

Table 1 Maneuver of the first-line companies

Unit	Distance of maneuver	Time of passing	Position in formation
1st motorized company	4,048 meters	20:34	West flank
2nd motorized company	4,233 meters	23:17	Center
3rd motorized company	3,784 meters	22:44	East flank

Source: author.

The variable speeds on the individual types of terrain are a key and variable characteristic for the route calculation; they are defined in the underlying digital model of the territory. Their specific values are dependent on the nature of the terrain, the technical condition of military equipment, the health condition and morale of the infantry units, the availability of fuel and the experience of the commanders. The most important factor influencing the passability of the maneuver route and the speed of the movement is the presence and abilities of the enemy. The movement speeds indicated in Fig. 3 have been selected for the above-mentioned tactical situation. Their values make provision for the tactical and technical parameters of motorized units´ vehicles, the tactical movement in the broken terrain and the active presence of the enemy.

In an environment of the digitized battlefield and the network of computer workstations, the maneuver routes of all companies (units) of the battalion are shared with all authorized users (commanders) using the COP. In this way, situation awareness on the battlefield in the area of the friendly units´ activities is fulfilled. Using the MCS CZ and the data connection on a computer station network, the maneuver routes for subordinate units (stations) can be created and the planned maneuver routes can be accepted.

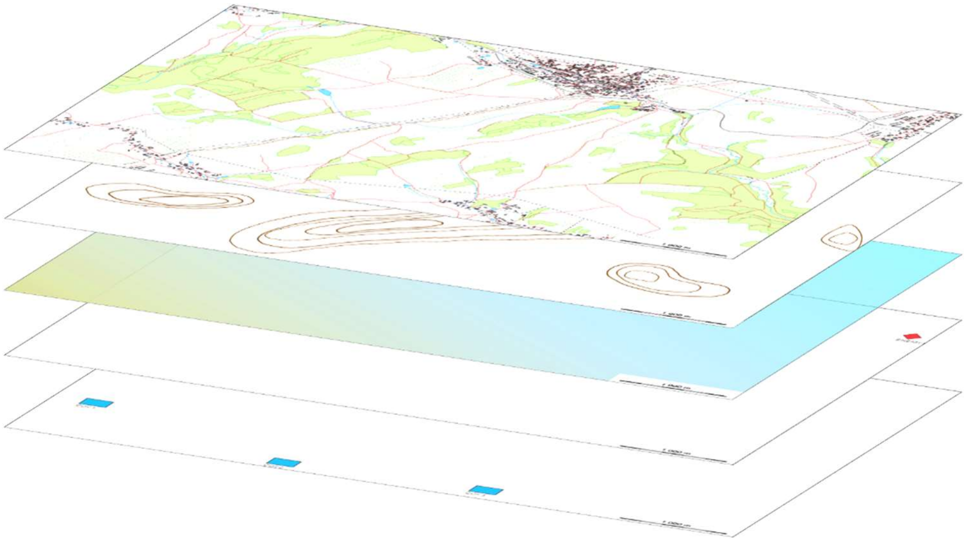


Fig. 1 Information layers
Source: author.

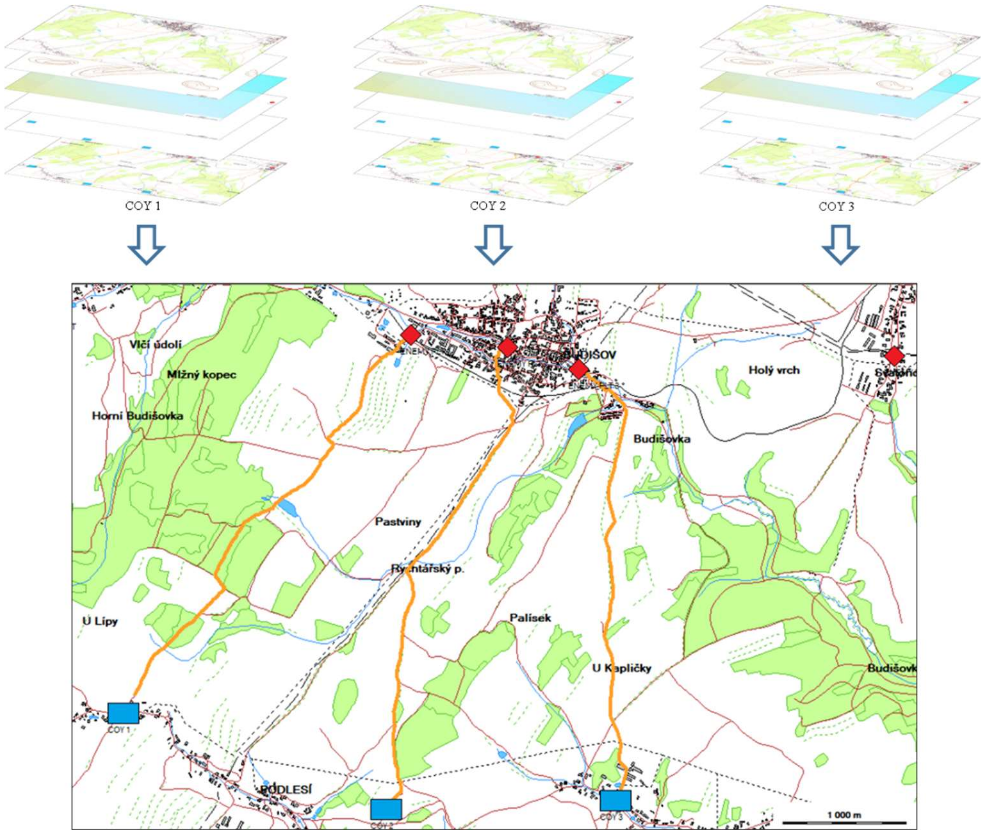
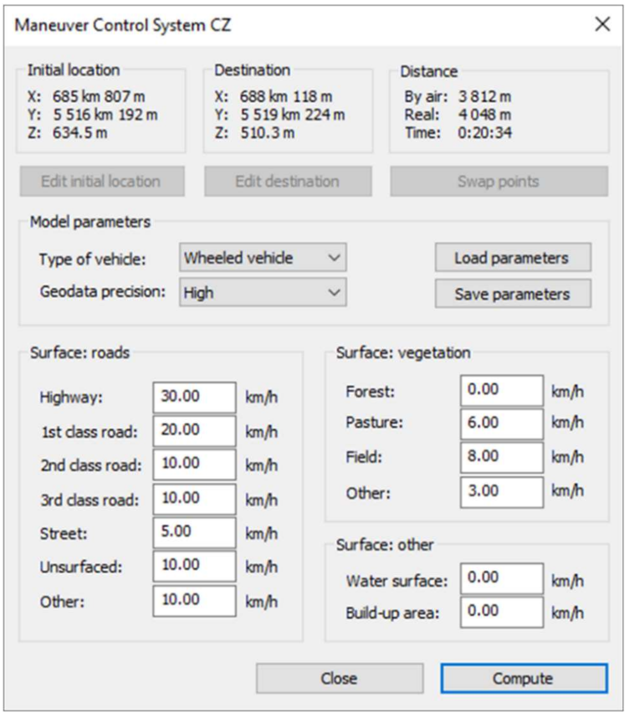


Fig. 2 The COP of the battalion commander
Source: author.


Maneuver Control System CZ

Initial location
X: 685 km 807 m
Y: 5 516 km 192 m
Z: 634.5 m

Destination
X: 688 km 118 m
Y: 5 519 km 224 m
Z: 510.3 m

Distance
By air: 3 812 m
Real: 4 048 m
Time: 0:20:34

Model parameters
Type of vehicle: Wheeled vehicle
Geodata precision: High

Surface: roads		
Highway:	30.00	km/h
1st class road:	20.00	km/h
2nd class road:	10.00	km/h
3rd class road:	10.00	km/h
Street:	5.00	km/h
Unsurfaced:	10.00	km/h
Other:	10.00	km/h

Surface: vegetation		
Forest:	0.00	km/h
Pasture:	6.00	km/h
Field:	8.00	km/h
Other:	3.00	km/h

Surface: other		
Water surface:	0.00	km/h
Build-up area:	0.00	km/h

Fig. 3 Variable speeds
Source: author.

4 SHARING A MANEUVER ROUTE ON A COMPUTER NETWORK

The resulting maneuver route of forces and equipment, created on the basis of the influences of all five layers, takes the form of a group of consecutive points with an exact geographical form. The route points of the created maneuver can be exported to a text format file for the external transmission. The text file is then transferred and imported to other Maneuver Control Systems CZ installed on the computer workstations. The imported route represents only a graphical object in the next assigned raster model layer, which does not require additional editing. If the unit itself has planned its route within decentralized command and control and the independent performance of tasks, then it must be approved by the superior. If it does not harmonize with the commander's intent, then the command station can replace it using its own calculation, which will also include the facts unknown to the subordinate station. However, the facts mentioned must be included in the MCS CZ so that the algorithm can take them into account in the calculation. From the viewpoint of operational security, their existence and character do not have to be known to all users.

The use of the MCS CZ on a network of interconnected computer workstations will make demands on the exact definition of the organizational structure, i.e. the superiority, and the authorized access to the information. One of the major advantages of digitizing the battlefield is the ability of all computer workstations to share any information. According to the nature of authorization, the individual information is then displayed on the Common Operational Picture, based on the geographical location and the usability in performing the task.

5 CONCLUSION

The results of simulating the frontal attack maneuver of the first-line companies of the battalion show clearly their course in the zone of planned attack. The times to reach the objective have been calculated for all three companies in the range from 20 minutes and 34 seconds to 23 minutes and 17 seconds, which, ideally, will allow the timed attacking the enemy defense in urban areas.

The COP processed and shared on a computer workstation network represents a tool essential for fast situation awareness. The friendly forces´ maneuver routes, calculated through the MCS CZ based on the speed and safety criteria, enable commanders to gain operational superiority over the enemy. Due to utilizing and sharing their spatial specifications in the field, a subordinate unit can be tasked directly to execute a specific maneuver. Similarly, the MCS CZ creates conditions for autonomous decision-making when planning a maneuver for units in military operations. Within the decentralized command and control process, the subordinate weapon systems, platoons, or companies can plan their own maneuver route in the superior's zone of attack and then submit it for approval through a joint COP. In this way, each commander will get an overview of the planned maneuver of the subordinate forces and means, its duration, the time of reaching the individual coordination lines or areas and the time of reaching the objective. The action of air, artillery and engineer support can be planned to calculate maneuvers and their time characteristics.

In every military operation, the plan does not survive the contact with the enemy. However, in the environment of networked computer workstations using the MCS CZ, it is possible to react flexibly to any change in the situation on the battlefield through a fast creation or recalculation and sharing of a new maneuver route of friendly forces and equipment.

References

[1] RYBANSKY, M.: Effect of the Geographic Factors on the Cross Country Movement during Military Operations and the Natural Disasters. In: *Proceedings of the International Conference on Military Technologies ICMT 07.* Brno : (Czech Republic), 2007, 7 pp. ISBN 978-80-7231-238-2.

[2] RYBANSKÝ, M., VALA, M.: Geographic Conditions of Military Transport Using Roads and Terrain. In: *ICMT'09 - International conference on military technologies 2009.* Brno : 2009. 9 pp, ISBN 978-80-7231-649-6.

[3] SPAK, U.: The common operational picture : A powerful enabler or a cause of severe misunderstanding? In: *22st International Command and Control Research and Technology Symposium (ICCRTS)* : *Frontiers of C2*, 2017, vol. Topic 4.

[4] Sophronides, Panayiotis & Papadopoulou, Chrysaida-Aliki & Giaoutzi, Maria & Scholten, Henk. A Common Operational Picture in Support of Situational Awareness for Efficient Emergency Response Operations. In: *Journal of Future Internet.* Vol 2. pp. 10-35. 10.18488/journal.102.2017.21.10.35.

[5] KUUSISTO, R., KUUSISTO, T., ARMISTEAD, L.: *Common Operational Picture. Situation Awareness and Information Operations*. 2005. pp. 175-186.

[6] HODICKÝ, J., CASTROGIOVANNI, R., LO PRESTI, A.: Modelling and Simulation Challenges in the Urbanized Area. In: *Proceedings of the 2016.* 17th International Conference on Mechatronics - Mechatronika (ME) 2016. Prague : Czech Technical University in Prague, 2016, p. 429-432. ISBN 978-80-01-05882-4.

[7] DUDCZYK, J., RYBAK, L.: *Adaptive Decision Support System in Network Centric Warfare Process.* Elektronika: konstrukcje, technologie, zastosowania. 7. 39-42. 10.15199/13.2018.7.10.

[8] NOHEL, J.: Possibilities of Raster Mathematical Algorithmic Models Utilization as an Information Support of Military Decision Making Process. In: *Modelling and Simulation for Autonomous Systems.* Cham, Switzerland : Springer: NATO Modelling and Simulation Centre, 2018, p. 553-565. ISSN 0302-9743. ISBN 978-3-030-14984-0. DOI: 10.1007/978-3-030-14984-0_41.

[9] NOHEL, J., STODOLA, P., FLASAR, Z.: Model of the Optimal Maneuver Route [Online First], IntechOpen, DOI: 10.5772/ intechopen. 85566. Available from: https://www.intechopen.com/online-first/model-of-the-optimal-maneuver-route

Capt. Dipl. Eng. Jan **NOHEL**, Ph.D.
Department of Intelligence support
University of Defense in Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: jan.nohel@unob.cz

Assoc. Prof. Dipl. Eng. Zdeněk **FLASAR**, CSc.
Department of Tactics
University of Defense in Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: zdenek.flasar@unob.cz

Prof. Dipl. Eng. Petr **STODOLA**, Ph.D.
Department of Intelligence support
University of Defense in Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: petr.stodola@unob.cz

Jan **NOHEL** is active as lecturer at Department of Intelligence support at the University of Defense in Brno in Czech republic. He holds Ph.D. in Military management (2015). His research interests include the information support of the decision-making process of commanders at the tactical command and control level, tactical and terrain analyses and cross-country movement modelling. He is focused on the issue of mathematical algorithms design for data processing and fusion and their integration in C4ISR systems. Before starting his research career, he accumulated military experience from being a commander and staff officer of Czech Republic army units and also he took part in the foreign missions as RS (2013 and 2017).

Zdeněk **FLASAR** is an Associate Professor at University of Defense in Brno, Czech Republic, where he works as a senior researcher of the Department of Tactics. He served as battalion commander and started his research career in 1985. His scientific and professional also educational work is connected with tactics of military units, Command and control process and methodology of military training. He participates on national military exercises, research and cooperation projects.

Petr **STODOLA** is a Professor at University of Defence in Brno, Czech Republic, where he works as a senior researcher of the Department of Intelligence support. He received his Ph.D. degree in the field of military technology at University of Defence in 2006. His research interests include optimization, combat modeling and simulation, command and control decision support systems and C4ISR systems. He is the author or co-author of more than 100 scientific papers, and more than 10 functional samples and application software. He participated in more than 10 scientific projects.

NTSP 2020
NEW TRENDS IN SIGNAL PROCESSING
15TH INTERNATIONAL CONFERENCE ON NEW TRENDS IN SIGNAL PROCESSING 2020

NEW TRENDS IN SIGNAL PROCESSING 2020

October 14 – 16, 2020

in Hotel Chopok, Demänovská dolina, Slovakia

The conference covers main topics:

- **Signal Processing;**
- **Applied Electronics;**
- **Information and Communication Engineering;**
- **Microwave Engineering;**
- **Signal Processing in Military Applications.**

All papers for the NTSP 2020 will be reviewed and published in electronic form on DVD and will be submitted to **IEEE Xplore database**.

Organizers: Armed Forces Academy of General M. R. Štefánik, Liptovský Mikuláš, Department of Electronics and The Slovak Elektrotechnic Society – affiliated branch Liptovský Mikuláš.

For more information see the conference website: **http://ntsp2020.aos.sk/**

USE OF DATA MINING FOR NETWORK BEHAVIOR ANALYSIS OF SELECTED OPERATING SYSTEMS

Július BARÁTH

Abstract: The aim of this paper is to use data mining techniques to obtain characteristic behavior patterns of operating systems with a focus on the communication observed by a remote observer. Network communication of selected operating systems is observed, and the list of contacted targets is recorded. Based on the list, we try to identify the type of operating system used or a group of installed applications. Obtained data can be used for passive reconnaissance of remote networks, detection of possible undesirable leaks of information, filtering of selected communication, etc.

Keywords: Network analysis; Data mining; Operating systems; SIEM; NetFlow.

1 INTRODUCTION

The networking of computers allows us to ensure the proper operation of the operating system and installed applications. This includes the process of activating and updating the operating system, system applications supplied by hardware manufacturers and application software. At the same time as using such a system, the manufacturer collects operational and diagnostic data at varying levels and intensities. Network communication is also heavily used by cloud solutions and other online services. When we add user activity and use of web services, social networks, and a wide range of multimedia delivery services, we get an indicative picture of the type, amount, and volume of data transmitted by the host.

In general, network analysis can be performed from different points of view [6], [7] - in the paper, we analyze the possibility of recognizing the type of operating system based on passive monitoring of network communication. We analyze computer-used protocols and target networks, linking the information we gather with operating system manufacturers, cloud services, and application programs while determining the likely type of operating system.

2 DESCRIPTION OF TEST ENVIRONMENT AND EXPERIMENTS

To analyze the network behavior of selected operating systems in laboratory conditions, we used 15 physical computers installed on different hardware platforms, 3 virtual machines, one firewall and SIEM ArcSight for data collection and analysis.

The test environment contained 5 Dell computers running Windows 10 1809 with MS Office, Google Chrome, and Java installed. 5 HP Notebooks with Linux Mint 18.3 with no extra software installed, 5 MacBook Pro with Mac OS X Mojave 10.14.3 plus MS Office, Google Chrome and Java. Virtual machines installed 2 x Windows server 2016 with DNS, DHCP, AD and Exchange server 2016, and 1x Debian. Outbound communication was monitored on the FortiGate 60D firewall using the NetFlow protocol and analyzed using the ArcSight Console 6.11, see Fig. 1.

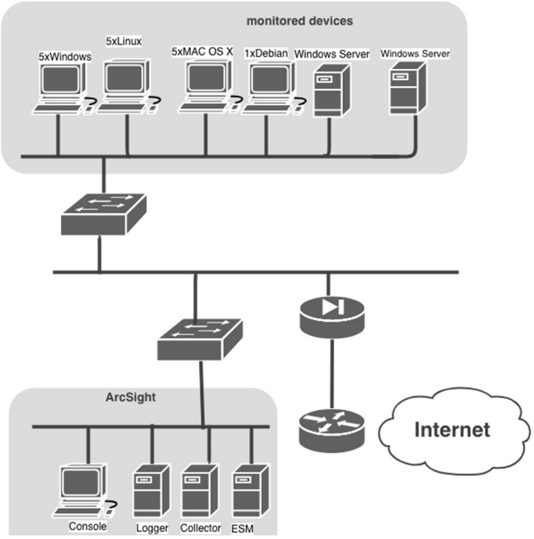


Fig. 1 Test site configurations
Source: author.

The experiment ran in three phases. The phases vary in duration, number of monitored computers and installed software.

The first experiment was one day with one Windows, Linux, and Mac OS X computer monitoring. Operating data were collected locally using tcpdump and remotely using the firewall and NetFlow protocol. Due to the large volume of data captured by tcpdump, this experiment variation was short-lived and unusable for a larger number of computers over a longer period of time. In this experiment, a local switch was configured to send all monitored computer communications to a monitoring device - a Linux workstation.

The second experiment lasted for a week and we monitored 5x Windows, 5x Linux, 5x Mac OS X, and 2x Windows Server devices. Only data obtained by firewall and NetFlow protocol were analyzed.

Third - a supplementary experiment lasted a week and monitored were Debian and Windows 10 computers with a configuration that minimizes the sending of service data to Microsoft [4]. The

Windows 10 computer and the iCloud application were also included in the experiment. Only data collected by firewall and NetFlow protocol was collected.

For all experiments, computers were forbidden to switch to hybrid mode and were not used by any user.

3 OBTAINED DATA AND THEIR ANALYSIS

Data collection was performed using SIEM ArcSight, which collects, normalizes, and evaluates operational data, which it then displays in aggregate monitoring panels. When dealing with security incidents, SIEM displays them in near real time with all the details available.

ArcSight Logger is an event storage device that is optimized for extremely high event flow throughput. Logger stores security events in a compressed form but can always provide unmodified historical data on request.

ArcSight ESM collects, normalizes, aggregates and filters millions of events from thousands of network resources into a manageable flow that is prioritized according to the risk, vulnerability, and criticality of the assets. These priority events can then be correlated, investigated, and analyzed by ESM to help you get an overview of the current situation and enable real-time response.

Smart Connectors are interfaces to network objects that create correlation-related event data. After collecting event data from network resources, they normalize data in two ways: normalizing values (such as severity, priority, and time zone) to a common format and normalizing the data structure to a common scheme. Smart Connectors can then filter and collect events to reduce the number of events sent to the manager, increasing the efficiency and accuracy of the ESM and reducing event processing time. Smart Connectors also add information to the data they collect, such as searching hostnames or their IP addresses.

The ArcSight Console is an interface designed for full-time security professionals in the Security Operations Center or similar security monitoring environment. It is an authoring tool for creating filters, rules, reports, pattern detection, dashboards, and data monitors. For the purpose of experiments, a set of source filters was created to define traffics from monitored computers and used NetFlow collector, which subsequently provided data for identifying target devices in communication and calculating the volume of transmitted data. These values were processed by reports containing the destination addresses, the volumes of data transferred that could then be exported, the names of the target networks added, and the manual processing of results (Fig. 2).

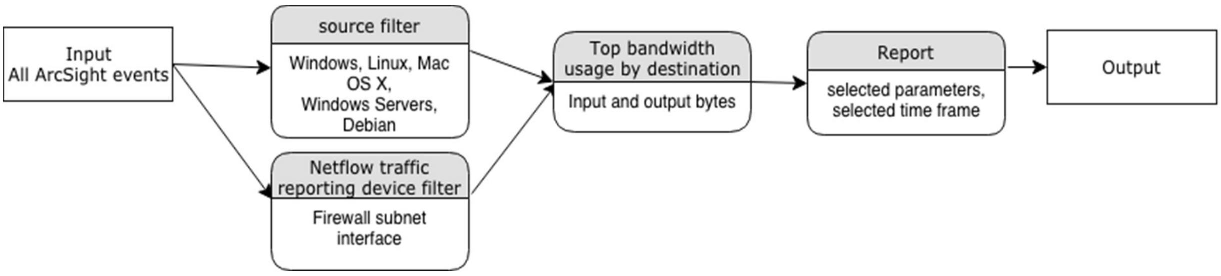

Input
All ArcSight events
source filter
Windows, Linux, Mac OS X, Windows Servers, Debian
Netflow traffic reporting device filter
Firewall subnet interface
Top bandwidth usage by destination
Input and output bytes
Report
selected parameters, selected time frame
Output

Fig. 2 Extraction of experiment data from collected events
Source: author.

Target network name detection was done by reverse DNS script and manually on registrar web pages for automatically undetected records.

3.1 Experiment 1

One-day test of three operating systems on three computers. A Windows 10 computer created a total of 225 unique connections, see Table 1. Unique connection means one or more contacts to the same destination address.

The two largest categories of connections (Microsoft and AOS + OS SR) were linked directly to the operation of the Microsoft operating system and applications - windows update, telemetry, and OneDrive [1]. Equally evident is the communication of the Eset antivirus tool, the Chrome app from Google, and the system utility from Dell's hardware manufacturer.

At the same time, a computer running MAC OSX created a total of 157 connections, see Table 2.

The most common was the traffic-related communication and directed to Apple - telemetry, Siri Assistant, and other company services [2] followed by Chrome application communication and Microsoft application communications (MS Office for Mac OS installed).

The Linux Mint computer has created 39 connections, see Table 3.

These were OS application and service repository services, time synchronization, and search services. Fig. 3 shows the periodic 2-hour contacting of Linux repositories. For better readability, the NTP port 123 communication is filtered out.

Table 1 List Of Unique Windows 10 Contacted Addresses

Target name	Unique addresses
Microsoft Corporation	97
AOS + OS SR	80
eset.com.	16
Level 3 Communications, Inc.	9
google.com	8
other	7
dell.com	3
Verizon Business	3
Cloudflare, Inc.	2

Source: author.

Table 2 List Of Unique Mac Osx Contacted Addresses

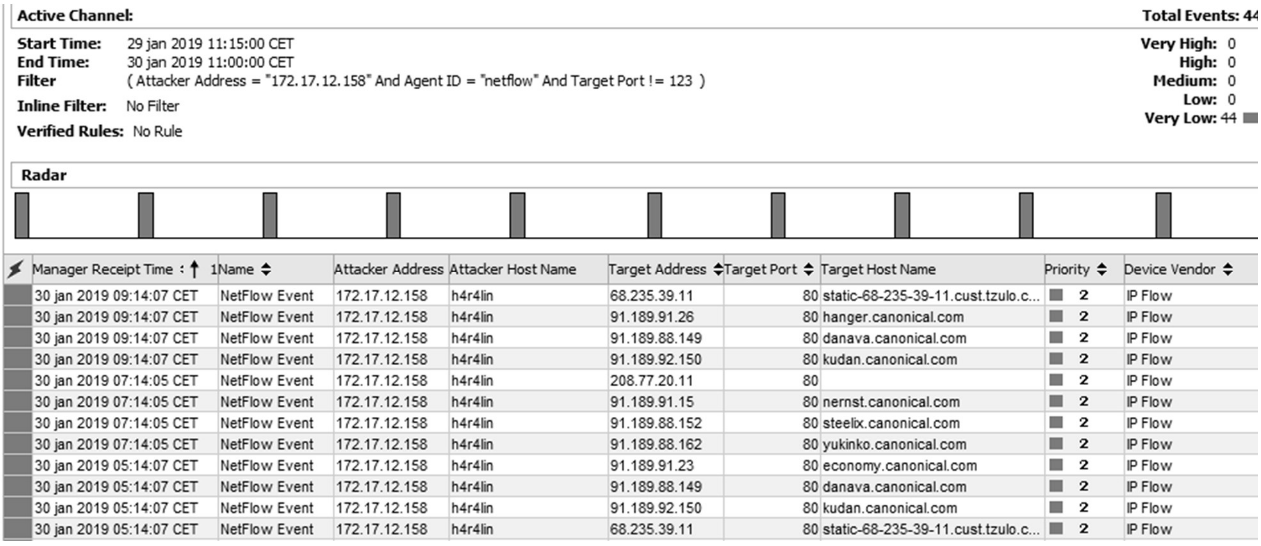
Target name	Unique addresses
apple	116
google.com	24
Microsoft Corporation	13
other	3
Verizon Business	1

Source: author.

Table 3 List Of Unique Linux Contacted Addresses

Target name	Unique addresses
canonical.com	13
other	9
amazonaws.com	8
google.com	6
cloudfront.net.	3

Source: author.



Active Channel: Total Events: 44

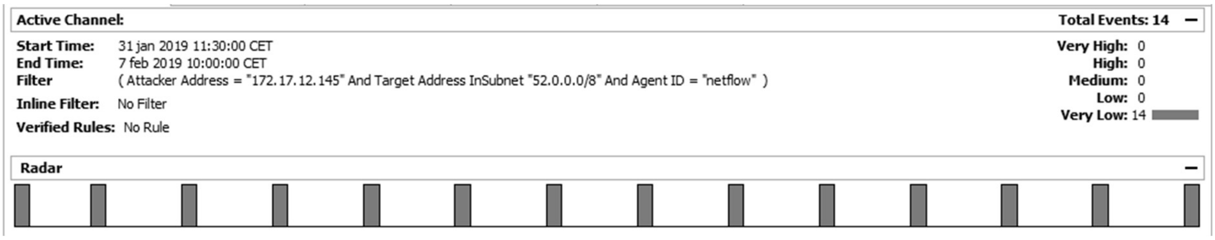
Start Time: 29 jan 2019 11:15:00 CET
End Time: 30 jan 2019 11:00:00 CET
Filter (Attacker Address = "172.17.12.158" And Agent ID = "netflow" And Target Port != 123)
Inline Filter: No Filter
Verified Rules: No Rule

Very High: 0
High: 0
Medium: 0
Low: 0
Very Low: 44

Radar

Manager Receipt Time	Name	Attacker Address	Attacker Host Name	Target Address	Target Port	Target Host Name	Priority	Device Vendor
30 jan 2019 09:14:07 CET	NetFlow Event	172.17.12.158	h4r4lin	68.235.39.11	80	static-68-235-39-11.cust.tzulo.c...	2	IP Flow
30 jan 2019 09:14:07 CET	NetFlow Event	172.17.12.158	h4r4lin	91.189.91.26	80	hanger.canonical.com	2	IP Flow
30 jan 2019 09:14:07 CET	NetFlow Event	172.17.12.158	h4r4lin	91.189.88.149	80	danava.canonical.com	2	IP Flow
30 jan 2019 09:14:07 CET	NetFlow Event	172.17.12.158	h4r4lin	91.189.92.150	80	kudan.canonical.com	2	IP Flow
30 jan 2019 07:14:05 CET	NetFlow Event	172.17.12.158	h4r4lin	208.77.20.11	80		2	IP Flow
30 jan 2019 07:14:05 CET	NetFlow Event	172.17.12.158	h4r4lin	91.189.91.15	80	nernst.canonical.com	2	IP Flow
30 jan 2019 07:14:05 CET	NetFlow Event	172.17.12.158	h4r4lin	91.189.88.152	80	steelix.canonical.com	2	IP Flow
30 jan 2019 07:14:05 CET	NetFlow Event	172.17.12.158	h4r4lin	91.189.88.162	80	yukinko.canonical.com	2	IP Flow
30 jan 2019 05:14:07 CET	NetFlow Event	172.17.12.158	h4r4lin	91.189.91.23	80	economy.canonical.com	2	IP Flow
30 jan 2019 05:14:07 CET	NetFlow Event	172.17.12.158	h4r4lin	91.189.88.149	80	danava.canonical.com	2	IP Flow
30 jan 2019 05:14:07 CET	NetFlow Event	172.17.12.158	h4r4lin	91.189.92.150	80	kudan.canonical.com	2	IP Flow
30 jan 2019 05:14:07 CET	NetFlow Event	172.17.12.158	h4r4lin	68.235.39.11	80	static-68-235-39-11.cust.tzulo.c...	2	IP Flow

Fig. 3 Linux periodic repository check example
Source: author.



Active Channel: Total Events: 14

Start Time: 31 jan 2019 11:30:00 CET
End Time: 7 feb 2019 10:00:00 CET
Filter (Attacker Address = "172.17.12.145" And Target Address InSubnet "52.0.0.0/8" And Agent ID = "netflow")
Inline Filter: No Filter
Verified Rules: No Rule

Very High: 0
High: 0
Medium: 0
Low: 0
Very Low: 14

Radar

Fig. 4 Mac OSX periodic contact of Microsoft Network Example
Source: author.

3.2 Experiment 2

The aim of the second experiment was to verify the behavioral model of selected operating systems for more computers monitored over a week. 5 computers with Windows 10 created a total of 490 unique connections, see Table 4.

Table 4 List Of Unique Windows 10 Contacted Addresses

Target name	Unique addresses
AOS + OS SR	244
Microsoft Corporation	185
Level 3 Communications, Inc.	27
eset.com.	17
google.com	11
Verizon Business	3
other	3

Source: author.

Local area network communication (AOS + OS SR) used ports 7680 - Windows Update Delivery Optimization (WUDO) in Windows LANs, 3128 - Web Proxy, 2222 - ESET Remote Administrator and 123 - Network Time Protocol (NTP) - this communication from a remote could not be observed and is given for illustration only. The structure of Microsoft network connections was the same as in Experiment 1, and 16 networks were contacted overall.

At the same time, computers with MAC OS X created a total of 299 connections, see Table. 5.

Table 5 List Of Unique Mac Osx Contacted Addresses

Target name	Unique addresses
apple	240
Microsoft Corporation	31
google.com	25
Verizon Business	2
yahoo.com	1

Source: author.

The structure of Microsoft network connections was consistent with the findings in Experiment 1, and 5 networks were contacted overall, and periodic links Fig. 4. could be found in this case as well.

Linux Mint computers created a total of 16 connections, with only port 123 time synchronization services and repository control on communication port 80. Windows Server computers behaved similarly to Windows 10 computers, see Table 6.

Table 6 List Of Unique Windows Server Contacted Addresses

Target name	Unique addresses
Microsoft Corporation	73
eset.com.	34
Level 3 Communications, Inc.	6
Verizon Business	2

Source: author.

The structure of the Microsoft network connections was similar, with 13 networks being contacted in total, as opposed to 16 - which could be due to the absence of MS office on the servers. Installed network services, such as the DNS server array, which generated a large number of connections on port 53 and so on, have shown up on servers.

3.3 Experiment 3

The goal of this experiment was to verify:

- the distinctive behavior of different Unix OS types - Linux Mint and Debian in our case,
- the effect of setting privacy options in Windows 10 on the number of networks contacted,
- add apple iCloud services on a Windows 10 computer.

Linux-based systems in default configuration communicate with the lowest intensity compared to other OSs. A common feature of system behavior was that both systems were using time synchronization service port 123 and periodic repository checks using port 80 only.

For a Windows computer, we've taken advantage of [4] privacy settings and verified the number and structure of Microsoft contacted networks. The experiment did not confirm a decrease in the number of Microsoft networks contacted.

Finally, iCloud for Windows was installed on a Windows OS computer. Within one week, the activities of the system and the way of communication were monitored. As expected, the system contacted Apple's network, and from the records, it was possible to distinguish which services it used. The list of ports used by Apple for OS and application communications is available, for example, on [2].

3.4 Data evaluation

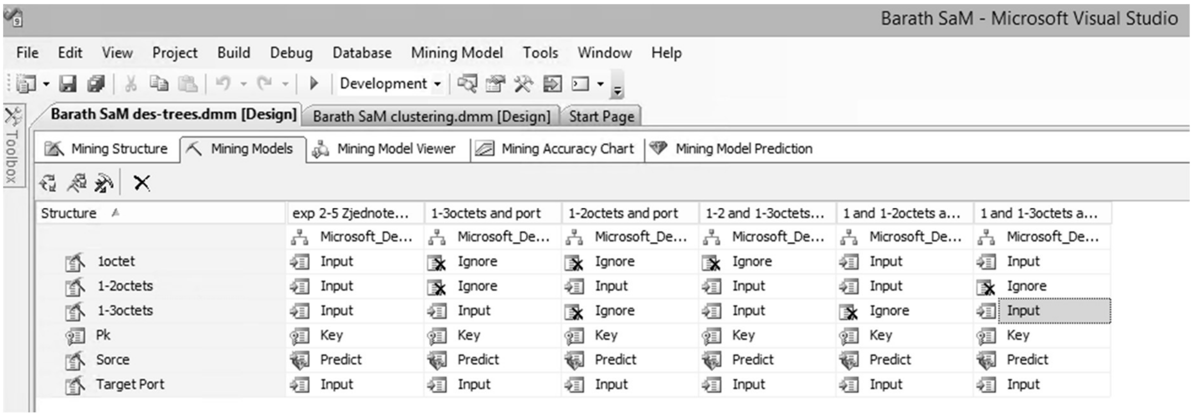
Data mining techniques were used to find the signatures characterizing each operating system.

Preprocessed input data were loaded into the MS SQL database, where the data table contained the OS type, 1. Octet, 1-2. Octets, 1-3. Octets of destination IP address and finally destination port.

The first method used to search for OS signatures was the Microsoft decision trees method. The Microsoft Decision Trees algorithm learns Bayesian networks from a combination of prior knowledge and statistical data. An important part of the algorithm is the methodology for assessing the information value of the priors needed for learning. The approach is based on the assumption of likelihood equivalence, which says that data should not help to discriminate network structures that otherwise represent the same assertions of conditional independence. Each case is assumed to have a single Bayesian prior network and a single measure of confidence for that network. Using these prior networks, the algorithm then computes the relative posterior probabilities of network structures given the current training data, and identifies the network structures that have the highest posterior probabilities. The Microsoft Decision Trees algorithm uses different methods to compute the best tree. The method used depends on the task, which can be linear regression, classification, or association analysis. A single model can contain multiple trees for different predictable attributes. Moreover, each tree can contain multiple branches, depending on how many attributes and values there are in the data. The shape and depth of the tree built in a particular model depends on the scoring method and other parameters that were used. Changes in the parameters can also affect where the nodes split[1].

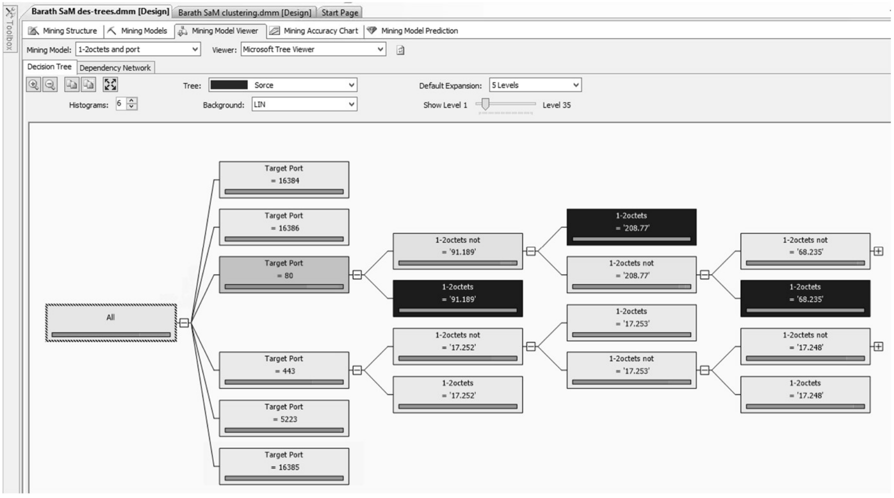
A total of 6 experiments were performed with different combinations of input data, see Fig. 5

The simulation divided the dataset into a training and test set, and after learning the results were generated for each model in the form of a decision tree, see Fig. 6.


Barath SaM - Microsoft Visual Studio
File Edit View Project Build Debug Database Mining Model Tools Window Help
Development
Toolbox
Barath SaM des-trees.dmm [Design]
Barath SaM clustering.dmm [Design]
Start Page
Mining Structure
Mining Models
Mining Model Viewer
Mining Accuracy Chart
Mining Model Prediction

Structure	exp 2-5 Zjednote...	1-3octets and port	1-2octets and port	1-2 and 1-3octets...	1 and 1-2octets a...	1 and 1-3octets a...
	Microsoft_De...	Microsoft_De...	Microsoft_De...	Microsoft_De...	Microsoft_De...	Microsoft_De...
1octet	Input	Ignore	Ignore	Ignore	Input	Input
1-2octets	Input	Ignore	Input	Input	Input	Ignore
1-3octets	Input	Input	Ignore	Input	Ignore	Input
Pk	Key	Key	Key	Key	Key	Key
Sorce	Predict	Predict	Predict	Predict	Predict	Predict
Target Port	Input	Input	Input	Input	Input	Input

Fig. 5 Definition of models and input data for deision trees
Source: author.



Mining Model: 1-2octets and port
Viewer: Microsoft Tree Viewer
Tree: Sorce
Default Expansion: 5 Levels
Histograms: 6
Background: LIN
Show Level 1 Level 35

Fig. 6 Display the result for the decision trees method
Source: author.

[1] Microsoft Visual studio on-line help.

The accuracy of the model was verified on a test set and evaluated based on the classification matrix from the Mining accuracy chart. To evaluate the results, SV and FV values were generated from the classification matrix of each model. SV is a 3-dimensional vector of success OS (WIN, LIN, MAC OSX) classification and FV is a 6-dimensional vector of failure OS classification. The H value was calculated for each model using

$$H = \left\| \underset{SV}{\rightarrow} \right\| - \left\| \underset{FV}{\rightarrow} \right\| \tag{1}$$

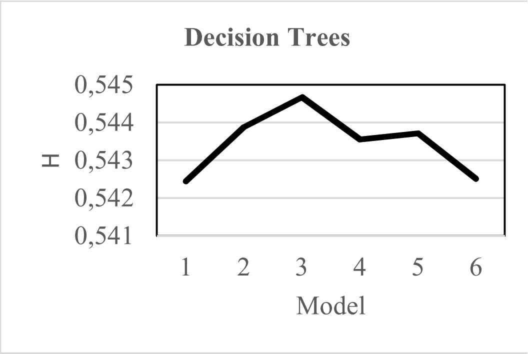
where Euclidean norm of SV is

$$\left\| \underset{SV}{\rightarrow} \right\| := \sqrt{SV^{2}_{\frac{win}{win}} + SV^{2}_{\frac{lin}{lin}} + SV^{2}_{\frac{mac}{mac}}} \tag{2}$$

and Euclidean norm of FV is

$$\left\| \underset{FV}{\rightarrow} \right\| := \sqrt{FV^{2}_{\frac{lin}{win}} + FV^{2}_{\frac{mac}{win}} + FV^{2}_{\frac{win}{lin}} + FV^{2}_{\frac{mac}{lin}} + FV^{2}_{\frac{lin}{mac}} + FV^{2}_{\frac{win}{mac}}} \tag{3}$$

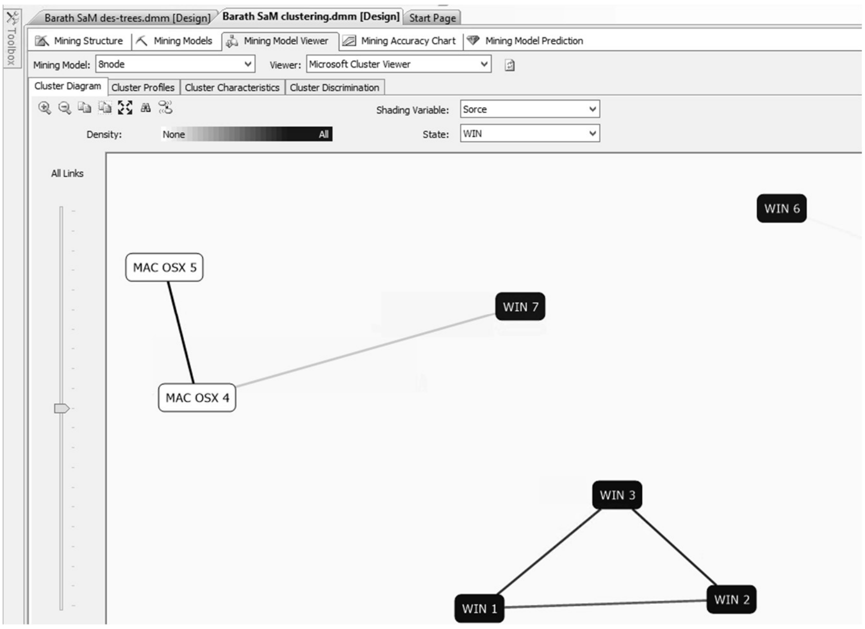
The best solution was the model with the highest H value, see Graph 1.



Graph 1 Graph of H values for analyzed models
Source: author.

The second method used to search for OS signatures was the Microsoft clustering method.

The Microsoft Clustering algorithm provides two methods for creating clusters and assigning data points to the clusters. The first, the K-means algorithm, is a hard clustering method. This means that a data point can belong to only one cluster, and that a single probability is calculated for the membership of each data point in that cluster. The second method, the Expectation Maximization (EM) method, is a soft clustering method. This means that a data point always belongs to multiple clusters, and that a probability is calculated for each combination of data point and cluster. In EM clustering, the algorithm iteratively refines an initial cluster model to fit the data and determines the probability that a data point exists in a cluster. The algorithm ends the process when the probabilistic model fits the data.



Mining Model: 8node

Viewer: Microsoft Cluster Viewer

Shading Variable: Sorce

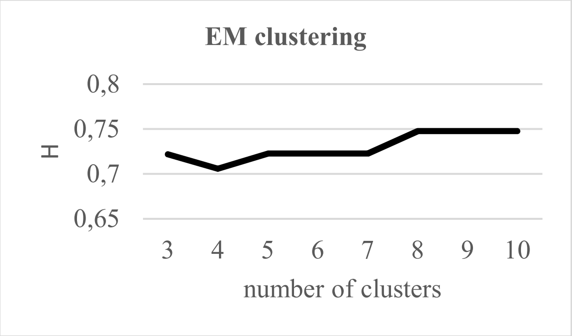
State: WIN

Fig. 7 View the results of EM clustering for 8 clusters
Source: author.

The function used to determine the fit is the log-likelihood of the data given the model. If empty clusters are generated during the process, or if the membership of one or more of the clusters falls below a given threshold, the clusters with low populations are reseeded at new points and the EM algorithm is rerun[2].

We used the EM method in our experiments. A total of 8 experiments were performed with a different number of clusters required, with an example of the result for 8 clusters being on Fig. 7.

As in the previous case, we also calculated H for each model and chose the model with the highest H value as best, see Graph 2.



Graph 2 Graph of H values for analyzed models
Source: author.

4 CONCLUSION

The aim of this work was to find out whether it is possible to find out the structure of operating systems or installed application software by means of passive monitoring of network communication. Measurements were made under laboratory conditions, while computers were not used for routine work during the experiment so that the results were not affected by user work and patterns of behavior of selected operating systems could be obtained. A monitoring probe was placed on the nearest router, in real terms it could be on ISPs. For measurements, only the IP address and port number of the transmitted datagrams were analyzed.

The collected data were analyzed by two methods of data mining - decision trees and clustering method. In both methods we were looking for the optimal configuration, with the highest value of H selected as the criterion. For the purpose of OS-type recognition based on communication, better results were achieved by the clustering method. The results of the measurements were shown on the respective graphs.

Based on the measurements, it was found that the main identifying indicator of the compared operating systems was communication with the manufacturer's networks. For Linux, it was contacting repositories.

The largest network activity was reported by Microsoft systems, followed by Apple's system, leaving Linux's lowest network footprint. Incorrectly configured devices using WUDO outside the local network have also been detected during the experiment, which can further increase the volume of data transmitted. In Tab. 1 and Tab. 4. WUDO communication in the local network is also marked as AOS + OS SR. Such communications would not be recorded in remote monitoring.

Based on passive monitoring, it was possible to determine the type of antivirus solution being used, in our case the Eset tool, as well as the use of Dell hardware. MS office suite was installed on both MS Windows and MAC OSX computers. This led to the detection of the Microsoft network connection from MAC OSX computers.

The characteristic behavior of operating systems and applications can be used to create communication patterns for remote passive network analysis.

Knowledge of network communication of the selected operating system, program or service can be used for centralized filtering to:

- reducing the content of transmitted data through public networks,
- masking used operating system types using packet filtering [5],
- stopping the provision of traffic data by the manufacturer,
- stopping the availability of selected services and so on.

Sufficient timeframes are needed to determine the identification patterns for OS and application recognition, as the target network contacting period for different products is different and consists of multiple unique characteristics.

By using the communication tracking method, it is possible to passively determine the size of the monitored network, as well as its likely use or type of monitored organization.

References

[1] HALFIN, D., KROKLI, T. B., LOHR, H.: "*Windows 10, version 1809, connection endpoints for non-Enterprise editions.*" 2018 26.06.2018 [cited 2019 March]. Available from: https://docs.microsoft.com/en-us/windows/privacy/windows-endpoints-1809-non-enterprise-editions.

[2] "*TCP and UDP ports used by Apple software products*." 2019 [cited 2019 March]. Available from: https://support.apple.com/en-us/HT202944.

[2] Microsoft Visual studio on-line help.

[3] "*Desktop Operating System Market Share Worldwide.*" [cited 2019 March]. Available from: http://gs.statcounter.com/os-market-share /desktop/worldwide#monthly-201704-201704-bar.

[4] HOFFMAN, C.: *"Windows 10 Sends Your Activity History to Microsoft, Even if You Tell It Not To.“* 2018 10.12.2018 [cited 2019 March]. Available from: https://www.howtogeek.com /fyi/windows-10-sends-your-activity-history-to-microsoft-even-if-you-tell-it-not-to/.

[5] TURČANÍK, M.: *"Packet filtering by artificial neural network"* ICMT 2015: International Conference on Military Technologies 2015. Brno : University of Defense, 2015. ISBN 978-80-7231-976-3. s. 415-418.

[6] VRÁNOVÁ, Z., ONDRYHAL, V., OTRADOVSKÁ, L.: "Evaluation of network behavior due to changes in network structure." In: *Proceedings of the 2011 Networking and Electronic Commerce Research Conference (NAEC2011)*. Riva del Garda (Italy) : ATSMA, 2011, p. 97-106. ISBN 978-0-9820958-5-0.

[7] MAZÁLEK, A., ONDRYHAL, V., PLÁTĚNKA, V., VRÁNOVÁ, Z.: "Detecting the trend component for selected network parameters." In: *Mathematical methods and techniques in engineering and environmental science.* Catania : WSEAS Press, 2011. p. 391-395. ISBN 978-1-61804-046-6.

Dipl. Eng. Július **BARÁTH**, PhD.
Department of Informatics
Armed Forces Academy of General M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš
Slovak Republic
E-mail: julius.barath@aos.sk

Július **BARÁTH** - graduated Military Technical University in 1991, received PhD. degree in 1996 and works 23 years as a assistant professor at the Department of Informatics, Armed Forces Academy, Liptovský Mikuláš, Slovakia. His professional interests include computer networks, operating systems and network security.

SMALL UNMANNED AERIAL VEHICLES – THREATS AND DEFENCE AGAINST THEM

Jakub VILÍMEK

Abstract: The article discusses actual small UAVs (Unmanned Aerial Vehicles) threats and ways of defence against them. The introduction contains UAVs regulations in the Czech Republic. The literature review of relevant papers in the UAV threats and defence follows. The third part is about off-the-shelf and professional UAVs, which can be misused to attack. The core of this article describes three vital processes for planning UAV protection: detection, identification and elimination. The goal of the article is to define vital questions, which has to be answered before designing any UAV protection system. The correct answers to these questions depend on the protected area, assets, etc.

Keywords: UAV; UAS; Threat; Detection; Protection; Sensors.

1 INTRODUCTION

Unmanned vehicles (land, aerial, surface and underwater) are very popular and actual topic today. The market is flooded with professional and amateur unmanned vehicles. On this fact reacted most of the nations' authorities and created some legal restrictions on UAV[1] usage.

The legal framework of UAVs usage in the Czech Republic is defined in the Regulation L2, Rules of the Air, Attachment X [1]. Attachment X restricts usage of UAVs in certain areas for all the time (e.g. airfield protection zones, restricted areas around nuclear plants, army objects, dangerous areas – gas release areas, etc.), or for certain time of the day (e.g. military training areas during the training).

Attachment X also restricts the minimal distance between UAV and persons, buildings and inhabited areas. The distance for small UAVs (up to 7 kg) is the distance described as safe[2]. This distance for UAVs heavier than 7 kg is again recommended as safe but the Attachment X orders minimal distances as well: 50 m for starting and landing, during the flight UAV cannot be closer than 100 m to persons, assets or buildings, which are not related to the flight. UAV cannot be closer than 150 m to any densely populated area [2].

The violation of the legal framework can be done by negligence or on purpose. The presence of the UAV in the restricted area (e.g. airfield vicinity) can disturb security or safety of the whole area. An intentional presence in the restricted areas can have various reasons.

UAVs can simply collect imagery, or in general sensor information and with this imagery the UAV's operator can search for weak spots in the security of the area of interest (airfield, ammunition dump, nuclear powerplant, etc.). In this case the UAV is just a first step before frontal assault on the protected object.

Next reason of the UAV's presence in the restricted area can be a direct attack with weapons or explosives attached to the UAV. Attachment X [1] forbids loading and transporting any dangerous substances or devices, as well as dropping any objects during the flight[3].

A price of an off-the-shelf UAV with improvised explosives is very low in comparison with possible effect, inflicted damage and injuries. Very unlikely scenario describes possible attack with a radioactive or poisonous material, explosives, both attached to the UAV. This UAV can fly over densely populated area, unprotected water source, etc. and then it can explode as a "dirty bomb".

Possible types of attack must be considered during planning any small UAV protection of the areas with critical infrastructure, or areas with high concentration of people. Next question is the type of UAV – amateur, professional or even military. Next level of any protection planning is protection against the whole swarm of cooperating UAVs. This type of attack exceeds scope of this article and it was not a part of the literature review.

2 THE LITERATURE REVIEW

The literature review was oriented to Scopus indexed papers with the goal to find the relevant papers in the theme "(UAV or UAS) and threats and (defence or defense)". The topic was found in 105 articles (on April 30, 2019), the result of the search was sorted by "Newest" and for further inspection were chosen only the most relevant 8 articles; see [3] to [10].

New problems with the fight against UAS were caused by the technology in the development of commercial drones that are available to the

[1] In the article will be used following terms: UAV: Unmanned Aerial Vehicle (drone), UAS: Unmanned Aerial System (UAV, control station, devices for communication, start and land). Sometimes the term UAX (UAV or UAS) is more suitable.

[2] The Civil Aviation Authority in the Czech Republic recommends the save distance as ration of 1:2 during forward flight (each 100 altitude meters safe radius 200 meters) and 1:1 during hovering (each 100 altitude meters safe radius is 100 meters) [2].

[3] Articles 10 and 11.

population without any problems. They can also be used in war and crisis situations; they can act as "paparazzi" and can be misused by criminal and terrorist entities. The primary task is detection in a fight against UAVs.

The paper [3] summarizes series of very complex measurements, that were performed by the authors during past 4 years. The experiments involved small UAV detection by radar (RL), radio frequency (RF), electro-optical (EO), infrared (IR), acoustic (AC); and detection by human senses (eyes and ears). The authors strongly suggest, based on the measurements results, using multispectral detection, building modular defence systems. The real-time detections are possible at these distances:

- standard X-Band radar: 3000 m;
- optical devices with zoom and skilled operators: 2000 m;
- infrared detectors: 350 m;
- personal audibility (unarmed ears): 250 m;
- personal visibility (unarmed eyes): 350 m.

UAVs are used in wide range of human activities and the amount of UAV users are growing rapidly. The risk of misuse of UAVs by criminals, guerrillas or terrorists is the actual threat. Importance of developing scientific fields for countering of UAVs rises. Areas of threats and defence include parts: Air surveillance; Command and Control; and Elimination [4].

UAV is becoming a threat to sensitive areas' defence, public safety, and privacy. For the difficulty of supervision, prevention, evidence collection, and punishment, the UAVs management is an urgent problem. The control signal of UAVs is an object for research with a goal to find the interference signal for smart jamming. Signal analysis using MATLAB was realized in time and frequency domain. Study of the typical civilian small UAV's communication protocols, and using the software defined radio to receive and store the control signals. After demodulation and data decryption are the signal parameters estimated effectively; the parsing command signal was used for generating the inference signal [5].

According to the study [6] the air defence used for civilian purposes, can include the long-term threat assessment and anticipation, infrastructure assessment, surveillance, tracking and imminent threat assessment, UAS target engagement and operator detection and capturing, and initiation of actions against UASs to prevent the intentions of rogue drones.

Nowadays, unconventional Low Slow and Small (LSS) air threats pose serious challenges that cause deep concerns among military and civilian security organizations. Consequently, there is a high demand for robust and reliable counter small unmanned aerial vehicles (C-sUAV) solutions. Detection challenges such as small air targets, unconventional flight patterns in low airspaces, terrain masking effects, or complex urban environments lead to high false alarm rates. Current C-sUAV systems in the market use improved radar components, originally either considered for VSHORAD[4] radar, battlefield radar, bird detection radar, perimeter surveillance radar, or high-resolution short-range radar [7].

The NATO has defined UAV categories in class 1 [7], see Table 1.

Table 1 NATO UAV class I

Type of UAV	Range	Altitude	Weight	Payload
Micro	5 km	100 m	< 2 kg	< 0.5 kg
Mini	25 km	1000 m	2 – 20 kg	< 10 kg
Small	100 km	1500 m	< 150 kg	< 50 kg

Source: [7].

An overview of the different sensors and properties can be found in Table 2.

Table 2 The sensor properties

	Long range	Position accuracy	Identification	Multiple targets	Low visibility conditions	Night	Passive
Visual	++	++	++++	++	-	-	++++
Infrared	++	++	++++	++	-[5]	++++	++++
Acoustic	-	-	+++	++	++++	++++	++++
ESM[6]	++++	++++	++	++++	++++	++++	++++
Human surveillance	+	+	++++	-	-	-	++++

Source: [7].

Research of the drone detection by means of different thermal imaging systems (infrared sensors) and development original thermal image enhancement algorithm for infrared scanner system is presented in the paper [8]. Main features of an infrared image, which are not occurring in case of visual images, are relatively low spatial resolution, low image contrast, presence of noise pattern or pulse disturbances.

The proliferation of LSS flying platforms brings with it a new and rapidly increasing threat for national defence and security agencies. Thus, defence systems must be designed to face such threats. Modern operational readiness bases on proper personnel training that is performed on high fidelity simulators. The aim of the paper [9] is to take into account the variety of the commercially available LSS aerial vehicles and to define LSS models from different points of view. The LSS can be modelled with respect to the behaviour during the flight and the user interface, signature against different type of detectors, and threat itself and the defence tactics.

While the technology for operating a single UAV is rather mature, additional efforts are still necessary

[4] Very Short Air Defence.

[5] Except SWIR (Short-wavelength infrared).

[6] Electronic support measures.

for using UAVs in fleets (or swarms). The Aid to SItuation Management based on MUltimodal, MUltiUAVs, MUltilevel acquisition Techniques (ASIMUT) project aims at investigating and demonstrating dedicated surveillance services based on fleets of UAVs. The goal is to enhance the situation awareness of an operator and to decrease his workload by providing support for the detection of threats based on multi-sensor multi-source data fusion. The operator is also supported by the combination of information delivered by the heterogeneous swarms of UAVs and by additional information extracted from intelligence databases. As a result, a distributed surveillance system increasing detection, high-level data fusion capabilities and UAV autonomy is proposed [10].

The summary of the literature review:

- New problems with the fight against UAS are caused by technology progress in the development of the commercial drones.
- UAVs are available to the population without any problems; UAVs can be used in war, crisis situations, and they can be misused by criminal and terrorist entities.
- Areas of threats and defence include air surveillance, command and control, and target elimination.

3 OVERVIEW OF OF-THE-SHELF AND PROFESSIONAL UAVS

The market is full of various UAVs categories. These machines can be equipped with various accessories based on their size, weight and battery capacity. Digital cameras are usually used for collecting information, but UAV can be geared with a lidar, a radar, a thermal camera or other sensors. UAVs can be also equipped with attached explosives or primitive drop mechanism, which release an explosive. UAVs can be also used for transporting a non-lethal cargo, mostly illegal (e.g. drugs, cigarettes and other contraband).

Size based classification of UAVs may differ in regions. The previously mentioned Attachment X [1] defines these categories based on their maximum take-off weight:

- ≤ 0,91 kg,
- 0,91–7 kg,
- 7–25 kg,
- > 25 kg.

The NATO uses slightly different classification, see Table 1.

Very similar UAVs classification is used in the paper called Multispectral Detection of Commercial Unmanned Aerial Vehicles:

Table 3 UAV Classes

Category	Range [km]	Altitude [m]	Operational time [hours]	Weight [kg]
Nano	< 1	< 100	< 1	< 0.025
Micro	< 10	< 250	1	< 5
Mini	< 10	< 300	< 2	< 25

Source: [3].

One other UAV classification:

Tab. 4 UAV type by usage

UAV Type	Price [€]	Video [px]	Flight Time [min]	Range [km]	Purpose
Amateur	< 200	1280x720	< 15	< 0.1	ISR[7]
Professional	> 800	4096x2160	< 30	< 8	ISR[7] + A[8]
Race/Custom	various[9]	4096x2160	< 30	< 4	ISR[7] + A[8]
Military[10]	> 4000	4096x2160	various[11]	various[12]	ISR[7] + A[8]

Source: [3].

3.1 UAVs for information collection

The author picked different size UAVs from the most known e-shop in the Czech Republic. The regulations don't require any failsafe system on these machines. This failsafe system would end the flight in the case that the communication between UAS and control station would be interrupted. Some of the representatives in this category can have a return command to the default position in their communication protocol. This command could be used in the taking over type of attack, because this command is usually standardized.

UAS created by the DJI company usually contains restricted areas, which are forbidden for UAVs to flight into. These forbidden zones are managed by the DJI company, which creates them based on data from the national authorities. The restricted zones can change during the time, so they are available online [12]. The company defines also a "Warning" zones, which can be entered after confirming that you really want to enter this zone. Next zone categories are Restricted and Authorization. Flight into these zones has to be permitted by the local authorities. In this case some type of UAV's registration has to be done.

[7] Intelligence, surveillance and reconnaissance – information collection.

[8] Attack – deliver explosive payload.

[9] Can start at 100 € and be up to thousands of €.

[10] These UAVs are usually out of the legal framework of Attachment X. It is a very wide group of UASs, which can be autonomous, which can cooperate in a swarm, etc. Planning of protection against this type of UAV is far beyond of this article purpose. So, they will not be further discussed.

[11] Larger UAVs can flight up to 24 hours. More advanced concepts with unlimited flight time are also in the development [11].

[12] These UASs are not limited thanks to a satellite communication between UAV and control station.

3.1.1 Syma X5SW PRO

Syma X5SW PRO [13] was in the model row SYMA X5C recommended [14] as the most suitable for the information collection. Like all X5C UAVs contains a 6-axis gyro for flight stabilization. It also contains HD camera with resolution 1280 x 720 px with ability to display a video stream on the smartphone. Flight time depends on the battery and it can be up to 20 minutes. Range is up to 100 m, which is very nice distance in the category of very cheap UAVs. According to the records available online, the video is not very good, but it still can be used for gathering some information. Control SW contains home return functionality.

3.1.2 DJI Mavic Air

DJI Mavic Air is very cheap representative of professional UAVs. But despite its low price it can offer a very good service to the potential attackers. Camera itself (not just the UAV's body) has a 3-axis stabilization and it supports a 4k video stream. With the weight of 430 g is still categorized as a Micro. Flight time is up to 21 minutes and with moving operator can flight up to 10 km on one charge. Maximum flight speed is up to 68 km/h. The UAV also contains a sensing system to avoid obstacles. This sensing system reduces maximum flight speed to 28 km/h. Control SW contains return home functionality. If the radio connection between UAV and control station is interrupted, the UAV will retrace its original flight route, until the connection is restored.

3.1.3 DJI Mavic 2 Enterprise (DUAL) Universal Edition

DJI Mavic 2 Enterprise (DUAL) Universal Edition [15] is the most equipped commercially available UAV[13]. The camera has a 3-axis stabilization and supports 4k videos as well. The UAV is also equipped with the Radiometric FLIR thermal sensor. The operator can have 3 types of imagery data – FLIR MSX, infrared spectrum or visible light spectrum. This provides whole new dimension of the information collection. The UAV can be equipped with the speaker, light or safe flight beacon. The discrete mode allows the operator to switch off the LED lights and make a hardly detectable night reconnaissance. An open terrain range is up to 8 km. The UAV was at first place designed for professionally usage – army, police, searching for persons in hardly accessible terrain, mass or natural disasters, energetics, telecommunications (mass inspections) [16]. But it is possible to buy it without any restrictions and potential attacker can gain very powerful tool for gathering information.

Table 5 UAVs for collecting information

UAV	Weight [g]	Size [mm]	Range [m]	Video Resolution	Price [€]
Syma X5UW PRO	967	320x70x320	100	1280x720	93
DJI Mavic Air	430	83x49x168	8000	4096x2160	860
DJI Mavic 2 Enterprise	910	322x224x114	8000	4096x2160	3000

Source: [3].

3.2 Direct attack UAVs

This article will not consider professional military UAS, as it was mentioned before. Due to the clear illegal intentions of usage are these UASs not commercially available. But it is not so hard to build an armed UAV by using two slightly different ways. Attacker can just attach a weapon or explosives to an off-the-shelf UAV; or the attacker can create a completely new UAS from obtainable components. This type of UAS was intentionally not mentioned before, but this does not mean, the attackers can't create a customized UAV platform, equip it with a stabilization mechanism, quality 4k camera and collect information with it.

3.2.1 Building custom UAV platform

How to build a custom UAV tutorials can be very easily found on the Internet, i.e. [17], [18]. These tutorials are very complex and skilled man is able to build this UAV. The custom UAV community is very open and a desperate builder can seek an advice there.

At first you have to choose a size of the UAV. Bigger size and thus payload are better for attack with explosives. It is possible to use online calculator [19] to verify, that designed UAV is flight-capable. This calculator also provides some expected flight characteristics based on many variables (number of rotors, type of motors, propellers size, battery capacity, etc.). With the help of tutorials, the designer is able to design the UAV core and then add weight and simulate size of the explosive payload. It is also possible not to attach a camera and increase an explosive payload. After this research it is possible to order the needed or recommended components and assemble the UAS.

3.2.2 Attaching explosives to UAV platform

Off-the-shelf UAVs usually have more power than it is needed for flight. Because of this the UAVs gain better flight performance and they are more

[13] In the most known e-shop in the Czech Republic.

attractive for the customers. So why not to utilize this fact and attach an explosive or a grenade to a UAV? This tactic was used by some extremist groups during the fights in Syria. Members of these groups attached grenades, mortar's ammunition or other explosives and dropped them with high accuracy thanks to a camera targeting [20].

The author conducted very simple experiment with 'obsolete' DJI Phantom 4 Pro [21]. A cargo of 350 g was attached to the UAV with weight of 1388 g and the UAV took off without any problems. But the not well-designed shape of the cargo caused minor problems with manoeuvrability during the flight and serious problems during landing. Control electronics was not able to deal with moved centre of mass. But landing is not the biggest issue during the 'suicide' or 'bombing' types of UAV attack. Some other sources, e. g. [22] presents safe payload weight about 462 g (1.02 lbs.) for DJI Phantom 4 Pro.

4 DETECTION AND IDENTIFICATION OF UAVS

Fully automated detection and identification is very complicated issue at the present state of art. Because of it, in the article it will be discussed detection and identification made by sensor's operators, or done in the integrated UAS protection solution. Any complex protection system against small UASs must be strictly modular, to allow easily upgrade individual parts and to improve detection capabilities.

The DJI company can offer a device that is capable of detect and identify most of the commercially available UAS [23]. The device uses a knowledge of the communication protocol used by UAS created by this company. The manufacturer presents an arbitrary range up to 50 km in stationary deployment and identification time from 2 seconds.

Types of sensors, which can be used for UAS detection and identification will be discussed in the next section.

4.1 Radar

Radar represents proven type of detection large flying objects. Various wavelengths were tested during time and now it is possible to manufacture a radar capable of small objects detection, with reflection surface just hundredths of square meter. In [3] was conducted a laboratory and field experiment with very interesting results. It is very unfortune, that most of these results are very sensitive and were not published by the authors.

Radar is best for long range detection, up to 30 km. Various manufacturers presents these instrumental ranges usually more optimistic than the real results.

However, this way of detection is not always precise and false detections may occur time to time. The reason is the size of a small UAV is very close to the size of larger birds.

4.2 Radio

Radio wave detection is relatively easy. The following radio spectrum analysis as well. Unlicensed Wi-Fi bands at 2.4 GHz or 5.6 GHz are used for commercial UAVs control. The communication is done by various protocols. A communication protocol of LTE mobile networks is very often used, but in the unlicensed Wi-Fi bands. It is because of its jamming resistance and better transmission properties than classical Wi-Fi protocol.

Off-the-shelf and racing UAVs are not usually autonomous and they use 2 radio channels. One for control signals and telemetry and the other with wider bandwidth for video stream from a digital camera attached to the UAV. This fact allows to detect and target the control station of UAS.

Identification of the UAS can be a problem. Operator has to analyse collected data from the control and telemetry channels, which is almost impossible in real-time.

4.3 Optics

UAVs automatic detection with digital cameras is great challenge for the image analysis specialists. At the time there are several systems, which declare an ability to detect a UAV in the field of view of the camera in the very few seconds. But these systems are not enough reliable and they are quite expensive.

More suitable approach of using optical sensors is using them for detection confirmation of other types of sensors. This confirmation can be easily and cheaply done by an operator. It is very easy to install a remote-controlled rotatable mast with set of cameras. The mast can be semi-automated controlled by the control system and an operator. The control system points the camera based on the information from other sensors and operator can adjust the parameters and then confirms the detection of a UAV. It is also possible to use the mast without connection to any sensors and to be controlled only by the operator.

It is not necessary to use only stationary cameras installation on the masts. Portable cameras equipped with GPS and laser range-meter can be connected to the command and control system and they can provide reliable detections as well.

4.4 Acoustics

Success rate of an acoustic detection depends on the area, where this type of sensor will be used. It is possible to detect UAVs with network of microphones, because of the limited range of this type of sensor. Yet microphones can be very cheap and easy to use.

It is also possible to use audio sensors to identify specific type of UAV [24] discussed possibility of using the Linear predictive coding (LPC) for UAVs detection and identification. The LPC uses sound samples and creates a numeral representation of the sound signature. It is possible to distinguish various types of sound sources, such as a truck, a gun shot or certain types of UAVs. But all of this is limited by the range of an acoustic sensor and its surroundings. Defence can contain many cheap sound collectors, but it should not be the only way of detecting UAVs.

5 ELIMINATION

UAV elimination is the last phase of the whole UAS defence. There are basically two ways of UAV elimination: Lethal and non-lethal with jamming. Both ways have their pros and cons, so there is no all-time right way of UAV elimination.

5.1 Non-lethal elimination

Non-lethal elimination is done by jamming radio control channel or by spoofing the positional data.

An interesting way of protecting the Russian president Vladimir Putin appeared recently. Russian security service uses GPS spoofing at places, where the president occurs. A non-profit organization C4ADS from the USA discovered from public data, that ships from certain waters moved to a land airfield approximately 200 km from the sea. This strange ship movement was done by transmitting false GPS coordinates which corresponds to the coordinates of nearby airfields to deceive commercial UAVs position restrictive systems. Because most of the manufacturers put into their UAVs restricted areas, the UAV is not able to fly in the area.

This way of protection can be effective against commercial UAVs, but it is ineffective against professional military UAVs with inertial navigation.

The GPS spoofing can also be very dangerous for any civilian GPS users. Many systems and people rely or even depend on the accurate position and time from GPS. In the piece time this type of protection can do more harm than good, especially in the Central Europe.

Decipherment of UAS's communication protocol and following take over can be another way of UAV elimination. This approach itself is on the edge of the law, because you have to decode a communication protocol with reverse engineering, which can be a violation of the EULA[14]. Big number of manufacturers and incompatibility between various UASs represents another disadvantage of this approach. Additionally, communication protocols change and evolve during time, so there is a time lack between launching a new UAS and gaining an ability to take over this new UAS.

Last conventional way is jamming the whole radio spectrum used for control channel. This is again usable only for a certain category of UASs. Again, it is on the edge of the law[15]. But this can be a way, how to eliminate unwanted UAVs from the protected area.

Big advantage of using a non-lethal elimination is the fact, that it can be used in densely populated areas, including cramped spaces in the cities. Lost of the UAV's control or fall of the UAV can only do any damage to the public or private property or harming people.

5.2 Lethal elimination

Lethal elimination is an ordinary usage of brute force to end a flight of the UAV. The best way is by damaging or destroying rotor blades. Only a slight damage can make worse the flight characteristics and manoeuvrability. The most suitable for this is using shotguns with many projectiles. This rises the probability of hitting a rotor blade. An experienced shooter should be able to hit a UAV flying at low altitude.

Using firearms at peace time is very controversial. Especially in the densely populated areas. A risk of collateral damage to a public property or human lives is too high there. So, this is the reason, why using firearms should be permitted only on very special cases and not in the cities or populated areas.

6 CONCLUSION

Protection of any area against small UAVs is very complex task. There is no "silver bullet" which will protect any possible area. It is necessary not only reflect the specifics of the protected area during the defence planning process, but it is vital to define the UAV threat type to which the defence should be effective.

A defence against small UAVs would have very different characteristics than defence against professional military UAVs, or swarms of these UAVs. This article focused on a single, or small number of UAVs, not swarms of cooperating UAVs.

The type of attack is also very important to decide. Should be the defence effective only against directly attacking UAVs with firearms or explosives, or even against an information collecting UAVs? Should be effective against high flying UAVs or low flying UAVs? These questions determine sensors and effectors usage.

Next question should be the assumed amount of losses during a successful attack. As a successful attack can be considered also a collecting and mining the information, especially on soft targets. These

[14] End-User License Agreement.

[15] Czech telecommunication office, the radio spectrum authority in the Czech Republic, would not be pleased, if the unlicensed band is being jammed for any time.

targets can be attacked with bigger impact after profound reconnaissance. This again affects the types of sensors and their quantity.

Another variable is concrete surroundings and ability to choose an elimination method. It is hard to say, which of the presented ways is less complicated or doable. Each of the approaches has its advantages. Using firearms is very limiting in populated areas, so they should be used only in uninhabited areas. If the UAV would quickly manoeuvre and the firearm operator would not be careful enough, there is very high risk of damaging the surroundings or harming any nearby people.

The primary task is detection using multispectral, multilevel, multimodal, and multisensory strategy in a fight against small UAS. The effective basis for the UAV detection is the multisource data fusion. The modelling and simulation are the often-used research methods, how to prepare and design any counter UAV protection and should be used for validating the design before building any defence system.

References

[1] Řízení letového provozu ČR: *Doplněk X – Bezpilotní systémy* [online]. [cit. 26. 4. 2019] Available at: https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-2/data/effective/doplX.pdf

[2] NOVÁK, V.: *Předpisy pro létání s drony v ČR*. [online] [cit. 26. 4. 2019] Available at: http://www.droneweb.cz/legislativa-provozu-dronu/item/37-predpisy-pro-letani-s-drony-v-cr

[3] FARLÍK, J., KRÁTKÝ, M., CASAR, J., STARÝ V.: *Multispectral Detection of Commercial Aerial Vehicles.* Sensors (Basel, Switzerland), 19(7), 1517. doi:10.3390/s19071517, pages 1–28. Available online at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6480366/pdf/sensors-19-01517.pdf

[4] KRÁTKÝ, M., FARLÍK, J.: *Countering UAVs – the mover of research in military technology.* Defence Science Journal. 68. 460-466. 10.14429/dsj.68.12442.

[5] TIAN, Y., WANG, Z., HIANG, Q.: *UAV Remote Control Signal Analysis based on GNU Radio and USRP X310.* Pages 2502-2506. 10.1109/IMCEC.2018.8469271.

[6] DAVIES, G., HORTON, H., JOSHI, A.: *Gatwick Drone Chaos Continues into a Third Day.* [online] [cit. 26. 4. 2019] 2018. Available at https://www.telegraph.co.uk/news/2018/12/20/gatwick-chaos-drones-cause-flights-cancelled-live-updates/.

[7] WELLING, P., SPEIRS, P., SCHUEPBACH, C., BOENIGER, U., PRATISTO, H.: *Radar systems and challenges for C-UAV.* 2018 19th International Radar Symposium (IRS), Bonn, 2018, pp. 1-8. Online ISBN: 978-3-7369-9545-1.

[8] SOSNOWSKI, T., BIESZCZAD, G., MADURA, H., KASTEK, M..: *Thermovision system for flying objects detection.* 2018 Baltic URSI Symposium (URSI), Poznan, 2018, pp. 141-144. Online ISBN: 978-8-3949-4213-7.

[9] PROIETTI, P., GOLDIEZ, B., FARLÍK, J., Di MARCO, B.: *Modelling and simulation to support the counter drone operations (NMSG-154).* Lecture Notes in Computer Science 10726, 2018. Pages 268–284. Online ISBN: 978-3-319-76072-8.

[10] BOUVRY, P., CHAUMETTE, S., DANOY, G. ROSALIE, M. SANDER, J.: *Using heterogeneous multilevel swarms of UAVs and high-level data fusion to support situation management in surveillance scenarios.* 2016 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems (MFI), Baden-Baden, 2016, pp. 424-429. Doi: 10.1109/MFI.2016.7849525. Electronic ISBN: 978-1-4673-9708-7.

[11] JOHN, R.: *Dron Phoenix: Pseudosatelit s neomezenou délkou letu.* [online] [cit. 7. 5. 2019]. Available at: https://www.armadninoviny.cz/dron-neomezenou-delkou-letu.html.

[12] *Geo zone map.* [online] [cit. 7. 5. 2019]. Available at: https://www.dji.com/cz/flysafe/geo-map.

[13] *DRON SYMA X5SW PRO.* [online] [cit. 7. 5. 2019]. Available at: https://www.rcprofi. cz/poradna/srovnani-verzi-dronu-syma-x5c.

[14] *Srovnání jednotlivých verzí dronu SYMA X5C.* [online] [cit. 7. 5. 2019]. Available at: https://www.rcprofi.cz/poradna/srovnani-verzi-dronu-syma-x5c

[15] *DJI Mavic 2 Enterprise (DUAL) Universal Edition.* [online] [cit. 7. 5. 2019]. Available at: https://www.alza.cz/dji-mavic-2-enterprise-dual-universal-edition-d5548224.htm.

[16] *Mavic 2 Enterprise.* [online] [cit. 7. 5. 2019]. Available at: https://www.dji.com/cz/mavic-2-enterprise

[17] *How to build a drone|Step by step guide.* [online] [cit. 25. 5. 2019] Available at: http://dronenodes.com/how-to-build-a-drone/.

[18] CARTER, J.: *How to build your own drone for $99.* [online] [cit. 25. 5. 2019]. Available at: https://thedronegirl.com/2018/05/06/build-your-own-drone/.

[19] *xcopterCalc – Multicopter Calculator.* [online] [cit. 25. 5 2019], Available at: https://www.ecalc.ch/xcoptercalc.php.

[20] GIBBONS-NEFF, T.: *ISIS drones are attacking U.S. troops and disrupting airstrikes in Raqqa, officials say.* [online] [cit. 25. 5. 2019]. Available at: https://www.washingtonpost.com/news/checkpoint/wp/2017/06/14/isis-drones-are-attacking-u-s-troops-and-disrupting-airstrikes-in-raqqa-officials-say/

[21] DJI: *Phantom 4 Pro.* [online] [cit. 25. 5. 2019] Available at https://www.dji.com/cz/phantom-4-pro.

[22] Dronethusiast.: *5 best heavy lift drones [2019]- large drones that have high lift capacity.* [online] [cit. 25. 5. 2019] Available at: https://www.dronethusiast.com/heavy-lift-drones/

[23] *DJI Aeroscope.* [online] [cit. 26. 4. 2019], Available at: https://www.dji.com/cz/aeroscope.

[24] VILÍMEK, J. BUŘITA, L.: *Ways for copter drone acustic detection.* ICMT 2017, pages 349-353. Online ISBN: 978-1-5090-5666-8.

Mgr. Jakub **VILÍMEK**
CIS Department
University of Defence Brno
and URC Systems Brno
Kounicova 65
662 10 Brno
Czech Republic
E-mail: jakub.vilimek@urc-systems.cz

Jakub VILÍMEK - is a software developer in the company URC Systems in Brno. He is a Ph.D. Candidate of the Faculty of Military Technology at University of Defence in Brno. His dissertation thesis is focused on planning defence system against the small UAV threats. He was part of the solvers team for the project SIMULEB - Simulator of command and control systems radio networks of defined combined brigade units for EW units training. The main aim of this project was to develop the SW tools for training of CZE Army EW specialists which includes SW simulator for modeling of "clasical" and sophisticated radio networks and communications of the combined task forces up to brigade level.

COOPERATION BETWEEN EU AND THE USA IN THEIR POLICY TOWARDS RUSSIA

Marek HARGAŠ

Abstract: The article is focused on the legislative and institutional background of the mutual cooperation of the EU and the USA within their policy framework towards Russia. It also briefly points out the use of sanctions as one of the main tools.

Keywords: European Union; USA; Russia; Sanctions; Security.

1 INTRODUCTION

At the end of the 2nd decade of the 21st century it seems that the so-called „unipolar“ world development being characterised by a global dominance of one superpower – the USA – is threatened. The globe has to deal with a range of political, economic and social issues together with security problems inevitably linked to them. The new global or regional powers try to break the dominance of the USA.

One of the challenges for the West – as we traditionally label the transatlantic area plus Australia and the New Zealand - is an undoubted increase of power of the „non-west“ countries. Another, and obviously a hotter, question is the relationship between the EU and the USA, as the representatives of the western civilisation on the one hand, and Russia, as the new and old power, on the other hand.

2 BASIC FRAMEWORKS OF THE EU POLICY

The Common Foreign and Security Policy (CFSP) had been created by the Treaty on the European Union, while the CFSP was the second from the three pillars on which the inception of the EU was established. The Lisbon Treaty, which had entered into force in January 2009, formally confirmed not only the legal status of the European Union and institutional means for its foreign activity but, at the same time, removed its pillar structure. Several key players entered the CFSP area, inter-alia, the post of the European Union representative for foreign affairs and the security policy who is the Deputy Director General of the Commission and the post of a permanent President of the European Council. Since 2012, the European Parliament and the Parliaments of Member States have been organising inter-parliamentary conferences, where the issues related to CFSP are mutually discussed.

On 28 June 2016, the High Representative for Foreign Affairs and Security Policy Frederica Mogherini submitted a global strategy for foreign and security policy of the EU [1]. The global strategy is particularly focused on 5 areas: 1) security of Union, 2) stability of states and communities to the East and South of Union, 3) integrated approach to conflicts, 4) cooperative and regional arrangement, 5) global management to be used for the 21st century. By its adoption a revision of sectoral strategies, together with the inception of thematically and geographically new strategies, occurred. During 2017, a report on the performance of global strategy was released where the progress in terms of cooperation with NATO was highlighted and the Parliament issued an annual report [2] on the pursuance of CFSP, where the common judgement of threats and a joint approach on their solution was stressed.

The Lisbon Treaty also strengthened the Common Security and Defence Policy (CSDP), which is an integrated part of the CFSP. The main institutional role was taken over by the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, who chairs the Foreign Affairs Council. Its members are foreign ministers. Parliament organises discussions and seminars on, inter alia, the topic of international crises with security and defence implications, and multilateral frameworks on security issues.

3 FOREIGN POLICY OF THE USA AND EU TOWARDS RUSSIA

Within the course of recent years the relationship between the USA and Russia has become one of the top priorities of the U.S. foreign policy. The American political representatives are aware that they should neither overvalue nor undervalue the ability of Russia to influence or distort the American national security planning. The relations between both countries are too deep and interlinked to take lightly such problems as the interventions in Syria, Ukraine or the nuclear weapons cut-off.

With reference to Wallin [3], there are several main areas the U.S. foreign policy should be focused on. One of them is the membership in NATO. The Member States committed themselves to spend 2% of GDP on defence, what causes difficulties to some of them and are therefore heavily criticised by the USA. In addition to the USA, only six NATO Member States exceeded 2 % of GDP on defence in 2018, namely Greece, Estonia, United Kingdom, Latvia, Poland and Lithuania, as stated in the press release published by NATO Public Diplomacy Division on 14 March 2019.

Another domain is the nuclear weapons issue. Despite the fact that the USA and Russia are aware of the importance of programme on the diminishing of the number of ballistic missiles, they consider each other as a nuclear threat. In particular, Russia considers whatever technology in the field of nuclear weapons developed in the USA as a threat directed against the Russian Federation.

The cyber security is another domain, which is considered by the USA very intensively. The reason lies in several hacker attacks from Russia, China and other countries. Officially Russia disavows these activities of any kind. On June, President Putin said that the Russian government did not play any role in terms of hacker attacks during the US elections in 2016, however, at the same time he declared that „*as long as some Russian citizens are thinking patriotically, they start to organise on their own will - what is according to their opinion appropriate – different activities against those, who have addressed bad things on Russia*" [4].

Another challenge for the USA is to cope with the increasing number of regular incidents on sea and in air caused by Russian mariner and aviation powers. The incidents are frequently accompanied by a dangerous and provocative behaviour what, at the end of the day, could lead to casualties on all sides involved. The Treaty between the USA and the Soviet Union as of 1972 is out of date and Russia is not abiding by its terms. Both, the revisiting of this issue and the creation of exact mechanisms for diminishing the tension escalation are echoed in the USA.

The USA and the European Union do not coincide in all foreign policy questions, however, they still remain the most important allies. Nonetheless, their mutual cooperation is long-term, e.g. the contacts between the Parliament and the US Congress went down to 1972. These relationships had been institutionalised in 1999 and the Institute of Transatlantic Legislator's dialogue was created. The last, 82nd inter-parliamentary meeting was in 2018 in Sofia, Bulgaria. The importance of this Institute is growing mainly by the authority of the US Congress when approving the interventions of the USA during the world crises and influencing the US activities within the global administration institutions. With regard to the key role of NATO when ensuring the European security, the EU Parliament is also participating in the plenary meetings of NATO.

Although the attitude of the USA towards EU and the transatlantic alliance has changed since the accession of Donald Trump to the Office of President, it returns into a constructive mode. For example, the negotiations on the Transatlantic Business and Investment Partnership between the USA and the EU, which had begun in July 2013, were interrupted after the election of President Trump. The situation is even more complicated due to the fact that in 2017 the USA were the main export market of the Union and that EU and the USA are mutually the biggest investors. However, in terms of security the partnership covered by the cooperation of allies within NATO is ongoing.

The representatives of the EU are aware of Russian ambitions and a complicated relationship between both parties. As one of the steps for a better security assurance of the EU countries, a so called Permanent Structured Cooperation (PESCO) [5] has been established. It is to be considered as a reinforced cooperation of 25 EU member States in the field of security and defence, which have committed themselves to take over more duties and criteria in order to comply with the EU ambitions resulting from the Global strategy for the foreign and security policy of the EU. The level of defensive capabilities of particular countries should be increased and harmonised in order to achieve a better cooperation in the fulfilment of goals. In addition to the security of citizens living in the EU member states, the members of PESCO committed themselves also to a more active participation in the EU operations focused on the support of worldwide peace and security. The participation in PESCO is voluntary and the defensive capabilities remain in the ownership of the EU Member States involved, thus, it has no impact either on the state sovereignty or on the security and defence policy of some of them.

PESCO contains 20 commitments [6] which are common for all EU Member States involved. They are focused on the increase of national expenditures on defence and the reinforcement of cooperation of these states in the areas of harmonisation of defence planning, increase of military forces deployment, removal of critical abilities and the performance of multinational projects. The participating countries of the EU have prepared the national plans of PESCO pursuance, which are to be upgraded annually and which contains the way how and in which time intervals the commitments will be jointly fulfilled.

National pursuance plans will be submitted by Member States to the European External Action Service (EEAS) and to European Defence Agency (EDA). EEAS and EDA will provide administrative and technical support for the EU Member States involved. The High Representative for Foreign Affairs and Security Policy, who leads the EEAS and the EDA simultaneously, will provide the ministers of foreign affairs and the ministers of defence with an assessment report on the PESCO pursuance state of play, including the fulfilment of commitments of each EU Member State according to its national pursuance plan. In practice, the assessment report will compare the content of national pursuance plans of particular EU Member State involved with the actual state of play. In case of non-fulfilment of joint commitments, the EU Member State could be excluded from PESCO.

As it has been mentioned above, the multinational projects focused on the creation of defence capabilities and their use in the joint EU missions are also part of PESCO. Making these projects feasible should lead to the strengthening of the strategic EU autonomy in the field of security and defence and their ability to react to crises. On 11 December 2017, the participating EU Member States had released a declaration of the PESCO projects [7], by which they announced the first wave of projects pursued from 2018. 17 projects have been selected into the first phase from 49 proposed projects, among them also a Slovak project EuroArtillery being intended for an indirect fire support.

PESCO should help also to the strengthening of the so-called European Pillar of NATO, by the means of which the EU Member States, which are simultaneously the NATO Member States, confirm that NATO with its collective defence principle remains the main security guarantee. At the same time, they repeatedly declare the cohesion of their security and defence with those EU Member States which are not NATO members.

4 RUSSIA – „THE NEW AND OLD GREAT POWER“

After the collapse of the Soviet Union, the rising Russian Federation must cope with the enormous, literally, subsistence issues. The former obstructers from the cold-war times began to consider Russia as a second-rate power, mainly due to its big losses in terms of military power and capabilities. All the more the EU and USA were shocked by observing the Russian intervention to Ukraine and Syria. Despite the fact that Russia is economically relatively less powerful, militarily it regains its lost position. To compare, GDP of Russia in 2017 was only by 12 % higher than the joint GDP of Belgium and Netherlands. In 2017, the military expenditures amounted to 61 billion USD. The USA spent approximately 10 times more during the same time period. However, it has to be mentioned, that a simple comparison of military budgets does not perfectly reflect the reality. Whereas Russia buys prevailingly on the domestic market often from government producers, it pays lower price as compared to the majority of other states on the world market. Another difference is visible in the ratio of expenditures on wages of military employees and on purchases of new military equipment. While in NATO Member States approximately 80 % from the budget on defence goes to wages, in Russia this ratio is 50 : 50 [8].

One of the factors supporting the Russian Federation's powers is the nuclear arsenal. According to Rumer [9], the Russian military strategists rely on the nuclear potential of their country and the ability of Russia for a second strike is considered as inevitable. They react also to the attitude of the US President D. Trump who in February terminated the participation of the USA in the Intermediate-Range Nuclear Forces Treaty (INF) [10]. Immediately on the next day the Russian President V. Putin declared that Russia terminates its participation in the Treaty as well.

All three parties involved (EU, Russian Federation and the USA) are concurrently accusing themselves from the abuse of the airspace by the aircraft of the „opponent“. Above the international air space, the Russian long-range bombers and multipurpose combat aircrafts meet the NATO airplanes, which watch over, for example, the Baltic sea; however, the incidents occur also at the coast of United Kingdom or Canada and the USA. The incident of Ukraine ships being blocked and captured by Russian Navy at the coast of Crimea, annexed by Moscow, was heavily criticised by the EU.

For more than a decade, the increasingly aggressive demonstrations of Russian policy in different forms can be observed. Alleged attempts to meddle into the election processes of democratic countries done by Russia are not new phenomena but their methods have changed. In recent years Russia directly financed the political parties which should deteriorate the situation in concrete countries [11]. The expansion of NATO and American military troops, together with the missile shield, represent a traditional stumbling block between West and the Russian Federation. Inter alia, the Russian Federation reacted also by the deployment of sizeable military equipment in Crimea being unlawfully occupied. The USA, EU and their allies have been forced to respond to these steps in order to prevent the escalation of tension.

5 ECONOMIC SANCTIONS POLICY OF THE USA AND EU TOWARDS RUSSIA

Since the end of cold war, the sanctions have become a popular tool, especially for the USA (Illieva, Dashtevski, Kokotovic 2018). The European Commission considers the sanctions as one of the EU tools for supporting the goals of Common Foreign and Security Policy too. There are several forms of sanctions. The military ones (use of military forces), political or diplomatic or cultural sanctions could be in question. The economic sanctions represent a relatively new phenomenon in the international affairs, nevertheless in the 20th century they occurred relatively often. In general, they are focused on the prevention against the delivery of goods and services, funds or know-how to a concrete recipient.

In March 2014, the EU imposes sanctions focused on the prohibition of travelling and freezing of financial means of concrete persons. It was a reaction to the annexation of Crimea and Sevastopol to Russian Federation, which was considered by the EU as a sovereignty threat for Ukraine.

Another impetus for economic sanctions of EU against the Russian federation was the military conflict in Ukraine. In July 2014, the EU adopted a Decision 2014/512 of the CFSP Council on restrictive measures with regard to the activities of Russian Federation, by which it had destabilised the situation in Ukraine. The USA, EU, Japan and Australia imposed economic sanctions on Russian official representatives, firms and private persons. Illieva, Dashtevski, Kokotovic (Illieva, Dashtevski, Kokotovic 2018) have concretely identified what EU has focused on and separately what the USA have targeted on.

EU sanctions are targeted on:

- individuals or legal entities who have been involved in actions undermining or threatening the territorial integrity, freedom and independence of Ukraine and their property is frozen in the EU;
- restrictions and afterwards a complete ban of import of goods originating from Crimea or Sevastopol to the EU, as a response to the illegal annexation of Crimea and Sevastopol;
- economic sanctions against Russia restricting the use of EU financial markets and a prohibition of export of armament and goods of duplicitous use, furthermore of equipment and services related to the oil industry.

On the other hand, the US sanctions are related to [12]:

- property freeze of concrete persons (close to President Vladimir Putin) and the prohibition for physical persons and legal entities from the USA to carry out whatsoever financial transactions with the sanctioned persons;
- property freeze and a prohibition to perform economic transactions with concrete entities especially with the banks owned by the government, defensive and energetic firms
- restrictions related to financial transactions with Russian firms belonging to key sectors, i.e. defence, energetic, financial);
- restrictions on export of technologies related to oil and goods of duplicitous use;
- restrictions related to specific export (e.g. military goods).

As retaliatory measures against EU, the USA, Canada, Australia and Norway, the Russian Federation introduced tools hampering import of three goods and services – vegetables and fruit, milk products, meat and meat products. In addition, it has to be mentioned, that a list of countries which had joined the EU and USA was extended in 2015 by Japan, Switzerland, Albania, Iceland, Lichtenstein and Monte Negro.

According to Korhonen, Simola and Solanko (Korhonen, Simola, Solanko 2018), the economic crisis, which broke out fully in 2015, has only very little to do with sanctions from the USA and the EU. The origin must be sought in the sharp drop of oil prices what has had a significant impact on the Russian economy.

Illieva, Dashtevski, Kokotovic (Illieva, Dashtevski, Kokotovic. 2018) pointed out that if the economic sanctions are to be effective, especially in the country where the political elite, headed by the President, has the media in power, it will be necessary to have a clear transmission mechanism at disposal, which might appropriately force the Russian electors to vote for an alternative solution. The main reason why the majority of UN Member States is against the sanctions imposed on Russia is the fact that instead of solving one problem (Crimea), they have caused the creation of other problems. The authors also emphasise that there is no international organisation or generally accepted mechanism, which is authorised to govern the legality of these sanctions. There is even no definition of economic sanctions in international law, so their illegality is often the subject of debate.

6 MILITARY MEASURES AND THE COOPERATION BETWEEN THE USA AND THE EU WITHIN THE FRAMEWORK OF NATO

The incidents as of the end of 2013 and the beginning of 2014, and especially the annexation of Crimea by Russia, led to concrete steps of the NATO Member States. Within the summit in Wales, they adopted, among the other things, the implementation of the Readiness Action Plan and the reinforcement of the collective defence and the Eastern wing of NATO. In the next summit in Warsaw in 2016, further decisions were adopted in order to strengthen the positions of NATO especially on the Eastern border of Alliance. Alliance defense ministers confirmed the creation of four multinational combat groups as part of a forward presence program (Enhanced Forward Presence) [13]. These battle groups consisting of soldiers from different countries are deployed in the area of Poland, Lithuania, Latvia and Estonia and their total number represents more than 4 500 soldiers and civilians.

The groups cooperate with the local military forces, however, they still fall under the leadership of the Alliance through the so-called Multinational North-East Corps [14], based in Poland in Szczecin.

The Estonian Armed Forces cooperate with a battle group led by the United Kingdom based in Tapa. This group consists of British troops, Danish soldiers and Icelandic civil servant responsible for the management of communication systems.

A Canada-led military group is located in the Latvian city Adazi and consists of Canadian troops, soldiers from Spain, Italy, Poland and 50 soldiers from Slovenia, as well as from the military service of the Czech Republic, Albania and Monte Negro. In 2018, the Slovak Republic sent 150 soldiers to Latvia.

The base of the battle group led by Germany is in the Lithuanian city of Rukla. It involves soldiers from Germany, France, Croatia, the Netherlands and military personnel from Norway, Belgium and Iceland.

The last battle group is led by the United States and based in Orzysz, Poland. It is made up of American, British, Romanian and Croatian troops.

As far as the size is concerned, each group consists of around 1000 people, which does not necessarily represent a force large enough to deter. For this reason, in mid-2017, the Lithuanian President asked for the permanent presence of US troops in Lithuania in order not only to deter, but also to defend.

Within the framework of increasing the readiness and capability of their armed forces to cooperate, the Alliance's defense ministers agreed to create two new headquarters, bringing approximately 1 200 new personnel to the NATO Command Structure. The Joint Support and Enabling Command (JSEC) center will be based in Ulm, Germany, and its primary task will be to supervise the movement of military units and materials within Europe. The NATO Joint Command for the Atlantic region will be resided in Norfolk, Virginia, in the USA, and at the same time will be involved in the management of operations in the North Atlantic region, including the management of redeployment of troops and materials in the region.

The Secretary-General of the North Atlantic Treaty Organization said: “We are currently in the process of adapting NATO's command structure, which is a key building block of our alliance ... to ensure the deployment of the right type of armed forces at the right places and at the right time. These headquarters will be indispensable to strengthen the Alliance in the Atlantic region and across Europe [15]. ”The Defense Alliance also agreed to launch a NATO Emergency Initiative, known as the “Four Thirties”. In practice, this plan would mean that by 2020 the Member States should have 30 mechanized battalions, 30 air squadrons and 30 combat vessels at their disposal, and these units should be deployed no later than 30 days after the crisis. Albeit the proposed plan did not include data on specific numbers of units, usually one battalion includes 600 up to 1000 soldiers.

It is not yet clear how the Four Thirties plan would correspond to further efforts to improve the combat readiness of NATO military forces, many of which have commitments in different regions while facing a shortage of weapons and equipment. It is also unclear how quickly the Alliance could move large numbers of troops to its Eastern borders and how long it could keep them there. Stoltenberg explained that the Emergency Initiative “is not based on increasing the number of new armed forces, but rather on increasing the preparedness of the existing armed forces. This initiative highlights our determination to encourage a culture of readiness across the alliance“ [16].

7 CONCLUSION

It is clear from the above mentioned that the relationship between the EU, the USA and Russia requires a combination of several foreign policy tools. In addition to the diplomacy itself, which however fails in many cases, different forms of controls are necessary. The policy of sanctions are in question, which have not fully reached in practise the required result but they still are considered as an important foreign policy tool towards countries acting similarly as Russia.

On the one hand, there are ill-considered political statements, on the other hand business relationships, which to a great extent depend on the geopolitical situation and the concrete economic interest. Russia is rather to be considered as a single player. It relies on its nuclear arsenal representing the power, which has to be taken into account, but mainly it relies on the mineral sources. The use of energy card for enforcement of its geopolitical interest is in case of Russia very often. In the EU, however, there is a split in attitudes towards such behaviour, both between individual EU Member States and between the EU itself and the US.

The EU and USA are traditional political allies. However, the facts related to the recent five years show that in some cases the political will is not enough. Both partners have faced with the unwillingness of the other party to take some joint measures, mainly for economic reasons. President Trump's policy keeps the European Union's attention mainly for the announced custom duties on the automotive industry.

In addition to disagreement in the field of energy, there is an obvious conflict of interests also in the military domain. Currently, the European Defense Area is fully covered by NATO forces, which also serve to deter any efforts to undermine the sovereignty of EU states and all Member States support the activities of the North Atlantic Alliance. However, frequent criticism from the US is the attitude of European states towards their commitments and, above all, the lack of NATO funding.

It is the sufficient deterrent military force of the EU or NATO countries to serve as a support for diplomatic efforts to reach agreements with the Russian Federation on current sensitive issues. Cooperation between the two most important representatives of the "West" - the USA and the EU - is therefore inevitable.

References

[1] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union´s Foreign and Security Policy. [online]. 2016. Available at: http://eeas.europa.eu/

archives/docs/top_stories/pdf/eugs_review_web.pdf

[2] CFSP Report – Our priorities in 2017. [online]. 2017. Available at: https://data.consilium.europa.eu/doc/document/ST-10650-2017-INIT/ en/pdf

[3] WALLIN, M. 2017. U.S. Foreign Policy Towards Russia. In: *American Security Project*. [online]. Available at: https://www.americansecurityproject.org/white-paper-u-s-foreign-policy-toward-russia/

[4] HIGGINS, A. 2017. Maybe Private Russian Hackers Meddled in Election, Putin Says. In: *The New York Times*, 2. July 2017, ISSN: 0362-4331.

[5] Permanent Structured Cooperation – PESCO. Deepening Defense Cooperation Among EU Member States. [online]. Available at: http://eeas.europa.eu/sites/eeas/files/pesco_ factsheet_november_2019.pdf

[6] Council decision: establishing Permanent Structured Cooperation (PESCO) and determining the list of Participating Member States. [online]. 2017. Available at: https://www.consilium.europa.eu/media/32000 / st14866en17.pdf

[7] Declaration on PESCO projects. [online]. 2017. Available at: https://www.consilium. europa. eu/media/32020/draft-pesco-declaration-clean-10122017.pdf

[8] ŠMIHULA, D.: 2017. Záhada ruského zbrojenia. In: *Hospodárske noviny*. ISSN: 1335-4701, 2017, roč. 22, 10. októbra, s. 14.

[9] RUMER, E. 2016. *Russia and the security of Europe*. [online]. Carnegie Endowment for International Peace. 2016. [online] Available at: https://carnegieendowment.org/2016/06/30/russia-and-security-of-europe-pub-63990

[10] INF Treaty. [online]. Available at: https://2009-2017.state.gov/t/avc/trty/102360.htm

[11] WESSLAU, F. 2016. Putin´s friends in Europe. In: *European Council on Foreign Relations*. [online]. 2016. Available at: http://www.ecfr.eu/article/commentary_putins_friends_in_europe7153

[12] ILIEVA, J., DASHTEVSKI, A., KOKOTOVIC, F. 2018. Economic Sanctions in International Law. In: *UTMS Journal of Economics*. ISSN 1857-6974. 2018. Vol. 9, No. 2.

[13] Warsaw Summit Communiqué. [online]. 2016. Available at: https://www.nato.int/cps/en/ natohq/official_texts_133169.htm? selectedLocale=en

[14] Multinational North-East Corps. [online]. Available at: https://mncne.pl/docs/ convention. pdf.

[15] Press conference by NATO Secretary General Jens Stoltenberg. [online]. 2018. Available at: https://www.nato.int/cps/en/natohq/opinions_155264.htm

[16] Available at: https://www.nato.int/cps/en/ natohq/opinions_ 155264.htm

[17] KORHONEN, I., SIMOLA, H., SOLANKO, L. 2018. Sanctions, counter-sanctions and Russia – Effects on economy, trade and finance. In: *Policy Brief* [online]. 2018, no. 4. Available at: https://helda.helsinki.fi/bof/bitstream/handle/ 123456789/15510/bpb0418.pdf?sequence=1

[18] PALONKORPI, M. 2006. *Matter over Mind? Securitizing Regional Energy Interdependencies*. Helsinki : Aleksanteri Institute, University of Helsinki, 2006.

[19] HOFREITER, L. 2016. *Bezpečnostné prostredie súčasného sveta*. Zlín : VeRBuM, 2016. 160 s. ISBN 978-80-87500-79-8.

[20] MALMLÖF, T. et al. 2014. *Economy, Energy and Sanctions*. In: Swedish Defence Research Agency [online]. 2014. Available at: http://media.aff.a.se/2014/06/ARude-Awakening-FOI-2014-06-.pdf# page=73.

[21] RAHN, R.W. 2014. *How the Greens help Putin in Crimea incursion*. [online]. Available at: http://www.cato.org/publications/commentary/how-greenshelp-putin-crimea-incursion .

[22] DE BRUYCKERE, L. 2018. Ukrajinská kríza a jej vplyv na Európske debaty o energetike. In: *Medzinárodné vzťahy*. ISSN: 1336-1562, 2018, vol. 16, no. 1, p. 94-111.

Dipl. Eng. Marek **HARGAŠ**
Statistical Office of the Slovak Republic
824 67 Bratislava
Slovak Republic
E-mail: marek.hargas@statistics.sk

Marek **HARGAŠ** is a the Head of Civil Service Office of the Statistical Office of the Slovak Republic. His professional backround is management. Actually he studies PhD. degree program on Armed Forces Academy of General Milan Rastislav Stefanik. His area of study is focused on relations between Russia and NATO.