

THE GENERAL JONAS ŽEMAITIS MILITARY ACADEMY OF LITHUANIA



CHALLENGES TO NATIONAL DEFENCE IN CONTEMPORARY GEOPOLITICAL SITUATION CNDCGS`2018

International Conference and Live Firing Show` 2018



COGITA UNIVERSALITER – AGE REGIONALITER
NATIONAL DEFENCE FOUNDATION



GENERAL JONAS ŽEMAITIS MILITARY ACADEMY OF LITHUANIA



**CHALLENGES TO NATIONAL DEFENCE
IN CONTEMPORARY GEOPOLITICAL SITUATION
CNDCGS` 2018**

ABSTRACTS OF THE 1TH INTERNATIONAL SCIENTIFIC CONFERENCE
EDITED BY S. BEKESIENE AND S. HOŠKOVÁ-MAYEROVÁ

April 25-27, 2018
Pabrade, Lithuania

CONFERENCE IS ORGANIZED BY

General Jonas Žemaitis Military Academy of Lithuania
Kaunas University of Technology
National Defence Foundation
Lithuanian Riflemen's Union

The abstracts of the 1th International Scientific Conference CHALLENGES TO NATIONAL DEFENCE IN CONTEMPORARY GEOPOLITICAL SITUATION contain short reviews of presented works.

All abstracts were reviewed.

The style and language of authors were not corrected. The quality of language of papers is under the authors' responsibility. Only minor editorial corrections have been carried out by the Publisher.

All rights preserved. No part of this publication may be reproduced, stored in retrieval system, or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without the permission of the Publisher.

© The General Jonas Žemaitis Military Academy of Lithuania, 2018

ISBN 978-609-8074-77-2

CONFERENCE SCIENTIFIC COMMITTEE

CHAIRMAN

Assoc.Prof. Svajonė Bekešienė, Military Academy of Lithuania

SCIENTIFIC SECRETARY

Assoc. Prof. Hošková-Mayerová Šárka, Brno University of Defence, Czech Republic

MEMBERS

Major Assoc. Prof. Eng. Dorel Badea, PhD., “Nicolae Balcescu” Land Forces Academy, Romania

Prof. Ž. Bazaras, Kaunas University of Technology, Lithuania

Assoc. Prof. Svajonė Bekešienė, Military Academy of Lithuania

Prof. Eugeniusz Ciesliak, University of Military Technology, Poland

COL Dipl. Eng. Ph.D. Vladan Holcner, Brno University of Defence, Czech Republic

Prof. Martin Holmberg, Swedish Defence University, Sweden

Assoc. Prof. Hošková-Mayerová Šárka, Brno University of Defence, Czech Republic

Prof. Volodymyr Hutsaylyuk, Military University of Technology, Poland

Prof. Algimantas Fedaravičius, Kaunas University of Technology, Lithuania

Assoc. Prof. Cristina Flaut, Ovidius University, Romania

Prof. Jan Furch, Brno University of Defence, Czech Republic

Assoc. Prof. Saulius Japertas, Kaunas University of Technology, Lithuania

Prof. Aušrius Juozapavičius, Military Academy of Lithuania

Prof. Fabrizio Maturo, University of Chieti-Pescara, Italy

LTC Ing. Vlastimil Neumann, Ph.D., Brno University of Defence, Czech Republic

Dr. Soili Paananen, Finnish National Defence University, Finland

Assoc. Prof. Audronė Petrauskaitė, Military Academy of Lithuania

Assoc. Prof. Rolanda Kazlauskaitė-Markelienė, Military Academy of Lithuania

Col. Dr. R. Kostrow, Military Institute of Armament Technology, Poland

Dr. Jolanta Sabaitytė, Military Academy of Lithuania

Prof. Rasa Smaliukienė, Military Academy of Lithuania

Prof. Lucjan Śniezek, Military University of Technology, Poland

Assoc. Prof. Alena Vagaská, Prešov Technical University of Košice, Slovak Republic

Prof. Ing. Zdeněk Vintr, CSc., Brno University of Defence, Czech Republic

1th International Scientific Conference “CHALLENGES TO NATIONAL DEFENCE
IN CONTEMPORARY GEOPOLITICAL SITUATION”

PREFACE

The first international conference „Challenges to National Defence in Contemporary Geopolitical Situation” (CNDCGS-2018) was held during April 25th-27th, 2018 at the PABRADE TRAINING AREA, Lithuania.

The conference was organized by the General Jonas Žemaitis Military Academy of Lithuania, Kaunas University of Technology in cooperation with the National Defence Foundation and the Lithuanian Riflemen’s Union.

The CNDCGS-2018 brought together practitioners and researchers to discuss important issues related to the current and future challenges to Europe defence capabilities and helped to collect the great innovative ideas for future developing. Also there was made an important contribution to the defence innovation. This conference attracted significant attention of the Lithuanian society, and increased the attention to the security of the Baltic region of international political community and US and European decision makers.

The CNDCGS-2018 aimed at sharing the latest relevant information on the issues of national defence in contemporary geopolitical situation. The papers in the Abstracts book include the following areas:

- Defence Technologies and Aviation
- Cyber Threats and Security Issues
- Democracy, Contemporary Threats and Warfare
- Modern Technologies and Social Sciences
- Multi-Criteria Decision-Making
- Sustainable Defence Solutions
- The Impact of New Defence Technologies on Human
- Defence Technologies: Education and Training
- Environmental Issues and Modern Technologies
- Challenges to Face New Defence Technologies

The primary goal of the CNDCGS-2018 was to present the highest quality research results. The key element in achieving it was the evolution and selection procedure developed by the Scientific Committee of the conference.

The invitations to the CNDCGS-2018 listed the instructions for preparing reports, abstracts, manuscripts and the deadlines. All works presented during conference and published in Abstracts book underwent the procedure for submitting proposals, including requirements and deadlines, are published at: http://www.lka.lt/lt/moksline-veikla/konferencijos-ir-seminarai/2017-m._983/tarptautine-moksline-konferencija-zne8/guidelines-for-abstracts.html

The CNDCGS-2018 participants presented their research results in an extended abstract format of 500-1000 words, including references, following the requirements that have made the Abstracts a valuable resource of new information which allows evaluating the researches of scientists from different countries.

Assoc. Prof. dr. S. Bekesiene
Conference Chair

CONTENTS

Automatic Modulation Recognition Based on Artificial Neural Network.....	9
Juozas Adamonis, Jonas Matuzas, Gediminas Molis	
Consensus in Multiperson Decision Making by Neutrosophic Sets.....	12
Romualdas Baušys, Svajone Bekesiene	
Peace Time Protection Systems Against Unmanned Vehicle	15
Svajone Bekesiene, Nikolaj Dobržinskij	
MEMS Device Frequency Response Modeling for Molecules Sensing Application.....	19
Tomas Gadišauskas, Aušrius Juozapavičius, Mangirdas Malinauskas, Valdas Eidukynas, Rita Plaipaitė-Nalivaiko	
Laser 3D Printing of Ceramic Micro-/Nano-Structures.....	22
Darius Gailevičius, Viktorija Padolskytė, Simas Šakirzanovas, Tomas Gadišauskas, Vygtantas Mizeikis, Kestutis Staliunas, Saulius Juodkazis, Mangirdas Malinauskas	
Internal Aspects of National Security: Lithuanian Case	24
Jadvyga Ciburiene, Jurate Guscinskiene	
Understanding people and Technology. Professional Military Education and Challenges in Development of Future Commanders.....	27
Eugeniusz Cieslak	
Sustainable Financial Security Paradigm Management in the Baltics.....	29
Gediminas Dubauskasa	
Land Force Soldier System Evaluation: a Case of Lithuania Troops.....	33
Svajone Bekesiene, Šarka Hošková-Mayerová	
Military Training Equipment: Design, Research and Implementation.....	37
Algimantas Fedaravičius, Arvydas Survila	
High Efficiency Logical Filters Approach in Early-staged Cyber Attacks Detection.....	40
Saulius Japertas, Tautvydas Bakšys	
Analysis of Military UAV Vulnerabilities and Losses	45
Saulius Japertas	
Cybersecurity in the Context of Criminal Law Protection of the State Security and Sectors of Critical Infrastructure.....	48
Miroslav Kelemen, Stanislav Szabo, Iveta Vajdová	
Security Management in the Air Transport: Example of an Interdisciplinary Investigation of Special Security Questions.....	51
Miroslav Kelemen, Stanislav Szabo, Iveta Vajdová	

Small EU Initiatives in the Process of Pooling and Sharing of Military Capabilities...54 Zbyšek Korecki	
Contemporary Challenges to Polish Cultural Security56 Mariusz Kubiak	
Conceptual Model for Minimization of Threats Caused by Illegal Immigrants to EU Road Freight Carriers.....57 Margarita Marija Lietuvnikė, Aidas Vasilis Vasiliauskas, Virgilija Vasilienė-Vasiliauskienė, Jolanta Sabaitytė	
Heavy Robots for C-IED Operations59 Marian Janusz Łopatka	
Analysis of Dismounted Operation Support with Robots62 Marian Łopatka, Tomasz Muszynski	
Analysis of Engineer Obstacle Negotiation Possibility with Grouping Robots.....65 Marian Janusz Łopatka	
Future Robots Using in C-Ied Detection68 Marian Łopatka, Tomasz Muszynski	
Clausewitz's Trinity and Contemporary Low Intensity Conflicts (Theoretical Approach).....71 Leonas Lukoševičius	
Visualization of Narrative Structure73 Justina Mandravickaitė, Tomas Krilavičius, Danguolė Kalinauskaitė	
Design of Electromagnetic Rail Powered Missile for Penetrating Missile Defence System.....75 Hari Prasanna Manimaran, Naga Manikanta Kommanaboina, Mastan Raja Papanaboina	
Significant Impact of Cyber Threats to National Security77 Svajone Bekesiene, Emile Mazeikaite	
Assessment of the Influence of RGO Content on the Static Strength of Silicone.....79 Barbara Nasiłowska, Piotr Wawrzyniak, Zdzisław Bogdanowicz, Paweł Bogusz, Aneta Bombalska, Wojciech Skrzeczanowski, Monika Mularczyk-Oliwa and Zygmunt Mierczyk	
Undercarriage of Combat Tracked Vehicles82 Vlastimil Neumann	
ARDL Models of Military Spending and its Security and Economic Determinants.....84 Jiří Neubauer, Jakub Odehnal	
The New Trend - Environmental Data and Information Collection Using Unmanned Aerial Vehicles.....87 Josef Novotný	

Meteorological Application of UAV as a New Way of Vertical Profile of Lower Atmosphere Measurement.....	89
Josef Novotný, Radek Bystřický, Karel Dejmál	
Utilization the New Advanced Structural Materials in the Military Vehicles and Heavy Equipment.....	92
Tomasz Ślęzak	
Electronic Defence Systems Comparison: Nato and Russia Case.....	95
Jolanta Sabaityte, Aušrius Juozapavičius, Pranas Karčiauskas	
Experimental Study on Ballistic AA 2519 –AA 1050 -Ti6Al4V Laminate According to STANAG 4569 Level 2.....	98
Ireneusz Szachogluchowicz, Lucjan Sniezek, Marcin Wachowski, Volodymyr Hutsaylyuk, Wojciech Koperski	
Knowledge Management in Military: a Systematic Review.....	101
Rasa Smaliukiene, Vidmantė Giedraityte	
Postmodern Threats for National Security in Postmodern World.....	103
Audronė Petrauskaitė, Rolanda Kazlauskaitė Markelienė	
Composites Containing Ag Nanoparticles for X-ray Protection	105
Rita Plaipaitė-Nalivaiko, Diana Adlienė, Igoris Prosyčėvas, Valery Luhin, Tomas Gadišauskas	
Influence of Social Media on National Security.....	108
Dalia Prakapienė, Romas Prakapas, Gitana Dudzevičiūtė	
Grenade UAV for Reconnaissance and Rapid Combat Assistance (GURRCA) Project.....	112
Sathvik Sathyanarayana Rao	
Peculiarities of ICT in Securing Energy Sector in Lebanon	116
Youssef El Tabsh, Vida Davidavičienė, Jolanta Sabaitytė	
The Influence of Substitutions on the Explosive Properties. N-(2,4,6-trinitrophenyl)-1H-1,2,4-triazol-3'-amine	121
Jelena Tamuliene, Jonas Sarlauskas, Svajone Bekesiene	
Societal Security in Poland	124
Maciej Tołwiński	
Information Security in Poland	126
Stanisław Topolewski	
The Value of Staff Loyalty at Security and Defence Institutions: A Case Study of the Public Security Service Vilnius Unit.....	128
Vladas Tumulavičius, Karolis Kriaučionis	

Implications of the Fragmentation of Lithuanian Uniformed Services.....	130
Svajūnė Ungurytė-Ragauskienė, Mantas Bileišis	
Authors' index.....	132

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Automatic Modulation Recognition Based on Artificial Neural Network

Juozas Adamonis, Jonas Matuzas, Gediminas Molis

Baltic Institute of Advanced Technology, Sauletekio al. 15, LT-10224, Vilnius, Lithuania,

Introduction. For the task of making high-throughput secondary user system that can coexist with minimal or no interference with primary user by predicting its channel utilization pattern, new and more effective approach for mitigating radio frequency interference signals in radio data, comes from using latest advances in deep learning. The most prominent techniques include Recurrent Neural Networks (RNN) as well as Convolutional Neural Networks (CNN).

When backpropagation was first introduced, its most exciting use was for training recurrent neural networks. RNNs process an input sequence one element at a time, maintaining in their hidden units a 'state vector' that implicitly contains information about the history of all the past elements of the sequence. Thanks to advances in their architecture and ways of training them, RNN have been found to be very good at predicting the next character in the text or the next word in a sequence. Similarly they were adapted for the use in cognitive radio for rapid protocol decoding [1] or predicting occupation of the spectral channel [2].

Another very attractive deep learning architecture for signal modulation recognition in cognitive radio systems is convolutional neural network. CNN layers were introduced in [3] to provide an efficient learning method for 2D images. By tying adjacent shifts to the same weights together in a way similar to that of a filter sliding across an input vector convolutional layers are able to force the learning features with an invariance to shifts in the input vector. This technique was adapted for I/Q radio signal processing [4, 5]. T. Oshea in [1] even showed, that in signal modulation recognition task CNN can outperform standard techniques.

To demonstrate the concept, we used technique proposed by Oshea et. al. [4] to generate synthetic data of various signal modulations. Data set was generated with GNU radio, using GNU Radio channel model blocks. In our case we used audio record of human voice to generate 3 analog (WBFM, AM-SSB and AM-DSB) modulations and ASCII coded text to generate 8 digital (BPSK, 8PSK, QPSK, 16QAM, 64QAM, CPFSK, GFSK and PAM4) modulation signals. The recorded time series were cut into 128 sample length sections, sampling at 200 kHz rate. Data set was formed of 6000 sections of 128 samples of every modulation. Also the effects were taken into account such as, time varying multi-path fading of the channel impulse response, random walk drifting of carrier frequency oscillator and sample time clocks and additive Gaussian

white noise. All signals were passed through harsh channel models, which introduce unknown scale, translation, dilation, and impulsive noise onto signal.

Method of investigation. Modulation classification experiments with previously described data sets can be easily performed using modern libraries dedicated for deep neural networks, such as tensorflow, caffe or torch. These tools are used to build neural networks of desired configuration. System under the investigation was made of two convolutional layers and one dense layer accompanied by softmax classifier. The latter was used to determine against 11 different analogue and digital signal modulations. First convolutional layer was made of 64 filters of dimension 1x5, while second layer contained 128 filters of dimensions 2x3, respectively. Finally, dense layer was made of 128 neurons and all layers had ReLu non-linear activation elements.

The aforementioned neural network system was compared to the approach having pre-processing stage. I/Q signals 2D histogram of 100x100 bins (I values x, and Q-values y) was generated. To generate a histogram 2048 points from the signal was used.

Investigation Results. Modulation recognition task was performed on synthetically created data which, included not only modulated signal but fading channel noise component as well. The noise to signal level varied from -20 dB to 18 dB. Recorded I/Q signal of the form of 2D vector was passed to aforementioned system. After learning process, using method proposed by O’Shea at al. we observed maximal prediction accuracy of above 85%. The result was obtained using 128 samples. Longer samples were also classified, but no significant increase in accuracy was observed.

Using a system with a pre-processing stage, to classify 2D 100x100 grayscale images simple CNN was used (multiple 2D 3x3 convolution filters only). Using the particular network structure classification accuracy of 99.82% was achieved when testing with 10 different modulations dataset.

Conclusions. The following results of our investigation were obtained:

- although it is possible to feed a CNN with a signal time series data the pre-processing stage can improve the classification accuracy significantly.
- typically longer time series signal is needed to make a histogram and increase the classification accuracy.

Keywords: Convolutional Neural Networks; Recurrent Neural Networks; Automatic Modulation Recognition; Cognitive Radio;

References

- [1] T.J. O’Shea, S.Hitefield, and J.Corgan, “End-to-end radio traffic sequence recognition with recurrent neural networks” in Signal and Information Processing (GlobalSIP), 2016 IEEE Global Conference on}, pp.277-281, IEEE, 2016.
- [2] Z.-l. Tang and S.-m. Li, “Deep recurrent neural network for multiple time slot frequency spectrum predictions of cognitive radio,” KSII Transactions on Internet and Information Systems (TIIS), vol.11, no.6, pp.3029-3045, 2017.
- [3] Y.LeCun et al., “Generalization and network design strategies,” Connectionism in perspective, pp.143-155, 1989.

[4] T.J. OShea, J.Corgan, and T.C. Clancy, “Convolutional radio modulation recognition networks,” in International Conference on Engineering Applications of Neural Networks}, pp.213-226, Springer, 2016.

[5] K.S.K. Arumugam, I.A. Kadampot, M.Tahmasbi, S.Shah, M.Bloch, and S.Pokutta, “Modulation recognition using side information and hybrid learning,” in 2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), pp.1-2, March 2017.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Consensus in Multiperson Decision Making by Neutrosophic Sets

Romualdas Baušys^{a1}, Svajone Bekesiene^b

^a*Vilnius Gediminas Technical University, Saulėtekio al. 11, LT-10223 Vilnius,*

^b*The General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius*

Introduction. The chosen investigations have become currently relevant because the leaders in the military organization are usually identified with managerial personnel. To be a serviceman (commander, officer) leader in the military means to appropriately deal with subordinate soldiers. It means, that military leader have to know and be able to inspire soldiers to conduct joint activities (sometimes under very difficult environmental conditions) in order to achieve the established objective. The leader's-officer's behavior is appropriate when he is held up as an example to others, not only just exercising his powers and giving orders. Although leadership in the military organization is usually based on situational leadership and subordinates' motivation, the practical application of leadership theories and leadership itself can be effective only if the chosen leadership style and the ways, forms and means of influence are suitable to subordinates. The Lithuanian Army seeks to develop a military leadership identity as a way to promote mission success.

It is difficult to obviously identify what leadership is and provide its accurate definition, for there is no unique approach towards the notion of leadership. There are many skills and features that young officers must obtain and develop to become effective military leaders. There are three main characteristics for good military leaders: leadership, decision-making and situational awareness. It is, therefore, understandable that all militaries are trained to cultivate on these skills.

Some universal theories make the implicit assumption that successful or effective leadership does not depend on the characteristics of the situation in which the leader operates. Moreover, leadership is invariant within, as well as between, roles. Different circumstances encountered by the leader are not necessarily seen as requiring different forms of leadership. Because they propose that there exists a "one-best-way" to lead, such perspectives attempt to offer universal prescriptions for leadership.

On the other hand, other methodologies suggest that effective leadership depends

1 * Corresponding author.

E-mail address: Romualdas.Bausys@vgtu.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania,
Engineering Managing Department

on unambiguous features of the leader's position as on the originalities of the task as on the individualities of followers. These methodologies propose certain situational variables. When these variables are evaluated, they provide a situational analysis on which leadership recommendations are based. These theories therefore provide depending recommendations for leadership. Perspectives vary in the way the leadership construct is hypothesized. It is possible to view leadership mainly in terms of relatively established and long-term characteristics of people. Leadership can be viewed as a quantifiable and measureable property possessed in different amounts by different people. This study presents a multi-criteria decision-making (MCDM) framework that identifies the effective leadership abilities, which is appreciated by soldiers in the Lithuanian Armed Forces.

Method of investigation. From the methodological point of view there was chosen the MCDM framework. Formalized representation of problem can be described by individual's behaviour. If we have a set X of individuals which should be evaluated as leaders, it means that we'll have evaluate each of them from point of leader behaviour view $X=\{x_1, x_2, \dots, x_n\}$. Each individual (element of set X) have to be evaluated by set of criteria $C=\{c_1(x), c_2(x), \dots, c_m(x)\}$ that characterize main leadership qualities.

The general problem consists in ordering elements of set X on the ground of criteria $c_1(x), c_2(x), \dots, c_m(x)$. In other words the problem assumes constructing rating of x_1, x_2, \dots, x_n based on scalar multiple – factor estimates formed from $c_1(x), c_2(x), \dots, c_m(x)$. Particular case of the general problem consists in choosing “best” element of set X , i.e. individual with best general level of leader behaviour.

To solve the formulated problem based on the represented theoretical background it is necessary to collect all the results of measurement of leadership qualities for all the individuals from set X . Utility functions of type (5) for each criterion should be formed and calculated for all the elements of set X .

Using available information about relative importance of local criteria one of the basic situations about numerical values of weight coefficients $w_i, i=1, 2, \dots, n$, should be chosen. Generalized utility function $\Psi(x)$ calculated according to the situation is considered as scalar multiple-factor estimate of each alternative $x \in X$. $\Psi(x)$ is the base for constructing rating of individuals x_1, x_2, \dots, x_n (the general problem) and for choice of the individual with best general level of leader behavior.

Conclusions. The results of our investigations show us that:

MCDM methods provide a powerful framework to solve personal leadership problems;

Applied neutrosophic set allows to express the vagueness of the initial information explicitly;

The presented numerical example shows the applicability and effectiveness of the WASPAS-SVNS method.

Keywords: Fuzzy decision making, analytical hierarchy process, outranking methods, multi-criteria decision-making, leadership.

References

- [1] Aghaarabi E et al (2014) Comparative study of fuzzy evidential reasoning and fuzzy rule-based approaches: an illustration for water quality assessment in distribution networks. *Stoch Env Res Risk Assess* 28(3):655–679
- [2] Calvin (2011) Fuzzy logic decision making. https://www.calvin.edu/*pribeiro/othrlnks/Fuzzy/fuzzydecisions.htm
- Christos M (2014) Thinking platforms for smarter urban water systems: fusing technical and socioeconomic models and tools. *Geol Soc London Spec Publ* 408:SP408-4 46 2 Multi Criteria Decision Making
- [3] de Jalón SG et al (2014) Building resilience to water scarcity in southern Spain: a case study of rice farming in Doñana protected wetlands. *Reg Environ Change* 14(3):1229–1242
- [4] Dwivedi A, Bhadauria S (2014) Composite sustainable management index for rural water supply systems using the analytical hierarchy process. *J Perform Constr Facil* 28(3):608–617
- [5] Gamini H (2004) Incorporating community objectives in improved wetland management: the use of the analytic hierarchy process. *J Environ Manage* 70(3):263–273
- [6] Giri S, Nejadhashemi AP (2014) Application of analytical hierarchy process for effective selection of agricultural best management practices. *J Environ Manage* 132:165–177
- [7] Hajeer M, Al-Othman A (2005) Application of the analytical hierarchy process in the selection of desalination plants. *Desalination* 174(1):97–108
- [8] Hajkowicz S, Collins K (2007) A review of multiple criteria analysis for water resource planning and management. *Water Resour Manage* 21(9):1553–1566
- [9] Herath G (2004) Incorporating community objectives in improved wetland management: the use of the analytic hierarchy process. *J Environ Manage* 70(3):263–273
- [10] Kamodkar RU, Regulwar DG (2014) Optimal multiobjective reservoir operation with fuzzy decision variables and resources: a compromise approach. *J Hydro Environ Res* 8:428–440
- [11] Pelletier FJ (2000) Review of metamathematics of fuzzy logics in the bulletin of symbolic logic. *JSTOR* 421060 6(3):342–346

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Peace Time Protection Systems Against Unmanned Vehicle

Svajone Bekesiene^{a1}, Nikolaj Dobržinskij^b

^{ab}*The General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius,*

Introduction. The chosen investigations have become currently relevant because the activity of unmanned aerial vehicles (drones) in the world is increasing during last 10 years. The unmanned aerial vehicles are one of the fasters growing and most exciting technologies anywhere in the world. There are many companies that predict the UAVs market variations. These companies for market analysis used the different sources of information and methodologies, but their forecast analysis proves that the market of the UAVs is growing [1]. More than eighty countries produced the unmanned aerial vehicles for the different purposes, but there are only about twenty five countries which producing military UAVs [2].

The challenges of detecting low, slow, and small (LSS) unmanned aerial vehicles (UAVs) becoming an important capability for the maintenance of security. Consumer grade LSS UAVs are becoming increasingly complex, and represent a diverse new threat which must be addressed by physical security systems of the future. The conclusion drawn from internal discussions and external reports is the following; detection of LSS UAVs is a challenging problem that cannot be achieved with a single detection modality for all potential targets. Classification of LSS UAVs, especially classification in the presence of background clutter (e.g., urban environment) or other non-threatening targets (e.g., birds), is under-explored. Though information of available technologies is sparse, many of the existing options for UAVs detection appear to be in their infancy (when compared to more established ground-based air defence systems for larger and/or faster threats). Companies currently providing or developing technologies to combat the UAVs safety and security problem are certainly worth investigating, however, no company has provided the statistical evidence necessary to support robust detection, identification, and/or neutralization of LSS UAVs targets. Military conflict in Ukraine has shown the growing use of such aircraft in military and civil conflicts. Due to the capabilities and size of various drones, their shoot down has become difficult. Units of the Lithuanian Armed Forces, military exercises, the military equipment of Lithuania and its NATO allies attract more and more attention from the people. Such

1 * Corresponding author. Tel.: 370-6-86-48-000

E-mail address: Svajone.Bekesiene@lka.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

factors have led to the intensive use of drones over military areas and other restricted areas. Airborne threats coming from the drones have revealed a security loophole in the Lithuanian Armed Forces. However, Lithuanian Armed forces do not have any security measures that can effectively fight against hostile drones. In this reason conducted analysis deals with the dangers of the drones: a threat analysis and its types. The protection methods were raised by the Ministry of National Defense (MND). The following combat concept developed by MND was chosen as background for on how to combat the unmanned aerial vehicles (drones). The MND concept has three combat modules:

Module I – Detection. The first there are necessary to collect of some phenomenological information captured by a sensor.

Module II - Identification / Tracking. The received data in the detection phase analysis, with the goal being to separate real targets from highly clustered, noisy background data. This step of analysis is performed solely by a human.

Module III - Neutralization. Once a target is positively identified in the previous step, additional action must be taken to deny mission success, including the potential for target neutralization. An overview of detection methods, drone neutralization options, specific blocked frequencies, and the main weapon - the jammer.

Ultimately, the appropriateness of the methods for qualification or neutralization of LSS UAVs targets within the wanted setting is what will order their use and/or implementation in future ground based aerial defence systems or LSS UAVs qualification systems. We have not to forget, that the use of UAVs ammunitions and missiles for security or safety protection is obviously not ideal in a heavily populated civilian environment. On the other hand, these methods may be appropriate for engaging targets on a hostile battlefield. The decision for use of such devices must be heavily influenced by the inherent risks in each (e.g. collateral damage or ineffectiveness), and whether the consequences of those risks are determined to be acceptable.

Method of investigation. From the methodological point of view there was chosen the hierarchical clustering analysis, which helped to identify the best protection against a remotely controlled unmanned aircraft systems, which are similar to each other but different from individuals in other groups. It can be intellectually satisfying, profitable, or sometimes both to manage this without clustering analysis because it can't be known who or what belongs in which group and a number of groups can be known only after hierarchical clustering analysis.

Next analysis, which solve in part about goals and objectives was the experts' evaluation methods based on experts' surveyed sample analysis. The Kendall's coefficient of concordance (W) was selected for experts' data analysis. The statistical software package SPSS version 20 was used for the collected experts' data analysis and for the hierarchical clustering analysis as well [14].

Investigation Results. The results of our investigation were listed after the deep analysis of all protective measures which were chosen as the interest's area of the Ministry of National Defense. This analysis let us to clarify protective measures possibilities, advantages and disadvantages. There was found that all analyzed systems

and products had weakness - do not have a final solution that can be effective in the future. This analysis showed that manufacturers didn't provide for the possibility of continuous updating of equipment, installing new components to adapt to newly emerging threats. Also can be mention, that the commercial equipment designed to fight against civilian aircraft is ineffective against modified and / or military aircraft.

An expert survey has been used to quantify experts' opinions according to Kendall's concordance coefficient. The evaluation of the technical criteria of the experts resulted in the collection of 16 criteria. In the opinion of all ten experts, the compatibility was too low ($W1 = .174$) to make the decision. In this reason there was repeated statistical analysis with reselected groups of experts according to their specific experience and the maximum of Kendall's concordance coefficient was reached ($W2 = .518$). This result allowed us the use of expert judgment for decision making.

After hierarchical clustering of security measures, five clusters were identified: First- Blihter Surveillance Systems, Aquila Defense Group, NT Service, Radio Hills Technologies, Rohde & Schwarz and Lithuania; Second - HENDSOLDT; Third - Bukovel Fourth - Elbit Systems; Fifth - MOOG. Based on the calculated average of Lithuania's Euclidean distances matrix, the closest and distant security systems were established in accordance with the requirements of Lithuania. Closest: NT Service - Lithuanian and US Company and Rohde & Schwarz - Danish company. In the remote: Bukovel-Ukraine system and Elbit Systems - Israel's security tool.

Conclusions. The results of our investigations show us that due to the fast-paced technology, there is no ideal system or product against UVAs. With the assistance of a specific experience group of experts, four key technical criteria were identified: UVA identification, system mobility, and neutralization and operator location. The hierarchical clustering of security measures showed the closest and the remote security tools for Lithuanian demands.

All criteria were met by the Israeli company Elbyt Systems, the second system meeting the highest criteria is HENDOLDT with 35 requirements. The United Kingdom system remains in the third chart position with only 33 matching requirements.

Keywords: Unmanned Aircraft Systems, multidimensional database, hierarchical clustering, Kendall W.

References

- [1] Nagpal K. Unmanned aerialvehicles (UAV) market. Defence ProAc, New Delhi, Delhi, India, 2012.
- [2] Military Factory. Unmanned Aerial Vehicles (UAVs), Unmanned Combat Aerial Vehicles (UCAVs) and Drone Aircraft. U.S., 2016.
- [3] Williams K. W. A summary of Unmanned Aircraft accident/incident data: Human factors implications. Technical Report No. DOT/FAA/AM-04/24, Washington, DC. U.S. Department of Transportation, federal Aviation Administration, Office of Aerospace Medicine. 2004.
- [4] Ryan J. Wallace, Jon M. Loffi. International journal of aviation, aeronautics, and aerospace „Examining Unmanned Aerial System Threats &Defenses: A Conceptual

Analysis”, 2015, p. 6-13.

[5] Otto, R.P. Air Force ISR 2023: Delivering Decision Advantage; Headquarters United States Air Force:

Washington, DC, USA, 2013.

[6] Dempsey, M.E. Intelligence, Surveillance, and Reconnaissance Joint Force 2020 White Paper; U.S. Army:

Washington, DC, USA, 2014.

[7] Cluster Analysis Basic Concepts and Algorithms [online cit.: 2017-07-22]. Available from:

<https://www-users.cs.umn.edu/~kumar/dmbook/ch8.pdf>

[8] Bekešienė S., Guščinskienė J., Dvilaitis G. Intelligent Applications in the Development of Death Prevention by Suicide while on Active Duty, Active and Reserve Components. Kaunas: Technologija, 2015, p. 56-65. ISSN 2345-0088 (Print).

[9] Seffers, G. Joint Aerial Layer Network Vision Moves Toward Reality. [online cit.: 2017-06-22].

Available from: <http://www.afcea.org/content/?q=node/11123>

[10] Schechter, E. UAVs Could be Next Step for Electronic Warfare [online cit.: 2016-06-22].

Available from: http://archive.c4isrnet.com/article/20140507/C4ISRNET08/3_05070006/UAVs-could-next-step-electronic-warfare

[11] Cevik, P.; Kocaman, I.; Akgul, A.; Akca, B. The Small and Silent Force Multiplier: A Swarm UAV—Electronic Attack. J. Intell. Robot. Syst. 2013, 70, 595–608.

[12] Callam, A. DroneWars: Armed Unmanned Aerial Vehicles. Int. Aff. Rev. 2010, 18, 3.

[13] Lockheed/Piasecki Team Tackles Cargo UAV. 2014. [online cit.: 2016-07-22]. Available from: <http://aviationweek.com/awin/lockheedpiasecki-team-tackles-cargo-uav>

[14] Myers, M. New funds to aid coast guard in adopting a UAV. Navy Times, 25 April 2015.

[15] IBM SPSS Statistics [online cit.: 2017-07-22]. Available from:

<http://www.ibm.com/analytics/us/en/technology/spss/>

[16] Valvanis, K.; Vachtsevanos, G. Future of Unmanned Aviation. In Handbook of Unmanned Aerial Vehicles Springer: Dordrecht, The Netherlands, 2015; pp. 2993–3009.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

MEMS Device Frequency Response Modeling for Molecules Sensing Application

Tomas Gadišauskas ^{a*}, Aušrius Juozapavičius ^a, Mangirdas Malinauskas ^b,
Valdas Eidukynas ^c, Rita Plaipaitė-Nalivaiko ^d

^a *The General Jonas Žemaitis Military Academy of Lithuania, Silo Str. 5A, LT-10322 Vilnius*

^b *Vilnius University, Laser Research Center, Sauletekio Ave. 10, LT-10223, Lithuania,*

^c *Kaunas University of Technology, K. Donelaičio Str. 73, LT-44249 Kaunas, Lithuania*

^d *Kaunas University of Applied Engineering Sciences, Tvirtovės Ave. 35, LT – 50155, Kaunas, Lithuania*

Introduction. Due to the rising international terrorism involving explosives law enforcing agencies around the world encounter diverse threat scenarios. Luggage of air, sea and road travelers, as well as post parcels are being screened against hidden explosives, and every larger crowd gathering is under strong surveillance. Real-time detection of evaporated explosive material in the air is the main step towards preventing an attack. Hundreds or thousands of molecules of the explosive material are needed to detect it in the gas form [1]. Practically the detection process is random and the detection method is based on the recognition probability. A method with a larger rate of correct positives and smaller rate of false negatives is therefore desirable. Ideally the method should identify the material instantaneously from just one molecule. Spectroscopic methods have the best detection resolution [2]. Applications of linear and non-linear optics based on Raman scattering have been demonstrated to successfully detect traces of explosives [3-5]. Resolution of SERS technique reaches 10^{-12} mol concentrations of $\text{Fe}_3\text{O}_4/\text{Au}$ NPs in case of TNT and similar explosives and even 3×10^{-16} mol concentrations of Au NPs in porous alumina [7]. Unfortunately, spectroscopic methods alone are not efficient in practice due to a large area of search and it is better to supplement them by microelectromechanical systems (MEMS). In that case the precise moment of sample deposition onto a substrate is detected using a resonator and then a detailed spectroscopic analysis is performed [8]. Real-time chemisorption measurements using ultra-sensitive NEMS have achieved resolutions down to 10^{-15} g [9] or even down to one molecule mass using nano-mechanical mass sensors [10]. To create real-life mass detectors with chemical receptors an optimal ratio between their geometrical dimensions and sensitivity has to be established. Thus properties of a V and U-shaped cantilevers have been investigated with respect to the well-known rectangular cantilever used in atomic field microscopy (AFM) applications.

Method of investigation. Polycrystalline silicon was selected as the material for the MEMS device. A classical rectangular cantilever used in AFM and described by the Euler–Bernoulli beam theory was chosen as a reference base. For comparison a soft V-form triangular cantilever suitable for biological samples and a mode-enriched U-form cantilever were created. The frequency response function was investigated up to 10 MHz and the transfer function of a 100 nm excitation between the base and the apex was measured. The each model was realized in the SolidWorks environment using 10^4 finite elements. Finite element models were created for I-, U-, and V-form cantilevers. Frequency response was investigated by changing geometrical parameters: length ($L=30-120 \mu\text{m}$) and thickness ($T=0.4-1.3 \mu\text{m}$) while fixing the width (B) to keep the same proportions. The mechanical damping function was used as in the case of the rectangular cantilever. The forms of the models were specifically selected in order to compare single-, double-, and three-component cantilevers.

Investigation results. The frequency response function of the resonators was normalized to the amplitude of the first mode. The response was measured as a function of the geometrical parameters of the cantilevers. The more constituting parts a cantilever has, the richer modes (bending, torsional, lateral and others) it has. Due to an intrinsic mass of a probe the most prominent influence to sensitivity is exerted by the thickness and only then by the length. For measurements involving the optical lever read-out the most informative was the mode of the bending-type. However, if a symmetric optical read-out was used on the apex then some positions of bending modes had larger regions of linearity which is important to increase sensitivity.

Conclusions. Performed modeling reveals the behavior of cantilever vibrations in higher frequencies. Different Eigen-modes can be obtained by varying geometrical parameters of different-shape resonators at the same frequency. Sensitivity increase is also possible due to asymmetric optical lever read-out point. Model suggested regions of linear frequency response which can be useful for evaluating resonator shapes for applications based on their resonance frequency using stored elastic energy and Von Mises stress criterion. The proposed cantilever microstructures potentially could be realized *via* ultrafast laser 3D nanolithography technique [11].

Acknowledgement. This research is partially funded by a grant (Reg. No. NKPDOKT-13206) from the Research Council of Lithuania. The authors are thankful for the software resources and other support provided by the Kaunas University of Technology.

Keywords: explosive materials; MEMS; detection of explosives; spectroscopy; microcantilever; calculations; frequency response modeling; direct laser writing 3D nanolithography.

References

1. Kathryn E. Brown & Margo T. Greenfield & Shawn D. McGrane & David S. Moore. Advances in explosives analysis—part I: animal, chemical, ion, and mechanical methods. Anal. Bioanal. Chem. 2015, Springer:10.1007/s00216-015-9040-4.

2. A. Hakonen, P. O. Andersson, M. S. Schmidt, T. Rindzevicius, M. Käll. Explosive and chemical threat detection by surface-enhanced Raman scattering: A review. *Analytica Chimica Acta*. 2015. Elsevier: S0003-2670(15)00475-4.
3. M. Gaft, L. Nagli, "UV gated Raman spectroscopy for standoff detection of explosives," *Opt. Mater.* 30(11), 1739–1746 (2008).
4. B. Zachhuber, G. Ramer, A. Hobro, E. T. Chrysostom, B. Lendl. Stand-off Raman spectroscopy: a powerful technique for qualitative and quantitative analysis of inorganic and organic compounds including explosives. *Anal. Bioanal. Chem.* 400(8), 2439–2447 (2011).
5. R. Furstenberg, C. A. Kendziora, J. Stepnowski, S. V. Stepnowski, M. Rake, M. R. Papantonakis, V. Nguyen, G. K. Hubler, and R. A. McGill. Stand-off detection of trace explosives via resonant infrared photothermal imaging. *Appl. Phys. Lett.* 93(22), 224103 (2008).
6. Mahmoud, K.A. and M. Zourob. Fe₃O₄/Au nanoparticles/lignin modified microspheres as effectual surface enhanced Raman scattering (SERS) substrates for highly selective and sensitive detection of 2,4,6-trinitrotoluene (TNT). *Analyst*, 2013. 138(9): p. 2712-2719.
7. Ko, H., S. Chang, and V.V. Tsukruk. Porous Substrates for Label-Free Molecular Level Detection of Nonresonant Organic Molecules. *Acs Nano*, 2009. 3(1): p. 181-188. 125.
8. O. Zandieh, S. Kim. Multi-modal, ultrasensitive detection of trace explosives using MEMS devices with quantum cascade lasers. *Proc. of SPIE* (2016). Vol. 9836 98362H-1
9. M. Li, H. X. Tang, M. L. Roukes. Ultra-sensitive NEMS-based cantilevers for sensing, scanned probe and very high-frequency applications. *Nature Nanotechnol.* (2007). NPG:10.1038/nnano.2006.208.
10. M. S. Hanay, S. Kelber, A. K. Naik, D. Chi, S. Hentz, E. C. Bullard, E. Colinet, L. Duraffourg, M. L. Roukes. Single-protein nanomechanical mass spectrometry in real time. *Nature Nanotechnol.* (2012). NPG: 10.1038/nnano.2012.119.
11. M. Malinauskas, A. Zukauskas, S. Hasegawa, Y. Hayasaki, V. Mizeikis, R. Buividas, and S. Juodkazis. Ultrafast laser processing of materials: from science to industry, *Light: Sci. Appl.* 5, e16133 (2016). NPG: 10.1038/lsa.2016.133.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Laser 3D Printing of Ceramic Micro-/Nano-Structures

Darius Gailevičius^{a,b*}, Viktorija Padolskytė^{a,b}, Simas Šakirzanovas^c,
Tomas Gadišauskas^d, Vygantas Mizeikis^e, Kestutis Staliunas^f,
Saulius Juodkasis^g, Mangirdas Malinauskas^h

^aLaser Research Center, Vilnius University, Sauletekio Ave. 10, LT-10222, Vilnius, Lithuania,

^bFemtika LTD, Sauletekio Ave. 15, LT-10224, Vilnius, Lithuania,

^c Faculty of Chemistry and Geosciences, Vilnius University, Naugarduko Str. 24, LT-03225 Vilnius, Lithuania,

^dThe General Jonas Žemaitis Military Academy of Lithuania, Silo Str. 5A, LT-10322 Vilnius,

^eResearch Institute of Electronics, Shizuoka University, 3-5-3-1 Johoku, Naka-ku, 432-8561 Hamamatsu, Japan,

^fDepartament de Física i Enginyeria Nuclear, Universitat Politècnica de Catalunya, Colom 11, 08222 Terrassa, Spain,

^gSwinburne University of Technology, Victoria 3122, Hawthorn, Australia,

Introduction. Ceramics as advanced materials play an important role in science and technology and are attractive for use in harsh environments as they are mechanically robust, withstand immense heat, comparatively chemically inert. Thus there is a direct end user driven need to find ways for efficiently acquiring free-form 3D ceramic structures. During the last years, stereolithographic 3D printing of hybrid organic-inorganic photopolymer and subsequent pyrolysis was demonstrated to be capable of providing ceramic [1] and glass structures [2]. Up to now this was limited to the (sub) millimeter scale and naturally the next step is to acquire functional glass-/ceramic-like 3D structures in micro-/nano-dimensions.

Method of investigation. Here we explore a possibility to apply ultrafast 3D laser nanolithography [3] followed by heat treatment to create ceramic 3D structures down to micro-/nano-dimension. Laser fabrication is employed for production of initial 3D structures with varying (ranging within hundreds of nm) feature sizes out of hybrid organic-inorganic material SZ2080 [4]. Then, a post-fabrication heating at different temperatures up to 1500 °C under Ar, O₂ or air atmosphere facilitate metal-organic framework decomposition, which results in the glass-ceramic hybrid material. Additionally, this procedure densifies the obtained objects providing extra route for size control. As we show, this can be applied both to periodic 2D gratings and 3D (photonic stop-gap tuning) woodpile structures as well as bulk objects [5], which we observed via a scanning electron microscope.

Furthermore, in order to uncover undergoing chemical and physical processes

during heat-treatment we performed thermo-gravimetric analysis, micro-Raman spectroscopy and X-ray diffraction analysis and performed stress tests in the form of dry and wet chemical etching and focused ion beam milling.

Investigation results. We uncover that the geometric downscaling can reach up to 40%, while the aspect ratio of single features as well as filling ratio of the whole object remains the same regardless of volume/surface-area ratio. This validates the method as the isotropic reduction in size can be easily accounted for and pre-compensated before manufacturing the initial pre-ceramic object. The structures proven to be qualitatively resistant to focused ion beam milling, hinting at significantly increased resiliency. Finally, revealed physical (transparency, refractive index, emissivity in IR, mechanical rigidity) and chemical (wetting, resistance to harsh chemicals) properties prove the proposed approach paving a route towards 3D opto-structuring of ceramics at nanoscale for diverse photonic, microfluidic and biomedical applications.

Results. The following results of our investigation were obtained:

- In addition to downscaling up to 40% during heat-treatment of SZ2080 DLW structured, we observed chemical and physical change of the material composition and properties.
- Crystalline properties of the material typical to ZrO_2 - SiO_2 composite start to appear as the organic part evaporates.
- The material becomes more crystalline as heating temperature increases.
- 3D printing and pyrolysis of SZ2080 results in more resilient ceramic structures to chemical and physical environments: wet and dry etching, focused ion beam milling.

Acknowledgement. NATO grant No. SPS-985048 “Nanostructures for Highly Efficient Infrared Detection” and AMRDEC grant No. W911NF-16-2-0069 “Enhanced Absorption in Stopped-Light Photonic Nanostructures: Applications to Efficient Sensing” projects are acknowledged for financial support.

Keywords: direct laser writing, multiphoton 3D lithography, organic-inorganic photoresist, SZ2080, heat-treatment, pyrolysis, ceramic microstructures, advanced materials.

References:

- [1] Z.C. Eckel et al., Additive manufacturing of polymer-derived ceramics, *Science* 351 (6268), 58 (2016); doi: 10.1126/science.aad2688.
- [2] F. Kotz et al., Three-dimensional printing of transparent fused silica glass, *Nature* 544, 337 (2017); doi: 10.1038/nature22061.
- [3] M. Malinauskas et al., Ultrafast laser processing of materials: from science to industry, *Light Sci. Appl.* 5, e16133 (2016); doi: 10.1038/lssa.2016.133.
- [4] A. Ovsianikov, Ultra-Low Shrinkage Hybrid Photosensitive Material for Two-Photon Polymerization Microfabrication, *ACS Nano* 2, 2257 (2008); doi: 10.1021/nn800451w.
- [5] D. Gailevicius et al., in preparation.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Internal Aspects of National Security: Lithuanian Case

Jadvyga Ciburiene^{a1}, Jurate Guscinskiene^b

^a*Kaunas University of Technology, School of Economics and Business, Gedimino st. 50,
LT-44239, Kaunas, Lithuania,*

^b*The General Jonas Žemaitis Military Academy of Lithuania, Silo st. 5A, LT-10322, Vilnius, Lithuania*

Introduction. In general as challenges to National defence the current geopolitical risks of the concrete region and the centers of global power are analyzed. Mostly scientific studies focus on two interrelated aspects: political (cybercrime, civil wars, terrorism, religious extremism) and economic, using comparative research of countries relations [1, 2]. Another aspects of studies are: the main driving factors of secure and sustainable development and economic growth, such as foreign direct investment, education [3], energy security, including renewable and the integration energy systems [4, 5], identifying economic sectors which have important effect to the national security (e. g., production and supply of electric energy, natural gas, telecommunications, communications, rail and road transports, water supply, banking sector, etc. activities) [6, 7]. However, for any challenges to national security it is especially important sufficient state budget revenues which are needed to finance the solving of different problems and unexpected dangerous situations. The aim of this study is to analyze and to evaluate the factors that reduce the revenue of the state budget, i.e. the problems of emigration and high unemployment level, the high share of shadow economy, low wage level of employees of different regions of Lithuania.

The investigation of these factors compared with the average results in the European Union countries (EU-28) in the period of year 2007-2016. Both absolute and relative amounts of analyzed indicators are compared. The method of base indicators comparison is used, whereas the first year (e.g., year 2007) of the analyzed period is chosen as the base year. The results of theoretical research part are characterized with statistical indicators and the theoretical predictions made are checked with practical research.

Method of investigation. The estimation of the main factors that reduce the revenue of the state budget in Lithuania is used, giving the theoretical and practical research. The study was carried out using qualitative methods: scientific literature analysis, statistical data classification, systematization, synthesis, comparison, generalization and illustration, e.g., table and graphical analysis. For the evaluation of the challenges to national defence in the period of year 2007-2016 year 2007 was chosen as the base.

1 * Corresponding author. Tel.: +370-613-43-624.

E-mail address: jadvyga.ciburiene@ktu.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania,
Engineering Managing Department

Investigation Results. The paper summarized the scientific literature on the question of challenges to national defence and analyzed the internal security threats in Lithuania. Results contain elements of classification challenges to national defence, grouping and comparison of the EU-28 according to the government budget deficit. The Lithuanian government policy seeking both to reduce shadow economy, unemployment and emigration; and both to increase the wage level gives an impetus to be in the line with EU-28 government budget indicators and to create preconditions for more reliable national security in Lithuania and its regions. The comparison of situation in Lithuania and the EU-28 allows determining the direction and the rate of changes of economic indicators and comparing with expectations of population.

Conclusions. The following results of our investigation were obtained:

State excess budget or with less deficit state and sufficient budget revenues is especially important to national security of the country;

The main labor market indicators (unemployment, emigration and its structure), the transparency level of the country market (the share of shadow economy, low wage level of employees of different regions of Lithuania) reduces both budget revenues and both preconditions for national security in Lithuania;

We argue that there is a need for comprehensive analysis of internal security threats in Lithuania.

The above observations allow us to foresee that the determination of different aspects of challengers to national defence helps to discover the new aspects to enlarge the security of the country and to increase its competitiveness.

Keywords: national defence; state budget; emigration; shadow economy, wage level; unemployment level; regions of Lithuania.

References

[1] Special Eurobarometer 432. European's attitudes towards security. https://data.europa.eu/euodp/data/dataset/S2085_83_2_432_ENG

[2] Garbuz I. V. The transformation of the Russian economy in view of the current geopolitical risks. SGEM International Multidisciplinary Scientific Conferences on Social Sciences and Arts. Conference on Political Sciences Law, Finance, Economics & Tourism. Conference Proceedings. Volume IV. Economics & Tourism, September 1-10, 2014, Albena, Bulgaria. Instrumentation for trace detection of high explosives. *Rev. Sci. Instrum.* 2004; 75: 821–828.

[3] Maciulis A., Tvaronaviciene M. Secure and sustainable development: Lithuania's new role in taking the presidency of the EU. *Journal of Security and Sustainability Issues.* 2013; Volume 3(2): 5–13.

[4] Vosylius E., Rakutis V, Tvaronaviciene M. Economic growth, sustainable development and energy security interrelat. *Journal of Security and Sustainability Issues.* 2013; Volume 2(3): 5–14.

[5] Melas V., Lisin E., Tvaronavičienė M., Peresadko G., Radwański R. Energy security and economic development: renewable and the integration of energy systems. *Journal of Security and Sustainability Issues.* 2017; Volume 7 Number 1: 134–139.

[6] Lewandowski R. Economic sectors of strategic importance to the national security. A case of Poland. *Equilibrium. Quarterly Journal of Economics and Economic Policy.* 2016; VOLUME 11 ISSUE 3: 473-497.

[7] Smaliukiene R., Dudzeviciute G., Adekola A. F., Aktan B. The investigation of Lithuanian growth and industry export dependence on energetic resources. *Journal of Security and Sustainability Issues*. 2012; Volume 2(2): 69–78.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Understanding people and Technology. Professional Military Education and Challenges in Development of Future Commanders

Eugeniusz Cieslak

"Siedlce University of Natural Sciences and Humanities, Faculty of Humanities, Institute of Social Sciences and Security, 39 Żytunia st., 08-110 Siedlce, Poland

The security environment evolves rapidly and employment of military power becomes more and more complex. Military commanders face “compressed battlespace and levels of warfare” and act in complex social, cultural and economic environment. Despite the level of command and control, all future military commander require comprehensive knowledge stretching out of typical “military toolbox” to be effective in achieving objectives of a broad scope of military operations. Technology becomes one of the most rapidly changing aspects of security environment. It is especially true for emerging and readily available technologies with military relevance that may be available even to non-state actors. All that requires diligent efforts to prepare future commanders for making decisions and acting in intertwined social and technological scenarios. Understanding people and technology seems a prerequisite for success, while not understanding even one of those aspects may be disastrous. Lessons learned from military operations just in recent decades prove the value of comprehension of both social and technological dimensions of security environment.

Depending on the level of command and control as well as a type of military operations future commanders will need different mix of social and technological expertise. Professional Military Education offers unique opportunities for future commanders to grow intellectually, reflect and anticipate changes in security environments. Case studies serve as a way to improve future commanders’ skills to act in complex environments. Along with introduction to theoretical approaches to decision making under certainties and simulation and modelling, case studies proved to be effective in preparing commanders for operations in complex environments. Polish perspectives related to professional military education will be discussed to present best practices in preparing future commanders for future security environments. Lessons learned will be presented to spark discussion on possible improvements in professional military education related to preparation of future commanders for operations in complex environments.

Keywords: Professional Military Education (PME), social dimension, new technologies, military operations, commanders.

References

Report of the Panel on Military Education of The One Hundredth Congress of the Committee On Armed Services House of Representatives One Hundred First Congress First Session, April 21, 1989. U.S. Government Printing Office, Washington 1989

Another Crossroads? Professional Military Education Two Decades After the Goldwater-Nichols Act and the Skelton Panel. U.S. House of Representatives, Committee on Armed Services, Subcommittee on Oversight & Investigation, Committee Print 111-4, April 2010

R.H. Scales: Too busy to Learn. „Proceedings Magazine” February 2010, Vol. 136/2/1

C.D. Allen: Redress of Professional Military Education. The Clarion Call. „Joint Force Quarterly” 2010 Issue 59

J. L. Chameau, W. F. Ballhaus, H. S. Lin, Emerging and Readily Available Technologies and National Security — A Framework for Addressing Ethical, Legal, and Societal Issues, The National Academy Press, Washington 2014

W. Murray: Testimony. House Armed Services Committee, Subcommittee on Professional Military Education, not dated

Program reformy wyższego szkolnictwa wojskowego. Rekomendacje. Wydawnictwo Ministerstwa Obrony Narodowej, Warszawa 2007 r.

J. B. Grochowski: Kulisy kariery. Z generałem brygady Januszem Bojarskim o dylematach polityki kadrowej rozmawia Janusz B. Grochowski. „Polska Zbrojna” z 25 lipca 2010 r.

P. Bernabiuk, W. Kiss-Orski, T. Wrobel: Po pierwsze diagnoza. „Polska Zbrojna” nr 8 z 2013 r.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Sustainable Financial Security Paradigm Management in the Baltics

Gediminas Dubauskas^a

^aThe General Jonas Žemaitis Military Academy of Lithuania, Šilo g. 5A, LT-10322 Vilnius, Lithuania

Abstract. The finance management education is treated differently in different countries. That is becoming increasingly important provision that such a discussion does not directly benefit the common development of financial education in recent years. One of the possible ways to deal with personal finances in different economic conditions could be changing attitudes to finance knowledge among students in academies. The correct management of these programs helps to improve student and cadets learning experience and the economic well-being. Additionally, the learning based on the public administration and the public finance probably educate loyalists of the country and people intolerant to non-transparent activities of public servants. Eventually the best ways to determine the country consolidated tax paid by natural and legal persons could be the tax burden rate. Therefore, expenditures of the shared finance in many cases are even more important than revenues. Consequently, the increasing public debt service quantities could be an utmost importance for the each of taxpayers. Essential differences of governments' credit management took place in Baltic States during the crisis of 2008-2011. Lithuania decided to have an independent financial policy when Latvia accepted the majority of requirements from the International Monetary fund. Then we have an increase of the direct taxes burden by almost twice versus the official country's tax burden. However, the additional tax burden includes hidden taxes related to the accumulated spending. In that case the tax burden for an average employee could approach up to the two-thirds of the total (work-related) income. This observation of the tax burden should encourage each citizen of the country to be responsible for public servants' activities and for the increasing government debt and expenditures for debt services.

Sustainable Financial Security. Finance and public money management have a historical concept of educational process and is one of the key economic and financial preparation in contemporary education. Money subject is possible with a number of complex aspects, both permanent change in the market economy and historical origin of money and monetary politics.

* Corresponding author.

E-mail address: Gediminas.Dubauskas@lka.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

Why such knowledge is necessary for the first grade university education? Financial education is relevant to each

university undergraduate program. Incidentally, budget terminology and personal income taxation are known only from employment relationships or labour relations or comparable to labour relations income. The purpose of the topic is to reveal the importance of financial management to cadets and students, including public perception of administration and financial aspects of public revenues' mismanagement related to tax burden. The objective of the study is the financial competence and capability of the cadets of The General Jonas Žemaitis Military Academy of Lithuania and other students in understanding of public finance management and mismanagement. The purposes of the paper are to review financial and public finance development in the contemporary scientific literature; to display a necessity of education in public finance and public expenditure management. One of the key tasks of the paper is to reveal how taxation, public spending and fiscal policy are perceived by the citizens. In addition, it also attempts to answer the questions about the financial and economic importance on financial education. Furthermore, the theoretical task of the paper is to show the size of government debt service and expenditure in Baltic States. The research methods and methodological analysis used in the research were formal investigation and qualitative and quantitative research methods; the data was taken from Lithuanian, Latvian and some other EU financial institutions. The continuity and sustainability of the public finances paradigm is presently a sensual topic in economic policy discussion. This is because of the remainder on former debt crises in Europe and the long-term public spending pressures caused by the obstructive demographic change in more developed countries. This paper analyses some of the conceptualizations that have been used to evaluate the public finance continuity in the case of Lithuania. Also, hypothetical criteria for sustainability are examined. The article is partly conducted by a mode of the literature analysis. There is no consensus among economic experts about the accurate theoretical standard for public finance continuity and in particular its sustainability (Brammer 2017). There is many misconception of the importance concerning financial education programs in higher education and other institutions. Especially important for the public finances to understand their publicity in any case during totalitarian times the public finances were called "the state's finances" because the tax burden understanding was the quite secondary topic to the dominating idea of the creation of "a new world wide or at least nationwide socialism. In general, the concept of public finances in the education process starts with the tax and budget concepts. The municipal tax revenues and budget structure can be presented as a good example in which persons could see structure of public finance functioning and it should be likely the closest pattern to each citizen of a different country.

The Government Debt Management. The continuity and sustainability of public finance management could be represented by the example of the public debt policy in Lithuania and Latvia during the crisis of 2008-2011. These two different approaches can demonstrate how the national budget problems were solved in these two Baltic states. The effective debt management is critical especially during crisis (Aarma 2012). The high government debt leads to the increase of the tax burden, to the growth of the state budget deficit, to the dropping of the state consumption level, to the reduction of public sector salaries and social security payments. The above has a negative impact on the state economy, which is being already weakened by the crisis, and, thus, is forcing the

government to borrow more. The borrowing policy in Lithuania was to choose private Financial Institutions when in Latvia it was the International Monetary Fund (IMF). However, credits annual interest rates in Lithuania were from 4 to 9 percent versus Latvia's interest rates from 2.5 to 3 percent. Economical and financial policies during that crisis were independent in Lithuania versus regulated by the IMF in Latvia. Outcomes of the independent fiscal policies in Lithuania in 2009-2010 were quite positive without significant new taxation on property and other private wealth (Dubauskas, 2016). However new total taxes on property and on the all motor vehicles were introduced in Latvia. A possible difference of the debt service expenditures in Lithuania from the total national public debt 17,5 billion euro is around 800 million euro. We can assume that the average annual interest rates are five percent - then annual interest payments could be around 800 million euro.

Table No 1.

Lithuania's GDP and GDP growth changes before and after crisis 2005-2013

Lithuania's GDP at current market prices, in billions of Litas	Lithuania's GDP Growth/ Decline in percent, year by year	Year
76	7.8	2005
81.9	7.8	2006
90	9.8	2007
92.6	2.9	2008
78.9	-14.8	2009
80	1.4	2010
84.6	5,8	2011
86.7	2.5	2012
89.9	3.7	2013

Source: European Country Risk, 2018 [Access through Internet: <https://www.euromoneycountryrisk.com/wiki/Lithuania#Economic-Overview>; <https://countryeconomy.com/gdp/lithuania>]

Conclusions. The critical evaluations of the former “crisis time” Lithuania's parliament and government concerning financial policy (especially for expensive state credits supporting the independent financial policy) can be also used for the present-day government. Moreover, such behaviour illustrates not adequate financial decisions because of so high price paid for not introducing IMF suggested taxes during the economic crisis, but after a few years coming back to the same taxes.

Keywords: uniformed services, agencification, institutional fragmentation

References

Aarma, A., 2012. The Foreign Commercial Banks in the Baltic States: Aspects of the Financial Crisis Internationalization. *European Journal of Business and Economics*, Vol 5., DOI: <http://dx.doi.org/10.12955/ejbe.v5i0.161>.

Brammer, S.; Walker, H. 2017. Sustainable Procurement Practise in the Public Sector: An International Comparative Study. [Access through Internet] <http://www.bath.ac.uk/management/research/pdf/2017-16.pdf>

Dubauskas G. 2016. The Management of Public Finance Literacy for Sustainable Economic Environment. *Journal of Security and Sustainability Issues* 5(3):403-409. DOI: [http://dx.doi.org/109770/jssi.2015.5.3\(8\)](http://dx.doi.org/109770/jssi.2015.5.3(8))

International Monetary Fund, (2013). *World Economic Outlook: Tensions from the Two-Speed Recovery: Unemployment, Commodities, and Capital Flows* (No. April, 2013).

Lithuania Government Debt to GDP. 2018. [Access through Internet]: <https://tradingeconomics.com/lithuania/government-debt-to-gdp> //

Ministry of Finance of Lithuania. (2018). [Access through Internet]: <http://finmin.lrv.lt/lt/aktualus-valstybes-finansu-duomenys/valstybes-biudzeto-ir-savivaldybiu-biudzetu-vykdyimo-duomenys>.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Land Force Soldier System Evaluation: a Case of Lithuania Troops

Svajone Bekesiene^{a1}, Sarka Hošková-Mayerová^b

^a*The General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius,*

^b*University of Defence in Brno, Faculty of Military Technology, Kounicova 65, Brno, 66210, Czech Republic*

Introduction. Nowadays, all countries in the world care about their security. One of the institutions that helps to maintain the territorial integrity and protects its citizens is the army. The lessons learned during wars influence the development of military equipment. All countries arm its military forces with new technology which helps the military not only to accomplish its objectives, but also to improve the quality of their performance that can be expanded by targeting capabilities: the use of radio stations, GPS receivers and unmanned aerial vehicles enabling tracking of the battle in real time from remote distance. The Land Warrior system is also improving with more and more emerging technology-based elements that make the warrior even more effective in the battlefield during various operations.

The Lithuanian Land Force (LLF) forms the backbone of the country's defence force. The LLF is dedicated to the defence and security of the land territory of the Republic of Lithuania. It is one of the four Armed Forces of Lithuania, under the Chief of Defence. For this purpose, the Lithuanian Land Forces soldier system must be optimized, so that there would be no large corrections in supplement, the surplus production or unnecessary inventory, and that the existing parts of the soldier system would ensure its safety. This direction is also indicated in the 2015-2020 year guidelines (Minister of National Defence in 2015. January 27. Order No. V-82) by the Lithuanian Minister of National Defence, who made a decision that it is important for the individual soldier's equipment, armament, and outfit designed for soldiers to be comfortable, practical, and easy to use. Particular attention will be paid to the Lithuanian Land Force, because the use of military equipment in Navy or Air Forces is much more influenced by armaments and military equipment (e.g. aircrafts, ships).

However, the scientific literature does not analyse the Lithuanian Land Force soldiers system, for this reason it is particularly relevant to evaluate the current structure of the Land Forces soldiers system and its effectiveness in the context of other countries. This paper investigates the Lithuanian Land Force Soldier system optimization, for its intended purposes, technical characteristics and individual components.

1 * Corresponding author

E-mail address: Svajone.Bekesiene@lka.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

Method of investigation. For this research, the experts' evaluation methods based on experts' surveyed sample analysis were conducted, using quantitative assessments of their decisions. The investigated problem solution was the total surveyed experts' opinion. According to the experts surveyed, the average individual approach was determined by the following summaries of the expert group's opinion. The Kendall's coefficient of concordance (W) was selected for experts' data analysis. This coefficient was used as a measure of agreement among several (p) experts who were assessing a given set of n objects. Depending on the application field, the experts can be variables, characters, and so on. In the present work, they were the experts who rank parts of the Lithuanian Land Forces soldier system which, according to them, has to be optimized. Simulations were done by SPSS version 20. Following the analysis of experts' opinions, the main directions of improving the military system of the Lithuanian Land Forces were clarified: 1) technical characteristics of radio stations; 2) technical characteristics of helmets; 3) technical characteristics of bullet-proof vests.

In order to evaluate the current structure and effectiveness of the elements of the military force system of the Lithuanian Land Forces in the context of other countries, components of military systems used in six countries (radio communication equipment, ballistic helmets, and bullet-proof vests) were analysed. On the basis of these data, which were additionally standardized (variable measurements were changed to z-values), the hierarchical clustering analysis was performed by the SPSS 20 software package [14].

Investigation Results. The result of investigations in expert method depends on quality and quantity of evaluators as well. In this research we followed the suggestions which recommend choosing the right number of experts, because it is quite important for the research result. However, increasing the number cleared of these levels results in a diminishing scale of return, and doubling the number of evaluators to ten increases the percentage of usability problems identified to approximately 90% [4]. Following these recommendations, the group of ten experts was questioned in this research. All of them served in the Lithuanian army for approximately 17 years and have great military experience as Land force soldiers. Four of the experts were in the military service from 8 to 15 years, five of the experts from 16 to 20 years and one of the experts was in the military service for more than 24 years. The detailed characteristics are known to the author, but will not be presented in this paper.

For this research a list of 19 technical specifications for the Land soldier system was selected: *WSE1*- thermo-visual; *WSE 2*- longitude; *WSE 3*- glasses; *WSE 4*- military shoes; *WSE 5*- optical tuner; *WSE 6*- radio communication equipment; *WSE 7*- night vision devices; *WSE 8*- helmet system; *WSE 9*- bullet-proof vest; *WSE 10*- binoculars turnstile; *WSE 12*- collimator trick; *WSE 13*- GLOCK gun; *WSE 14*- automatic gun G-36; *WSE 15*- duckling; *WSE 16*- ammunition vest; *WSE 17*- CBRB safeguards; *WSE 18*- PMP measures; *WSE 19*- backpack. Experts' opinions were reached for each of the nineteen criteria after statistical analysis by the SPSS 20 package. Based on the results obtained, it can be concluded that the most important criteria, according to experts, are: a bullet-proof vest (*WSE9* rated 24) and a helmet system (*WSE8* rated 28 points). Criteria such as radio communication (*WSE6* rated 34 points), optical target (*WSE5* rated 54 points) and military boots (*WSE4* rated 75 points) are also important. These five criteria of significance are the key to improving the system of Lithuanian Land force troops.

The hierarchical clustering analysis helped to identify the essential differences between land force warrior systems. In this respect, the elements of the analysis of the Lithuanian military system are the most different from Poland. These differences could have been due to several reasons, but the key could be the fact that Poland has ordered radio communications on its domestic market, while other countries are guided by basic standards developed. The elements of the Land force military system are purchased on the basis of the companies offering the most satisfactory expectations.

Conclusions. From the obtained results, it can be concluded that the most appreciated parts of the system are a bullet-proof vest and backpack. This result was reached because these parts of the warrior system have been optimized very recently. In addition, the third criterion, which experts consider to be insignificant, is CBRB safeguards. Soldiers believe that CBRB's basic tools are reliable and good for use.

As we see from the study, all experts assessed the criteria *WSE16*, *WSE19* and *WSE17* as not significant. Therefore, we can say that these criteria in the system of Lithuania Land Forces are not decisive in order to improve the effectiveness of the tasks performed by the soldiers.

The hierarchical cluster analysis showed that Lithuanian Land Force soldier's system components are the most similar to those used in the US army. After technical parameter data analysis, it was found that Lithuania should take into account not only the US army warrior system, but also military system tools from other countries providing land forces soldier system optimization.

Keywords: Lithuanian Land Force soldier's system, multidimensional database, hierarchical clustering, Kendall W.

References

- [1] Advanced combat helmet [online cit.: 2017-10-15]. Available from: <https://www.military.com/equipment/advanced-combat-helmet-ach>
- [2] AN/PRC-117G (V)1(C) type-1 wideband multiband multimission radio with internal saasm gps, Harris, [online cit.: 2017-12-14]. Available from: http://www.midkiff.cz/obj/firma_produk_t_priloha_147_soubor.pdf
- [3] Apariko, J., Lovell, C. A. Knox, Jesus T. Pastor. (Eds). (2016). *Advances in Efficiency and Productivity: International Series in Operations Research & Management Science* [online cit.: 2017-10-15]. Available from: http://link.springer.com/chapter/10.1007/978-3-319-48461-7_1/fulltext.html
- [4] Codan radio communication, SENTRY-H™ SDR HF RADIO [online cit.: 2017-12-10]. Available from: https://www.codanradio.com/wp-content/uploads/Sentry-H_Datasheet_Screen_EN-Issue3-1.pdf
- [5] Department of defense, (1997). Test method standard: *V50 ballistic test for armor*. USA.
- [6] Elbit systems. DOMINATOR® [online cit.: 2017-11-29]. Available from: <http://elbitsystems.com/media/Dominator.pdf>
- [7] Federation of American scientists. Land warrior [online cit.: 2017-11-20]. Available from: <http://fas.org/man/dod-101/sys/land/land-warrior.htm>
- [8] French Army to Receive FELIN Systems, (2010 m.) [online cit.: 2017-10-10]. Available from: <http://www.army-technology.com/projects/felin/>
- [9] HA-03 AIRMOBILE HELMET [online cit.: 2017-10-10]. Available from:

<https://www.maskpol.com.pl/en/products/ha-03-airmobile-helmet.html>

[10] HARRIS FALCON III® AN/PRC-152A [online cit.: 2017-12-10]. Available from: [wideband-networking-handheld-radio.pdf](#)

[11] Harris RF-5000B Falcon 400W HF Radio System [online cit.: 2017-12-15]. Available from: <http://www.columbiaelectronics.com/id268.htm>

[12] Harris RF-5800V-HH Falcon II [online cit.: 2017-12-15]. Available from: <http://www.railce.com/cw/casc/harris/RF-5800V-HH.pdf>

[13] IdZ (Infanterist der Zukunft) Future Soldier System, Germany [online cit.: 2017-10-13]. Available from: <http://www.army-technology.com/projects/idz/>

[14] IBM SPSS Statistics [online cit.: 2017-07-22]. Available from:

<http://www.ibm.com/analytics/us/en/technology/spss/>

[15] Improved tactical vest [online cit.: 2017-10-13]. Available from: <https://www.military.com/equipment/improved-outer-tactical-vest-iotv>

[16] Land warrior, (2015 m.) [online cit.: 2017-10-15]. Available from: http://www.army-technology.com/projects/land_warrior/

[17] Military Defense Industry Technology - Body Armour & Helmet [online cit.: 2017-10-13]. Available from: https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/russian_soldiers_will_receive_new_6b43_6b45_body_armour_and_6b47_combat_helmets_tass_12705162.html

[18] NATO Standardization Agency, (2003). Stanag 2920 PPS (Edition 2) – Ballistic test method for personal armour materials and combat clothing.

[19] Racal PRC349 (Typ 1) [online cit.: 2017-12-10]. Available from: <http://www.helmut-singer.de/stock/1129024522.html>

[20] Radmor pr4g@stnet taktyczna radiostacja plecakowa vhf eccm 10w rrc 9210, Lenkija.

[21] Ratnik future soldier individual soldier combat gear system technical data sheet specifications pictures video 12205165 (2016 m.). [online cit.: 2017-12-16]. Available from: https://www.armyrecognition.com/russia_russian_military_field_equipment/ratnik_future_soldier_individual_soldier_combat_gear_system_technical_data_sheet_specifications_pictures_video_12205165.html

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Military Training Equipment: Design, Research and Implementation

Algimantas Fedaravičius¹, Arvydas Survila

Kaunas University of Technology, Donelaicio st. 73, LT-44249 Kaunas, Lithuania

Introduction. The Army is a constantly learning structure. This is why it is important to have effective and high quality training equipment.

Requirements for the training equipment are:

- realistic simulation of the armament operations;
- additional information about training process (statistics, functional operations etc.);
- safety and low cost.

The creation algorithm for the new equipment is: development of the engineering conception; theoretical research, computational modelling; experimental research; ground testing and practical implementation.

The main area of scientific research is dynamics of mechanical, electromechanical and mechatronics systems (modelling, control, optimal synthesis) and applications in the development of training and combat equipment and technologies for defence. Development of the new equipment and technologies are based applying the latest achievements in military science, mechanical engineering and mechatronics, material science, informatics, laser technologies and electronics, telecommunications and other areas of science and engineering.

In this paper the latest military training equipment projects for Land and Air Defence Forces are presented:

- few modifications of the laser simulation systems for riflemen;
- training equipment for 60mm and 120 mm mortars seminatural firing;
- rocket target for short range air defence systems.

Laser simulation systems for riflemen (G-36, FN MAG, CARL GUSTAF, Sig Sauer P226, Glock 17). Usage of the training equipment enables not only to reduce the ammunition - related economical costs used for shooting experts preparation but to significantly shorten the time of their training as well as improve the training quality.

¹ * Corresponding author. Tel.: +370-699-55231.

E-mail address: algimantas.fedaravicius@ktu.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

However, the training quality directly depends on the perfection of trainers as well as their functional facilities. Therefore, a new modification of riflemen trainer has been created: it includes three types of weapon imitators: automatic weapon G-36, machine gun FN MAG, recoilless rifle CARL GUSTAF, pistols Sig Sauer P226 and Glock 17 [1]. It is clear that the maximal reproduction of recoil and sound during single and burst shooting is a very important factor for the automatic gun G-36 and machine gun FN MAG and sound imitation only for the recoilless rifle CARL GUSTAF. The results of the preliminary analysis show that the pneumatic impulse systems with external control are the most perspective for the imitation of single and burst shots. The universal dynamical and mathematical models of the one way operation pneumatic drive for recoil imitation, results of its investigation and description of the new modification of laser trainer for riflemen are presented. The training weapons imitate the recoil and sound of the corresponding shooting regimes. The software supplies not only information about hits and statistics, but also the weapon trajectory during aiming, the position of the sights during each shot. It also lets choose the type of the target, the shooting distance, the target display time etc. It should be noted that it is possible to perform all the exercises appraised by the Commander of the Lithuanian Armed Forces. The Laser Shooting Simulation System has been successfully used in many training centres. The Laser Shooting Simulation System is included in NATO Master Catalogue of References for Logistics (NATO/ National Stock Number (NSN) codes: 6920-47-000-7909, 6920-47-000-7910, 6920-47-000-7911).

60 mm and 120 mm seminatural shooting mortar training equipment. They are very effective training means for the Land Forces.

The training equipment consists of training shells comprised of a warhead and sabot (ballistic barrel) of respective 60 or 120mm calibers. Such system allows full imitation of combat field firing in the firing position and ensures the preparation and correction of firing data in the firing control center. Mortar firing trainers not only reduce economic costs due to the fact that expensive battle bombs are not necessary, but also allow to avoid the expenses of transportation to the firing grounds and ensures high the efficiency and quality of the training process. The new problems of interior and exterior ballistics of two related masses was solved, because in this case during the explosion in the weapon's barrel not only one but two masses (the warhead and sabot) are ejected at the same time; problem of aerodynamic stabilization of a projectile; research of the warhead's fuse interaction with a non-deformable and deformable surface; development of the construction of mortar simulators and development of the experimental example of mortar simulators was performed. The 60 mm and 120 mm Mortar Training Equipment is implemented in Lithuanian Land Forces and included in NATO Master Catalogue of References for Logistics (NSN codes: 6920-47-000-2835, 6920-47-000-2836).

Rocket target RT-400 for short range air defence systems. The rocket target RT-400 is very effective training appliance for the Air Defence Forces. It is the target for the final training of the Stinger system service staff. The rocket-target must imitate the flight of aircraft, helicopters, and others air targets. In order to create a rocket target satisfying necessary parameters it is required to solve the following problems: determining the geometry of the target and its flight characteristics by taking into consideration the properties of the external ballistics of the Stinger missile and the parameters of the detection system (radars). The initial geometrical and flight parameters are:

- rocket length 5.4 m, diameter 0.4 m;
- flight velocity 160 - 250 m/s;
- maximum flight range 4.5 km, altitude 3.0 km;
- rocket mass less than 100 kg.

The second problem are analysis of the target's aerodynamical flow characteristics, determining the quantitative and qualitative thrust characteristics of the target's solid rocket motor and research the exterior ballistics of the rocket target [2]. On the basis of the research results the rocket target RT-400 was designed, manufactured and implemented in the Lithuanian Air Defence Forces. The rocket target RT-400 is included in NATO Master Catalogue of References for Logistics (NSN code: 6920-47-000-8331). The rocket target RT-400 has been successfully used in NATO exercises "Amber Arrow" in 2014, 2015 and 2017.

Conclusions and final remarks.

- The Department has a well developed basis for scientific research, design and practical implementation of the created equipment and technologies in the area of defence.
- Some examples of military training equipment for Air and Land Forces have been created and successfully implemented in Lithuanian and foreign countries Armed Forces. Twelve created products are included into NATO Master Catalog of References for Logistics.
- The experience accumulated in performing scientific research and practical implementation of its results allows further improvement of technical exploitation characteristics of the already developed training and combat equipment as well as development of new equipment.
- Scientists of the department are oriented towards the common Baltic States Region and European Research area the as well as common scientific projects and practical implementation with other countries.
- Acknowledgements. This work was supported by the Research Council of Lithuania, grant No. S-MIP-17-94 "Experimental Rocket: Research and Development".

Keywords: military training equipment, research, design, implementation

References:

[1] Fedaravičius, Algimantas; Survila, Arvydas; Patašienė, Laima; Sližys, Egidijus. Design, research and practical implementation of the laser shooting simulation system for 5.56 mm G-36, 7.62 mm FN MAG and 84 mm Carl Gustaf // Problemy mechatroniki: uzbrojenie, lotnictwo, inżynieria bezpieczeństwa = Problems of mechatronics: armament, aviation, safety engineering. Warszawa : Wojskowa Akademia Techniczna. ISSN 2081-5891. 2016, vol. 7, iss. 2(24), p. 7-17.

[2] Fedaravičius, Algimantas; Kiliukevičius, Sigita; Survila, Arvydas; Patašienė, Laima. Analysis of aerodynamic characteristics of the rocket-target for the „Stinger” system // Problemy mechatroniki: uzbrojenie, lotnictwo, inżynieria bezpieczeństwa = Problems of mechatronics: armament, aviation, safety engineering. Warszawa: Wojskowa Akademia Techniczna. ISSN 2081-5891. 2016, vol. 7, iss. 1(23), p. 7-16.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

High Efficiency Logical Filters Approach in Early-staged Cyber Attacks Detection

Saulius Japertas^{a*}, Tautvydas Bakšys^a

^a *Kaunas University of Technology, Department of Electronics Engineering, Vilniaus University, Studentu str. 50-438 LT-51368 Kaunas, Lithuania*

Introduction. Increasing digitization together with the benefits has also brought a lot of problems related to the challenges in cyberspace. Due to the ongoing cyberattacks yearly increase, losses in sectors that are using Telecommunication and IT services are growing.

The events of the past 10 years have shown that there are particularly dangerous incidents in the cyberspace, which are pre-planned, well-prepared and carried out by terrorist groups or even by some governments. Pre-planned cyber-attacks have some stages so it is possible to distinguish the early stages where attacks do not bring significant damage to data and information.

This article examines the features of the attacks and their characteristics and is the first part of the study's generalization. There is proposed a method for early staged detection of such attacks using a number of the logical filters. In the next paper, the logical mathematical model, an estimation of the sensitivity of such method and assessment of the probability of each initial stage will be presented. The results of theoretical simulation have shown that proposed method is capable of determining early-staged cyber attacks.

The most dangerous cyber attacks are those that are planned in advance [1-3], and they can be planned by both state structures and terrorist organizations. The planned cyber attacks consist of variety of different stages. Different authors describe the different number of the stages and parameters of such cyber attacks. Symantec designates five stages: Reconnaissance, Incursion, Discovery, Capture, and Exfiltration [4].

The same number of stages, but with different names, is proposed in [5]: Reconnaissance, Intrusion, Taking control, Collecting and leaking information, Eliminating traces. Meanwhile, Yadav and Rao [6] offer seven steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Act on Objective. More works [6-9] can be found, where a number of stages varies between three and eight. Different stages use different means and equipment to organize the attack. It can be assumed that certain actions in the early stages of the attack can prevent serious harmful effects [7, 8]. However, it is necessary to determine "early" stages and "late" stages, when damage created by an attack is mainly unavoidable. Therefore, it is needful to distinguish the various stages of attack in order to provide

the means and methods for preventing such attacks consequences. Yadav and Rao [6] suggested that the early stages include Reconnaissance, Weaponization, Delivery, and Part Exploitation Stages, in which, if an attack is observed, its effects can be eliminated.

Proposed methodology provides a network analysis structure, logical filter configuration and attack detection algorithms that enable the detection of network flow parameters that characterize potential attack vectors.

Method of investigation. The essence of the proposed method is to use the appropriate logical filters in order to classify the certain parameters of the traffic. For this purpose, the total analyzed data (information) flow is considered to consist of two parts: the normal flow (i.e., the flow that is not harmful) and the attacker’s flow (malicious flow). A generic filter structure is shown in Figure 1.

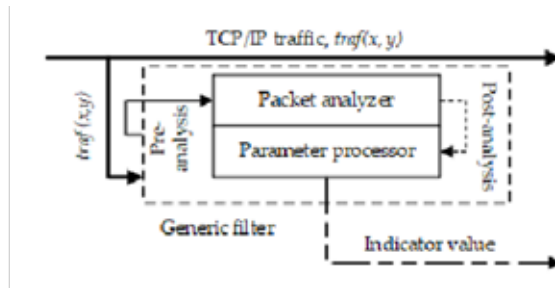


Figure 1. Structure of a Generic Filter.

The generic filter consists of two blocks: a packet analysis block and a parameter processor. The $traf(x, y)$ input into the filter is analyzed on the packet level, which results in a packet parameter (e.g., DST IP). The obtained parameter is passed to the internal parameter processor, which, according to the conditions provided, forms an indicator value. A schematic view of the activities of the detection method is shown in Figure 2.

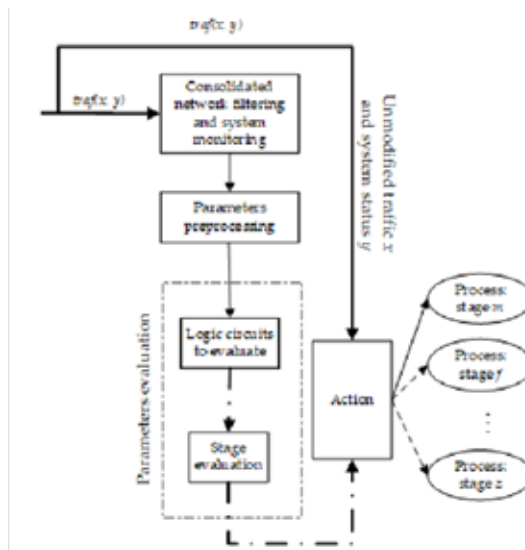


Figure 2. Schematic view of the detection method

In the proposed method, traffic $traf(x, y)$ is unmodified because there is a need to maintain the traffic of the system without affecting the system services reliability. It is shown as a separate line (“Unmodified traffic x and system status y ”). The detection method consists of three parts: filter part, evaluation block and action block. The filters are implemented in two blocks: consolidated network filtering and system monitoring (CNFSM) and parameter preprocessing (PP). In the CNFSM block, the filters are grouped into three groups: filtering of network parameters (NF), filtering of system parameters (SF), filtering of network stack flag parameters (LF). The evaluation block consists of three logical circuits that are connected at the outputs of the corresponding filter groups.

The purpose of the filters is to register parameters and, if their values exceed predefined values, indicate the malicious activity. The purpose of the evaluation block is to collect the binary parameters and process them for the indication of the possible attack action. The purpose of the action block is to decide which stage of the attack is observed.

Using this principle, it is possible to analyze network traffic and system behavior adaptively by adjusting filters for analysis according to the need (available resources, depth of analysis, speed and tolerances of created system or network delays).

Investigation Results. For the evaluation of the proposed algorithm, a logical circuit was synthesized and tested. The logical circuit used for aggregated analysis is shown in Figure 3. The analysis is based on seven criteria, so there are seven primary inputs and three primary outputs to identify value of the attack. The logical circuit consists of 26 logical gates.

As in the SSV logic circuit analysis case, primary input described as AA , where $A \in \{1 \dots 7\} A \in \{1 \dots 7\}$, corresponds to the binary „1“, and a member $\bar{A}\bar{A}$, where $A \in \{1 \dots 7\} A \in \{1 \dots 7\}$, corresponds to the binary „0“. This form contains output logical functions, which consist of inputs, resembling attack actions: HS, PS, SSV, SST, SP, LA and SE. Primary output S is a vector of “F21 ... F23” values.

$$S = \begin{pmatrix} F21 \\ F22 \\ F23 \end{pmatrix} = \begin{pmatrix} \overline{HS} \cdot \overline{PS} \cdot \overline{SSV} \cdot \overline{SST} \cdot SP \cdot LA \cdot SE \\ \overline{HS} \cdot \overline{PS} \cdot SSV \cdot \overline{SST} \cdot \overline{SP} \cdot \overline{LA} \cdot \overline{SE} \\ HS \cdot PS \cdot SSV \cdot \overline{SST} \cdot \overline{SP} \cdot \overline{LA} \cdot \overline{SE} \end{pmatrix} + \begin{pmatrix} 0 \\ \overline{HS} \cdot \overline{PS} \cdot SSV \cdot \overline{SST} \cdot SP \cdot \overline{LA} \cdot \overline{SE} \\ \overline{HS} \cdot \overline{PS} \cdot SSV \cdot \overline{SST} \cdot SP \cdot \overline{LA} \cdot \overline{SE} \end{pmatrix}$$

A simulation of third stage was done (aggregating SSV and SP attack actions). Simulation vector is given in (2).

$$S = \begin{pmatrix} F21 \\ F22 \\ F23 \end{pmatrix} = \{\overline{HS} \cdot \overline{PS} \cdot SSV \cdot \overline{SST} \cdot SP \cdot \overline{LA} \cdot \overline{SE}\}. \quad (2)$$

Generated bitstream of “0010100” was sent to the logic circuit. As it can be seen in Figure 16, primary outputs of F23 and F22 became active (shown in a red line), F21 left inactive (shown in a blue line). The primary output codes in binary and attack stages are described in Table 1.

Table 1. Primary output codes and attack stages.

Primary output code in binary			Stage number	Stage name
F21	F22	F23		
0	0	0	-	-
0	0	1	1	Recognissance
0	1	0	2	Weaponization
0	1	1	3	Delivery
1	0	0	4	Exploitation
1	0	1	5	Evasion

As shown in simulated logic circuit, primary outputs obtain values: F21 = 0, F22 = 1 and F23 = 1. That corresponds to a primary output code of S = 011, resembling a third stage number, that is named as “Delivery”.

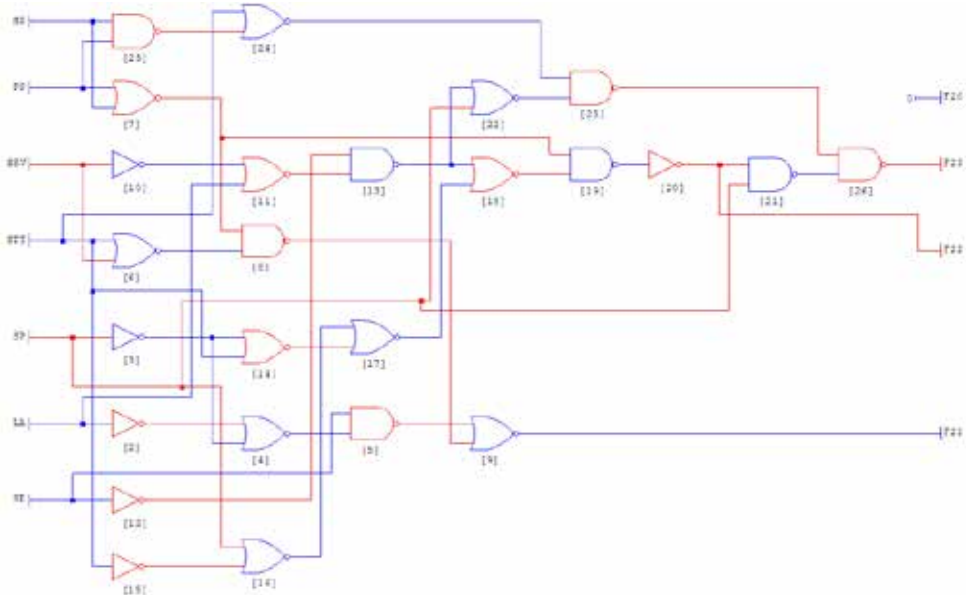


Figure 3. Simulation results. Detecting third stage – primary outputs generate a binary code of “011”.

According to the synthesized logic circuits and their simulated test results we are able to determine the early stage of the attack. This approach is a part of a large work, that is orientated to a near real-time cyber attack detection.

Conclusions. This work proposes an early warning method for a possible cyber-attack in IT and Telecommunication networks. This method is based on the use of a set of 31 logical filters. The collected information identifies features of ongoing attacks;

The set of parameters are analyzed in a proposed early-staged attacks detection system. This system collects network and system nodes information and evaluates the possible attacks stage. For early-staged detection there were provided software

implementations and hardware recommendations of the active nodes and a full Data Analysis Server logic setup;

The results of theoretical simulation have shown, that proposed method is capable of determining early-staged cyber attacks and the approach illustrates the possibility for practical method implementation;

In future works will be provided mathematical approach of the proposed method based on real computerized network data. The essence of this mathematical method would be to propose the probability of identifying the potential risk of each initial stage and evaluate the sensitivity of this model.

Keywords: communication system security; cyberspace; intrusion detection; logical circuits; telecommunication computing.

References

Weiman, G. Cyberterrorism How Real Is the Threat? *United States Institute of Peace Special Report* .2004; 119; 1-12 p. Available online: <https://www.usip.org/sites/default/files/sr119.pdf>.

Wade, M.; Maljevic, A. A war on terrorism? The European stance on a new threat, changing laws and human rights implications. *Springer*.2010; 51-78.

Ashmore, W. C. Impact of Alleged Russian Cyber Attacks. *School of Advanced Military Studies, US*. 2009.

Symantec. Preparing of a Cyber Attack. 2013. Available online: <http://symc.ly/1PHHl3n> (accessed on 02 December 2017).

Kearney, A. T. GmbH. Information Security: Preparing for the Next Hack Attack. 2013. Available online: <http://bit.ly/2vtIwkM> (accessed on 30 11 2017).

Yadav, T.; Rao, A. M. Technical Aspects of Cyber Kill Chain. *Proc. of Security in Computing and Communications: Third International Symposium on Security in Computing and Communication*. 2015; 438-452 p. doi: 10.1007/978-3-319-22915-7_40.

Husak, M. Early detection and mitigation of multi-stage network attacks. *PhD thesis, Masarykova Univerzita Fakulta Informatiky, Brno, Czech*. 2015.

Morinaga, M.; Nomura, Y.; Furukawa, K.; Temma, S. Cyber Attack Countermeasure Technologies Using Analysis of Communication and Logs in Internal Network. *Fujitsu Scientific and Technical Journal*. 2016; 52 (3); 66-71p.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Analysis of Military UAV Vulnerabilities and Losses

Saulius Japertas¹

*Kaunas University of Technology, Faculty of Electrical and Electronics Engineering, K. Donelaičio g. 73,
LT-44249, Lithuania*

Introduction. Unmanned Aerial Vehicles (UAVs) make significant contributions to the war fighting capability of operational forces. The types and capabilities of unmanned aerial vehicles (UAVs) have expanded with higher acceleration since the 9/11 terrorist attacks. The increasing number of UAV military missions also increases their losses. Unfortunately, currently there is not enough publicly available reliable data about the various civil and military drone crash accidents. Nevertheless, the information available allows us to form a certain picture of the loss of the UAV and its causes.

One of the first sources of information that provides some data on UAV crashes was “The Washington Post” [1]. It reported that about 400 US military drones have crashed since 2001 to 2014. A sufficiently large database of UAVs crashes provides [2], which cited accidents between 2007 and 2016. There are more sources of information on this issue. However, the information shows that the losses of military UAVs only increase year by year [3–5].

There are some works trying to analyze the causes of crashes. However, most of them are intended to analyze some of the specific causes of accidents. The work [6] analyses such reasons as the power propulsion, communications, losses the flight control, human factor and similar. The work [7] analyses of a large number of factors (more than 20) that were the causes of accidents and incidents in UAVs. These factors are subdivided into 5 main categories: Adverse Aircraft Conditions, Adverse Ground Support Conditions, Environmental Hazards / External Hazards & Disturbances, Abnormal Vehicle Dynamics & Flight Conditions. However, there is analyzed the technical reasons of crashes and incidents. Human factors influence to UAVs crashes is analyzed in [8]. Some incidents and accidents are analyzed in [9].

The analysis of the different works shows that the vulnerabilities can be classified differently and there have not adopted a unified classification. The works [10-12] suggest their own classification methods which differ from above-mentioned works.

Method of investigation. The work was done by data collection and analyzing the available information sources. More than 200 cases analyzed and evaluated in

¹ * Corresponding author. +37068525830

E-mail address: saulius.japertas@ktu.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania,
Engineering Managing Department

this work were collected from a number of publicly available accident investigation databases and safety reporting systems. About 50 references were analyzed.

The data collected focused mainly on military UAVs incidents and accidents. Data were collected on the events from 2004 to 2017. Data are collected from both war zones (Afghanistan, Iraq, Ukraine, etc.) and from non-war zones. Each accident and incident, event was categorized based on the suggested classification schema.

Investigation Results. The purpose of this work is to examine militaries unmanned air vehicles vulnerabilities in battlefield conditions. The unmanned air vehicles vulnerability classification and reasons of its losses in the military action zones are also investigated. Great attention is paid to smart attacks against UAVs.

As mentioned in above, the military's UAVs losses increase year by year. However, not all of these losses relate to direct losses due to military action. Part of the loss relates to such losses that are inherent in the operation of civilian UAVs. Also bearing in mind that the command and control system for UAV depends on the quality of the telecommunication channels and the sensitivity of the software and the electronics to the various impacts, it is necessary to understand the nature of such effects and the impact of UAV systems and the ability of the UAV to perform certain functions.

Three main categories of UAVs vulnerabilities are offered in this work: Physical attack, Smart attack and Miscellaneous (or Random) factors. The detailed description of these categories is provided in this work. UAVs loss reasons in battle zones and "hot" areas is provided as well. There is analyzed the smart attacks against to UAVs. It has been shown that although such attacks are increasing, their success rate is relatively small. There is proposed the algorithm to increase smart influence in UAVs.

Conclusions. The following results of the investigation were obtained:

- There is proposed the militaries UAVs vulnerability classification based on three main categories;
- It was found that UAVs the largest losses in the real battlefield consist of technical faults when smart effects are negligible despite the fact that it is widely developed a special smart measure and smart weapons;
- It is proposed that the development of smart impact of UAVs algorithms does not concentrate only on UAVs. Smart measures impact could increase if they affect to all UAVs elements of the system, even the pilot.

Keywords: unmanned air vehicles; Risk assessment, Cyber attack, Human factors, Incidents, Accidents.

References

[1] Whitlock G. When drones falls from the sky, *Washington Post*, 2014, www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky/?utm_term=.956ecdf63572.

[2] Drones wars UK. 2016. Available on: <https://dronewars.net/drone-crash-database>.

[3] McCarthy, N. Military Drone Crashes Are Climbing. 2014. Available from Internet: <https://www.statista.com/chart/2382/military-drone-crashes-are-climbing/>.

[4] King, D.W.; Bertapelle, A., Moses, C. UAV failure rate criteria for equivalent

level of safety. *International Helicopter Safety Symposium*. 2005, 1-9 p.

[5] Cole, C. What 200 military drone crashes tells us about the drone wars. 2015. Available from Internet: <https://dronewars.net/2015/02/27/what-200-military-drone-crashes-tells-us-about-the-drone-wars/>.

[6] Susini A. A Technocritical Review of Drones Crash Risk Probabilistic Consequences and its Societal Acceptance. *LNIS*. 2014; 7; 27–38.

[7] Belcastro C M, Newman R L, Evans J K, Klyde D H, Barr L C, Ancel E. Hazards Identification and Analysis for Unmanned Aircraft System Operations. *17th AIAA Aviation Technology, Integration, and Operations Conference*. 2017; 1-66.

[8] Williams K W. A Summary of Unmanned Aircraft Accident/Incident Data: Human Factors Implications. *DOT/FAA/AM-04/24; Federal Aviation Administration: Washington, DC, USA*. 2004; 14 p.

[9] Wild G, Murray J, Baxter G. Exploring Civil Drone Accidents and Incidents to Help Prevent Potential Air Disasters. *Aerospace*. 2016; 3 (22); 1–11.

[10] Hartmann K, Steup C. The vulnerability of UAVs to cyber attacks - an approach to the risk assessment. *Proceedings of the 5th International Conference on Cyber Conflict (CyCon), 4-7 June 2013*. 2013; 95-117p.

[11] Wallace RJ, Loffi J M. Examining unmanned aerial system threats and defenses: a conceptual analysis, *International Journal of Aviation, Aeronautics, and Aerospace*. 2015; 2 (4); 1-33.

[12] Borky J M. Vulnerabilities to Electromagnetic Attack of Defense Information Systems. *Information Assurance, Trends in Vulnerabilities, Threats and Technologies*, 65-92 p.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Cybersecurity in the Context of Criminal Law Protection of the State Security and Sectors of Critical Infrastructure

Miroslav Kelemen^{1*}, Stanislav Szabo, Iveta Vajdová

Technical University of Kosice, Faculty of Aeronautics, Rampova 7, Kosice 041 21, Slovakia

Introduction. The protection of state security by the legal standards of the criminal law is one of the key, the legally protected interests including the cybersecurity in the sectors of critical infrastructure: transport (road, air transport, ship, rail), electronic communications, energy, information and communication technologies, post, industry, water and atmosphere, health. An important period of strengthening the security and defense capabilities of the Slovak Republic is the practical implementation of the provisions of the New Cyber Security Act of 30 January 2018 [1]. The draft of law on the Cyber Security and Amendments to some acts no. 69/2018 Z.z. was prepared by the National Security Office of the Slovak Republic in cooperation with the Deputy Prime Minister for Investment and Informatisation. We also regard the cyber-security issues as an important part of protecting state security within the material and immaterial components of defense and protection.

The resilience of networks and the stability of the information system is a prerequisite for a smooth and the uninterrupted functioning of the EU internal market and a prerequisite for the credible international cooperation. Networks and information systems play a crucial role in free movement and are often interconnected and connected to the Internet as a global tool. The disruption of the network and information systems in one Member State therefore affects other Member States and the EU as a whole, explained the key issue the National Security Authority [2].

Method of investigation. This problem cannot be solved by one country in a comprehensive way, but a rigorous and professional international co-operation that relies on high-quality national capabilities.

The New Act transposes into the Slovak legal order a European directive on measures to ensure a high common level of network security and information systems in the Union (NIS). The NIS Directive is the first pan-European legislative regulation on cyber security that aims to strengthen the competences of the relevant national authorities, increases their mutual coordination and constitutes safety conditions for

¹ * Corresponding author. Tel.: 00421 902 040 250
E-mail address: miroslav.kelemen@gmail.com

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania,
Engineering Managing Department

key sectors as a methodological guide for Member States. This article uses the historical and content legal analysis to explore the issue.

Investigation Results. The experience of the security community confirms that the level of protection was heterogeneous and incompatible due to the mutual inconsistency of the current legal norms in which the cyber-security issue was solved partially in the conditions of the Slovak Republic, thus failing to reach the required level of EU member states. As a result, there is no adequate level of cyber security against existing threats, resulting in irreparable losses and disruptions in the credibility of organizations and the state. The goal of cyber security is therefore to minimize the potential for such threats and, in the event of the consequences, to minimize their impact, which is a prerequisite for both public administration and the private sphere.

The article presents:

- analysis of selected praxeological problems,
- and the legislative solutions of selected problems of cyber security,
- the cybersecurity as part of the security interests of the state protected by the criminal law standards.

Conclusions. The following results of our investigation were obtained:

The protection of state security by the criminal law standards is one of the key of the legally protected interests, and the cyber security is an important and indispensable part of it. Today's social empiricism confirms us that security is an important multidimensional factor of the quality of society and citizen's life, which we must systematically examine, forecast and ensure.

The importance of the topic and the use of the national defense potential is mirrored in the latest initiative under the ongoing structured EU security and defense cooperation - PESCO, with the emphasis on the cooperation and strengthening the cybersecurity capabilities. Due to the topicality and multidisciplinary, the solution of the problem will be supported also in the form of a national research project with partners. The priority is given to the security in the critical infrastructure sectors such as the transport (road, air, water, rail transport), electronic communications, energy, information and communication technologies, post, industry, water and atmosphere, and health.

Acknowledgements. This work was conducted within the framework of the Establish a national risk assessment and management of the security risks strategy. The authors are thankful for the cooperation provided by the Ministry of Foreign Affairs of the Slovak Republic

Keywords: Cybersecurity, legal norms, criminal law, protection, protected interests, state security, cooperation.

References

[1] Zákon č. 69/2018 Z.z. o kibernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

[2] LP/2017/407 *Dôvodová správa*. p. 1. Dostupné na internete: <https://www.slov->

lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2017-407

[3] LP/2017/407 Doložka vybraných vplyvov. *Dôvodová správa k návrhu zákona o kybernetickej bezpečnosti*, s.8.

[4] LP/2017/407 *Vznesené pripomienky v rámci medzirezortného pripomienkového konania*. [cit.2018-03-04]. Dostupné na internete: <https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2017/407>

[5] Kelemen, M., Blažek, V. *Obrana a krízový manažment vo verejnej správe I*. L. Mikuláš: AOS GMRŠ, 2011, 268 s. ISBN 978-80-8040-423-9.

[6] LP/2017/627 *Návrh Bezpečnostná stratégia Slovenskej republiky*. [cit.2018-03-04]. Dostupné na internete: <https://www.slov-lex.sk/legislativne-procesy/SK/LP/2017/627>

[7] Nečas, P., Kelemen, M. *War on insecurity: calling for effective strategy!* : Scientific monograph. Kiev:

The Center of Educational Literature, 2010. 158 p. ISBN 978-611-01-0023-6.

[8] Pozri: čl. 4 a 5 doterajšej *Bezpečnostnej stratégie SR 2005*.

[9] <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=25849>. [Cit.2018-03-04].

[10] Nečej, E., Žilinčík, S. *Analýza návrhu Bezpečnostnej stratégie SR 2017: Porovnanie so strategickými dokumentmi Českej republiky a Poľskej republiky*. Bratislava: STRATPOL – Strategic policy institute, 2017. 17 s. [2017-11-04]. Dostupné na internete: <http://stratpol.sk/wp-content/uploads/2017/08/BSSR-2017-SVK-v-final-OND-final.pdf>, s.5.

[11] Kelemen, M., Blažek, V. *Obrana a krízový manažment vo verejnej správe I*. L. Mikuláš: AOS GMRŠ, 2011, 268 s. ISBN 978-80-8040-423-9.

[12] Zákon NR SR č. 300/2005 Z.z. Trestný zákon, v znení neskorších právnych predpisov. Dostupné na internete: <http://www.epi.sk/zz/2005-300>

[13] Mašľanyová, D. a kol. *Trestné právo hmotné. Všeobecná a osobitná časť*. 2. vyd. Plzeň: Aleš Čeněk, 2016. 623 s. ISBN 978-80-7380-618-7. Šimovček, I. a kol. *Trestné právo procesné*. Plzeň: Aleš Čeněk, 2016. 479 s. ISBN 978-80-7380-617-0

[14] Kelemen, M. *Problems of protected interests in the security sectors: Professional and criminal law aspects of the protection of interests*. 2nd. suppl. ed. Banská Bystrica: Belianum. Matej Bel University Press, 2017. 112 p. ISBN 978-80-557-1261-1

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Security Management in the Air Transport: Example of an Interdisciplinary Investigation of Special Security Questions

Miroslav Kelemen¹, Stanislav Szabo, Iveta Vajdová

Technical University of Kosice, Faculty of Aeronautics, Rampova 7, Kosice 041 21, Slovakia

Introduction. The scientific cognition, expert education, education to professionalism and a challenging practical training of the personnel of the transport and specialised services providing and supporting its activity is rightfully in the centre of our attention. The ambition of the experts is therefore to contribute to the development of the scientific investigation and education in the field of *the security management in the transport (flight safety, security of persons and property, logistics and in the protection of the environment)* [1].

Method of investigation. The essential philosophy of the security management in the field of the air traffic service is a systematic approach to security risks and threats of the air transport. The most important component in the whole system of the security of flights is the management of the security of flights of the participants of the air traffic service. *The security of flights* is perceived as an internally integrated system of components (sub-systems) that respects its own identity (specifics, risks) and the existence of mutual relations and their connections with other areas of human activity, in line with the aim to eliminate the influence of the risk factors of a flight as well as of the service and to provide the maximum level of security of flights as a whole.

This article uses the historical and content professional and legal analysis to explore the issue [2].

Investigation Results. The term *management of the security of flights* can be defined as an active, predictive and preventive means within the range of a system of crisis management of a user of the aeronautical techniques (air operator) to eliminate the risks and solve exceptional events (situations) or crisis situations and states in the field of the security of flights.

An exceptional event (EE) in the air traffic service is understood as *a dangerous flight or ground situation* being a state in which life or health of the squad (passengers, other persons and property on the ground and in the air) or environment is threatened

¹ * Corresponding author. Tel.: 00421 902 040 250

E-mail address: miroslav.kelemen@gmail.com

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

or in which the aeroplane loses the capability to fly or the security of the air traffic service is threatened or there is a risk that it might be. It occurs in case of a technical fault of an aeroplane, failure activity of the squad, ground personnel or device or by means of the influence of external conditions during the air traffic service.

An exceptional situation is understood as a situation with a threatening or real exceptional event. The exceptional event might turn into a crisis or catastrophic situation.

Depending on:

- the conditions of the occurrence, process and consequences of a dangerous flight or ground situation,
- capabilities of flight and ground personnel or
- organs responsible for the security of the air traffic service to control these processes and perform non-standard processes, the following can occur:

an unflavoured situation – a state that requires or shall require an increased duty of the flight or ground personnel to perform the flight and provide the operation,

a boundary situation – a state accompanied with a high psychical endurance of the flight and ground personnel or with a damage to the aeroplane (property, environment) or with the limitation of the air traffic service,

an emergency (crisis) situation – a state with such a level of threat of health of the squad (passengers, personnel, ...) that the squad is not able to solve it in any other way than by an attempt to save their life by means of a crash-landing in a terrain or by means of an emergency abandonment of the aeroplane, whereby it is not possible to prevent the destruction or damage to the aeroplane (property, local damage to the environment) or in case the security of the air traffic service is threatened,

catastrophic situation – a state in which it is highly probable that the lifesaving of the squad (passengers, personnel, ...) is not possible and it is not possible to prevent the destruction of the aeroplane (property, regional damage to the environment) or in case the security of the flights within the range of the air traffic service is threatened.

A successful solution to a dangerous flight situation is dependent on an individual level of the flight preparedness of the aeroplane squad, on the amount of time available to solve the situation, on the perplexity of the situation but mainly on the right evaluation of the situation, on an early decision making and performing effective measures and processes. As a result of a dangerous flight situation, a flight incident or a plane crash may occur.

The solution to a dangerous ground situation is dependent on the state that occurred in the time except for the time defined as a flight of an aeroplane, in relation to the preparation of the aeroplane for a flight, its operation, attendance, maintenance, repairs or waiting, on the control of persons (cargo) before the flight/after the flight the result of which is damage to health, death of a person or damage or destruction of the aeroplane (property, environment) or a threat as well as a violation of the security of the air traffic service by means of an influence of the ground factors.

Conclusions. *Security management in the air transport* is understood as an integral part of the activity and the decision-making process of the managers of the

air operator and the security service, assigned to manage the security risks in the following dominant areas:

- the security of the air traffic service and
- the security of airports.

In line with the model of the situational management of selected processes (in the area of the security of flights), we accept the following types of *management* (risk management):

the management of tactical risks resulting from the usage of flight technique or security and defence measures in concrete crisis situations (terrorist attacks etc.) and

the management of operational (organisational, regime, technical, ...) *risks* that can influence the level of preparedness and the effectiveness of the applicability of the personnel.

This implies that it is desirable that the goals and tasks of the security management for the protection of persons and property in a specified environment of the air transport are realised within the range of the mentioned risk management although it is not the only frame way.

The main goal of the security management in the air transport is the operation of the flight activity, provision, protection and defence of the air traffic service with an acceptable flight security level based on an elimination, reduction or management of potential risks.

The security management in the sectors of national critical infrastructure is the important part of the protection of state interests [3].

Acknowledgements. This work was conducted within the framework of the Establish a national risk assessment and management of the security risks strategy. The authors are thankful for the cooperation provided by the Ministry of Foreign Affairs of the Slovak Republic

Keywords: Security management, air transport, air traffic services, airport security, cybersecurity, flight safety.

References

[1] Kelemen, M. Information problems of the air accidents' investigation and the prevention of the Air Force accidents: Theory and practise of forensic investigation of the crime of general threats. Boguchwala: Publishing house AMELIA Aneta Siewiorek, 2017. 171 p.

[2] Kelemen, M.: Vybrané problémy ochrany osôb, majetku a zaistenia chránených záujmov v sektoroch bezpečnosti. Bratislava: VEDA vydavateľstvo SAV, 2014, 371 p.

[3] Kelemen, M. Problems of protected interests in the security sectors: Professional and criminal law aspects of the protection of interests. Banská Bystrica: Belianum. Publishing house of Matej Bel University, 2017. 112 p.

[4] Szabo, S., Němec, V., Soušek, R.: Management bezpečnosti letišť. 1. vyd. Brno: Akademické nakladatelství CERM, 2015. 165 s. ISBN 978-80-7204-933-2.

[5] Socha, V., Socha, L., Szabo, S., Němec, V.: Air accidents, their investigation and prevention. In: eXclusive e-JOURNAL. 2014, no. 4, ISSN 1339-4509.

[6] Insider threat in civil aviation. Available at: <https://www.iata.org/policy/Documents/insider-threats-position>

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Small EU Initiatives in the Process of Pooling and Sharing of Military Capabilities

Zbyšek Korecki

University of Defence in Brno, Kounicova 65, Czech Republic

Introduction. The Pooling & Sharing project basically relies on activities related to arms and services procurement pooling, joint research background, such as sharing through the partial or full integration of the power structures, the introduction of training facilities or the establishment of joint units; and specialization. There are some practical examples of P & S in Europe: the France-UK Treaty of November 2010, which is a bilateral agreement on P & S; the vast experience of the Visegrad Group (Czech Republic, Hungary, Poland and Slovakia) and the Weimar Triangle (France, Germany and Poland). The above-mentioned cooperation examples can be more appropriately labelled as small initiatives for which the P & S model partially applies. The most important example of the “pooling” of EU Member States’ troops is the creation of the capabilities of the EU Battlegroup.

Notwithstanding these initiatives, however, the functioning of the EU P & S agenda depends on two fundamental factors that have not been fully implemented yet. The first important area is the effective liberalization of the European arms market, which will create more competition among national defence industries, where the necessary condition is the removal of national barriers, and the Europeanisation of a part of the defence budget. The other still missing area is a significant improvement in EU defence cooperation that would lead to the adoption of a concept of reduced diversification level in military equipment and technology in Europe.

Method of investigation. The methods of scientific knowledge used here based on the need of acquiring data, creating new knowledge, and continuously building on the previous knowledge and contexts of processes. Due to the amount of available book resources, the need for the ability to implement the knowledge gained due to the changes in the implementation of logistical support and the implementation of private and public sector partnership projects on a global scale has emerged. [1] The logical chain of inductive understanding [2] based on the collection of data from different sources in order to find regularity in the data obtained for the preliminary conclusions.

The historical-comparative method is based on the ability to find the same evolution of structures in the commercial sphere and subsequently implement them in the process of the armed forces in the implementation of logistic support at tactical and strategic distances. The dates of involvement of the Armed Forces of the Visegrad Group in the European Union Battlegroups were used.

Investigation Results. The Visegrad Group states, by taking a decision to create the V4 EU BG, sent a clear signal of their interest in consolidating the EU's position on the international scene [3], and the joint contribution was a practical expression of the support of the Common Foreign and Security Policy.

The creation of a joint V4 formation without the participation of a European "big" player demonstrates the maturity of states [4] and at the same time declares the ability of sub-Central European countries to cooperate within the complex political and military issues that the EU BG is building. State-of-the-art is also supported by the experience gained in previous combat groups together with experienced Union Member States. The positive development of the V4 EU BG was also the ability to offer a position to the Lead State where the Poland republic assumed responsibility for the planning, creation, training and certification of V4 EU BG, while the other participating countries respected PR authority and its responsibility towards the EU. Positive is also the finding of a consensus on the precise distribution of contributions and individual modules so as to eliminate possible shortcomings, particularly in the area of technical or logistical deficiencies [5].

Conclusions. The states of the Visegrad Group share the similarity of strategic cultures, the clarity of intentions, trust and solidarity, which are a prerequisite for the creation of sub-regional military co-operation. The level of homogeneity is given by units of similar strength and quality in the military structure, which is still low, as well as the homogeneity of the defence industry. The varying level of homogeneity of V4 states reflects the size of defensive budgets and PR dominance. Dominance is reflected not only in the budget but also in the concentration of military production capacities. However, the benefits of PR are not an obstacle to expanding military cooperation within the Visegrad Sub-Region.

Acknowledgements. This work was done within the framework of the UoD research project "Support for ACR Aviation Activities in Local Conflicts".

Keywords: pooling and sharing; smart defence, Visegrad group, EU battle group, strategic cultures, the clarity of intentions, trust and solidarity,

References

- [1] Manglig, F. Aplikační možnosti moderních simulačních systémů. [Habilitation práce], TU v Liberci, KVS (v tisku)
- [2] Manglig, F., Keller, P. Možnosti využití počítačové simulace. In: Automatizácia technologickej prípravy výroby. Odborný seminár s medzinárodnou účasťou Zvolen 17.09.1998, Zborník prednášok,
- [3] Korecki, Z., ... [et al.]. „Distribuce humanitární pomoci a udržitelnost subjektů v humanitární operaci“ - 1. vyd. - Ostrava : Key publishing s.r.o., 2015.
- [4] Korecki, Z., ... [et al.]. „Military Logistics during Operations on African Territory under the EU Flag“. - 1. vyd. - Ústí nad Labem - Střekov: Private Autonomy, 2010.
- [5] Korecki, Z., Cabicarová, M., „Logistika v humanitární operaci /Zbyšek Korecki, Monika Cabicarová – 1. vyd. –Brno: Univerzita obrany, 2014.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to National Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Contemporary Challenges to Polish Cultural Security

Mariusz Kubiak^{a1}

^aSiedlce University of Natural Sciences and Humanities, Humanities Department, Institute of Social Sciences and Security, 39 Żytnia st., 08-110 Siedlce, Poland

Introduction. The article offers a critical review of the national literature devoted to the issue of cultural security in context of its ties to national security. Author introduces the concept of cultural security, cultural identity and discusses challenges to cultural security. He argues that cultural security is a vital element of national security system as it contributes to shaping and reinforcing national identity.

Aim and methods The main aim of this paper is description and analysis of cultural security from Polish society viewpoint, especially including its contemporary challenges (chances and threats). The paper presents results of critical analysis of Polish source literature method is used.

Conclusions. The paper assesses the most important challenges to cultural security of Polish society and the state. Among them it discusses xenophobia, chauvinism, nationalism and populism. The author presents causes and consequences of each challenge to Polish cultural security. Impact of cultural security challenges is discussed in relation to national security. Contemporary examples of challenges to Polish security challenges are used to propose solutions on how to limit their negative impact on national security system.

Keywords: cultural security, cultural identity, cultural security challenges, Poland

References

Marian Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Siedlce 2007.

Wojciech J. Cynarski, *Globalizacja a spotkanie kultur*, Rzeszów 2

Jan Czaja, *Kulturowe czynniki bezpieczeństwa*, Kraków 2008.

Mariusz Kubiak, *Kulturowe uwarunkowania obronności państwa*, Siedlce 2012.

Anna Śliz, Marek S. Szczepański (red. nauk.), *Wielokulturowość: konflikt czy koegzystencja?*, Warszawa 2011.

Agata W. Ziętek (Sc.ed.), *Międzynarodowe stosunki kulturalne*, Warszawa 2010.

Paweł Żarkowski, Stanisław Topolewski (Sc.ed.), *Współczesne bezpieczeństwo kulturowe*, Siedlce 2014.

1 * Corresponding author. Tel.: +48 605550872.

E-mail address: kubmar11@gazeta.pl

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Conceptual Model for Minimization of Threats Caused by Illegal Immigrants to EU Road Freight Carriers

Margarita Marija Lietuvnikė^a, Aidas Vasilis Vasiliauskas^b, Virgilija Vasilienė-Vasiliauskienė^c, Jolanta Sabaitytė^{d1}

^{ac}*Vilnius Gediminas Technical University, Sauletekio al. 11, LT-10223 Vilnius, Lithuania*

^{bd}*The General Jonas Žemaitis Military Academy of Lithuania, Šilo g. 5A, LT-10322 Vilnius, Lithuania*

Introduction. Trending processes in certain regions of Africa, Middle East and Asia forced many people to immigrate to Europe. According to Eurostat, EU member states received over 1.39 million first-time asylum applications in 2015. There are two main paths, which are used by migrants to get to the Europe:

- the Mediterranean Sea (sea- transport);
- South-Eastern Europe road (land- transport).

After arriving to Europe's periphery, migrants apply for the asylum, or move to the predetermined countries. However, long-time frame for assessing asylum applications or frequent rejections encourages refugees to migrate illegally. During 2015, 1.82 million people were detained and arrested while attempting to cross the borders of the EU states illegally. As Europe is mainly covered by land, the illegal immigrants use land transport. From the land transport types, 27% illegal immigrants use road freight transport [1].

The intrusion of illegal immigrants into road freight vehicles to cross borders without being noticed has caused a great deal of damage to road freight transportation companies. The interruptions to road freight transport unit might disrupt the work of global supply chains [2]. It is difficult to eliminate various types of interruptions at the stage of operation [3]. The safety of the load, sent by road transport meets internal (predictable risk, e.g. a delay) and external risks (unpredictable risk, crime or hurricane). [4]. The worst risk of disruption is the one which is unpredictable, such as natural or man-made disruption, disaster or catastrophe. [5]. Because of the human ability to think, relying not only on instincts makes a person unpredictable. The unpredictability means the inability to control the future actions or ongoing processes.

The present paper provides an overview of threats which might come up from transportation as a Supply chain activity and the unpredictable human factor in transportation, which arise because of the European Migrant Crisis. Moreover, article discusses conceptual model which might be useful in order to minimize the effect of identified threats.

1 * Corresponding author.

E-mail address: Jolanta.Sabaityte@lka.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

Method of investigation. In order to reveal the magnitude of threats caused by illegal immigrants to international road freight operators a questionnaire-survey method was applied. Managers and specialists of European international freight companies that were transporting cargo to the United Kingdom were presented with questionnaires. The research was conducted verbally and in written. The questionnaire was sent to 41 representatives; however, due to only 17 fully completed and returned questionnaires, a verbal interview was carried-out to receive additional 19 questionnaires. Overall, 36 respondents took part in the research.

Investigation results. Results of conducted research prove that intrusions into the road freight transport units became better organized and planned. European road freight companies are taking preventive measures in order to reduce or avoid such incidences; however private sector is not able to control the risks of illegal immigrants through its preventive measures alone. This point might serve as initial background for the cooperation between private and public sector and joining their efforts towards elaboration of common actions necessary for solving this problem.

Conclusions. Transport and migration are inseparable from one another; however, the transfer of a person to another place, disobeying the law, is a criminal act. That's why illegal immigrants are elements of disruption risks and deliberate threat. The intrusion of illegal immigrants into road freight vehicles to cross borders of EU countries without being noticed has caused a great deal of damage to road freight transportation companies, involving property and cargo damage, physical and psychological violence against drivers, etc. Disturbances that happen because of illegal immigrant's intrusions have even more serious consequences: the disposal of cargo due to illegal immigrant intrusions into freight vehicles, termination of factory operations, dropping of sales, delays in the production, or product delivery into the market. Since intrusions of illegal immigrants became better organized and planned private transport sector is not able to control the risks of illegal immigrants through its preventive measures, therefore cooperation between private and public (public) sector is necessary. Presented model might serve as a keystone for development of such cooperation in the future.

Keywords: European migrant crisis, illegal immigrants, road freight transport units, international road freight operators, supply chain.

References

- [1]. Frontex Risk Analysis, 2016 -European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, online version: TT-AC-16-001-EN-N; ISBN 978-92-95205-46-8
- [2]. Courgeau –Andevalelievre, D. Individual and social motivations for migrations, 2016.
- [3]. Rushton A., et al. International Logistics and Supply Chain Outsourcing: From Local to Global. 2007.
- [4]. Chopra, S. et al. Managing risk to avoid supply chain breakdown , MIT-Sloan Management Review, Vol. 46 No. 1, London 2004, - pp. 53-61.
- [5]. Waters, I. et al. Global logistics: new directions in supply chain management. 2010.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Heavy Robots for C-IED Operations

Marian Janusz Łopatka

*Military University of Technology name Jarosław Dabrowski in Warsaw2 Witolda U|rbanowicza Street,
00-908 Warsaw, Poland*

Introduction. In recent years, the rapid development of combat engineer UGV, also called EOD robots and the scope of their range of uses has been observed. Their widespread use in the army was initiated by the conflict in Iraq due to the massive use of IEDs (Improvised Explosive Device). They were mainly used to the confirming the presence of IEDs, their identification and neutralization. Because the scope of the tasks carried out was similar to those performed by police pyrotechnics initially the pyrotechnic robots available on market were used for it. It quickly became clear that their usefulness is limited because their basic task was quick verification of the occurrence of a threat – usually the suspicious object was at a distance of 100-200 meters. Unfortunately, a long time to prepare the robot for work (Removal of transportation safety rolling off of the transport) and low speed (usually 1-2 km / h) did not provide the necessary efficiency of use. They were also not designed for intensive work in field conditions.

Existing EOD robots. Hence, in relatively short time the significantly lighter robots were introduced (weight approx. 20-60 kg in relation to approx. 300 kg of pyrotechnic robots) and faster (driving speed increased to 8-10 km/h) better suited to moving in a terrain. Their main purpose is recognition and identification of threats. In favorable conditions, they may also attempt neutralization. However, their capabilities in this area are much smaller than pyrotechnic robots due to the simplified manipulators construction and small lifting capacity. As a result, in American EOD subunits (*Explosive Ordnance Disposal*) with the largest experience in using robots, three types of robots are widely used:

- MK-1 – Packbot 510 (Endeavor Robotics) with a weight depending on the version;20-25 kg;
- MK-2 – Talon IV (Foster-Miller) with a weight depending on the version;50-70 kg;
- MK-3 – Andros (Northrop Grumman Remotec) with a weight depending on the version;300-350 kg.

Light robots (MK – 1, MK 2) are usually used in maneuvering operations, e.g.

as part of RCP (Route Clearance Patrol), while robots with extensive manipulation functions (MK-3) and lifting capacities up to 27 kg on the maximum range (1,4 m) are used for neutralization IEDS in urban area on firm grounds.

Heavy EOD robots. Operational possibilities of these robots are too small for effective taking and neutralization UXO (Unexploded Ordnance) - what is equally important task of the EOD subunits, because the weight of bombs and missiles can be 200-250 kg, and even up to 500 kg. Taking artillery shells and mortar grenades may also require large lifting forces at maximum range, when they are in a hard-to-reach place or driven into the ground. Additional difficulties may be caused by the necessity of digging them and removal in rough terrain. For these reasons, it is necessary to develop heavy EOD robots, with high lifting capacity and high terrain mobility – capable of long -term work in as rough terrain. Heavy robots can operate not only as intervention EOD robot but due to power, speed, payload capacity and stability they can operate as patrol robots [1,2,3,4,5].

Patrol robots should detect threats and confirm them under favorable conditions. The treats may be in the road lane (usually buried in the ground or hidden in ducts and culverts), shoulders (usually masked with various objects), in vehicles set by the roads, hidden behind or inside of infrastructural objects (junction boxes, walls, fences, ground floors, etc.) and near the road – in the case of using EFP - 50-70 m from the road. The main task of the patrol platform should be the detection of mines or IEDs located close the road and in the ground on the route of marching and their marking and determining the location. It can also verify the threat by using a patrol (reconnaissance) manipulator. The type of taken actions will depend on the tactical situation. One of the possible solutions is also not taking action and avoiding (driving around) the dangerous zone. One of the main problems for the patrol robot detection system is the lack of unambiguous characteristics of the searched objects. While in the case of mines - produced serially and in accordance with the conventions – there may be a number of characteristic shapes and the content of ferromagnetic materials, as in the case of IED, both shape, construction, material is not standard. In any case, they can take other forms and are very easily modified and adapted to local conditions which definitely makes them difficult to detect and practically eliminates the possibility of process automation. For their common feature can only be considered their considerable dimensions - comparable or much larger than anti-tank mines. The initiating systems are very diverse and are often found outside the main explosive device hence, there are often different types of wires connecting individual elements of the IED. For these reasons, the platform should effectively detect anti-tank mines and large objects hidden in the ground. The ability to detect wires, especially those connected to electronic remote control systems is also desired.

Intervention robots should be able to confirm the presence of danger on the road crown and in its vicinity, thanks to the ability to quickly reach the indicated point and the ability to remove masking materials by lifting them, pulling away or digging. In case of confirmation of occurrence, they should be able to neutralize the threat. UGVs activities should be coordinated within the robot groups. Because platforms should support the activities of motorized or mechanized subunits performing tasks as dismounted, they ought to be characterized by high terrain mobility.

Conclusions. Robotization of C-IED tasks is now a necessity due to the threats. The currently used mobile and light EOD robots are not able to effectively complete all the necessary tasks. The conducted analyzes clearly show the need for introduction of heavy robots. They are useful both during removal and neutralization of UXO, as well as during the detection, identification and neutralization of IEDs. To ensure high work efficiency it is necessary to have specialized robots forming groups. It should include patrol and intervention robots.

ACKNOWLEDGMENT

The work presented in this article has been supported by the Polish National Center for Research and Development – (Grant No. DOBR -BIO4/083/13431/2013).

Keywords: heavy EOD robot, C-IED operation, patrol robot, intervention robot, robot groups

References

[1] Blokhin Aleksandr, Koshurina Alla, Krasheninnikov Maxim, Dorofeev Roman: The Analytical Review of the Condition of Heavy Class Military and Dual Purpose Unmanned Ground Vehicle. MATEC Web of Conferences 26, 04002 (2015), EDP Sciences, 2015

[2] Bogue Robert: Detecting mines and IEDs: what are the prospects for robots?. The International Journal of Robotics Research and Application. Vol. 38 Issue: 5, pp.456-460

[3] Richardson Cedric: JIEDDO's Robotics Programs. Military Robotics Summit. 29 August 2012 *Washington* DC, USA

[4] Rogers Paul: Future Ground Vehicle Robotics. US Army Tank-Automotive Research Development and Engineering Center. 15 July 2015

[5] Robotic and autonomous system strategy. U.S. Army Training and Doctrine Command 950 Jefferson Ave, Fort Eustis, VA 23604 March 2017

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to National Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Analysis of Dismounted Operation Support with Robots

Marian Lopatka^a, Tomasz Muszynski^a

^aMilitary University of Technology, 2 gen. W. Urbanowicza Street., 00-908 Warsaw, Poland

Introduction. Increasing combat abilities and the range of tasks performed by certain subdivisions results in an upsurge in both the weight of armaments and. That problem is particularly prominent in groups carrying out their tasks on foot. It's currently estimated that a 3- day expedition requires each soldier to carry up to 75 kg of equipment, while a single day military patrol indicates a load of up to 45 kg. Single-handed carrying of such weights decidedly decreases the mobility of soldiers, thus prolonging the time needed to complete a task and lessening the probability of success. It also creates a considerable hazard in terms of battlefield survival.

In order to improve the situation, the carried weight would have to be limited to 25 kg per soldier – including standard armament, ammunition, uniforms, bulletproof vests, a helmet and personal means of connections. Other equipment necessary for fulfilling the task should be shipped via separate means of transport, moving directly with a sub-unit or a platoon, as indicated by military experience of British and American armies in Afghanistan. The forces used crossing quads with trailers (carrying capacity of 300-400 kg). That solution improved both the mobility and the combat quality of pedestrian subdivisions, but it was not devoid of shortcomings. When crossing a rough terrain, the speed of marching falls to 1-3 km/h and since the quads' powertrains were neither adjusted to such slow speeds, nor used to overcoming certain hurdles, problems arose. It is also worth mentioning that the number of soldiers ready for interventions was decreased, as drivers were forced to focus solely on steering the quads.

It can be concluded that in order to support the soldiers directly on the battlefield, one should use UGVs (robots) capable of following a guide – a selected soldier. They should navigate around obstacles autonomically and exhibit mobility close to that of an infantry soldier. The nature of performed tasks allows for qualifying them as logistic support UGVs.

Investigation Results. The tactics of logistic support robots' usage will depend on the nature of tasks performed by each subdivision. There are three main scenarios of their usage that can be predicted.

The elementary scenario consists of transporting the equipment of subdivisions on platoon level, a sub-unit, a group or a single soldier operating on foot on a rough terrain, where using standard SUVs proves to be difficult, impossible or futile. Another form of usage will be an autonomically transport of equipment between given points,

allowing for complementing soldiers' provisions or providing additional tools. The platform should then move in a coordinated way. The third nature of platform's actions will be tied to evacuating wounded soldiers from areas unsuitable for first-aid.

An example of a project of logistic support robots is a solution designed in cooperation with MUT scientists under the project "Platforma średnia (klasa 800 kg)". During shaping its constructions, following conditions were presumed:

- maximum speed - 12-15 km/h,
- climb slope - 60% (ability to drive),
- cross slope - 30% (ability to drive),
- payload - 250 kg,
- weight - 550 kg,
- turning radius (curb-to-curb)- 2,5 m,
- width - 1,25 m,
- worktime - 10 h.

Based on tasks analysis, two elementary loading standards were assumed – a military backpack (height of 70 cm, width of 35 cm, depth of 30 cm, loading mass of 30 kg) and an ammunition box (height of 17 cm, width of 35 cm, depth of 50 cm and mass of 24 kg). Moreover, possibilities of transporting the wounded on stretchers (width of 60 cm, length of 220 cm) were considered. It was assumed the platform should transport 10 ammunition boxes or 8 backpacks (payload 240 kg).

Conclusions. The developed conception will be the basis to building mobility demonstratives, which will allow for verifying the assumptions and for final shaping of the logistic support robots, which could – in the nearest future – become a part of equipment of the Polish military forces.

Acknowledgements. This work was conducted within the framework of the project "Platforma średnia (klasa 800 kg)" - grant no. DOBR-BIO4/083/13431/2013. The authors are thankful for the Polish "National Centre for Research and Development".

Keywords: mobile robot, Unmanned Ground Vehicle, UGV, logistic support, dismounted operation.

References

Studium wykonalności projektu Programu Strategicznego na rzecz bezpieczeństwa i obronności państwa pt.: Rodzina bezzałogowych platform lądowych (BPL) do zastosowań w systemach bezpieczeństwa i obronności Państwa. WAT, Warsaw 2012

Dąbrowska A., Konopka S., Przybysz M., Rubiec A.: *Ability to negotiate terrain obstacles by lightweight six-wheeled unmanned ground vehicles*. 10th International Conference ITELMS 2015, Panevėžys, Lithuania 2015

Dąbrowska A., Jaskółowski M., Krogul P., Spadło K.: *Mobility evaluation of a lightweight four-wheel unmanned ground vehicle with articulated steering system*. 10th International Conference ITELMS 2015, Panevėžys, Lithuania 2015

Dąbrowska A., Krogul P., Rubiec A.: *Co – simulation study into properties of wheeled robot hydropneumatic suspension system*. 3th European Conference of the International Society for Terrain Vehicle Systems, Rome 2015

Jaskółowski M. B., Konopka S., Łopatka M.J.: *Research of dynamic stability of articulated UGV*, Proceedings of 11th International Conference on Intelligent

Technologies in Logistics and Mechatronics Systems ITELMS'2016, Medimond Publishing Company, Panevėžys, Lithuania 2016,

Massey K: *Squad Mission Equipment Transport (SMET)*. Lessons Learned for Industry. NDIA Ground Robotic Capability Conference 2016

Patrick Lin, Ph.D. George Bekey, Ph.D. Keith Abney, M.A.: *Autonomous Military Robotics: Risk, Ethics, and Design*. Department of the Navy, Office of Naval Research, under awards # N00014-07-1-1152 and N00014-08-1-1209 December 20, 2008

Cedric Richardson : *JIEDDO's Robotics Programs. Military Robotics Summit. Washington* 29 August 2012 DC,USA, 2012

Aleksandr Blokhin, Alla Koshurina, Maxim Krashenninikov, Roman Dorofeev: *The Analytical Review of the Condition of Heavy Class Military and Dual Purpose Unmanned Ground Vehicle*. MATEC Web of Conferences 26, 04002 (2015), EDP Sciences, 2015

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Analysis of Engineer Obstacle Negotiation Possibility with Grouping Robots

Marian Janusz Łopatka

*Military University of Technology name Jarosław Dąbrowski in Warsaw 2 Witolda Ułrbanowicza Street,
00-908 Warsaw, Poland*

Introduction. Overcoming the engineering obstacles is an extremely difficult, complex and dangerous task, because the barriers are assumed to be protected (defended) by enemy fire and they consist of a variety of obstacles including:

- minefield barriers;
- wire obstacles, fences, picket holdfasts, steel hedgehogs, concrete blocks, e.t.c.;
- ground fortification barriers – antitank ditches, sidehill cuts, embankments and flooding.

Their breaching and clearance them requires ability to: making the lines in minefields by the explosive method; minesweeping; marking them; making lines in embankments and crossing ditches.

Combat engineer equipment. Because of the opponent's influence to making lines there are normally used manned, heavily armored tracked vehicles equipped with different attachments, tools and kits. The most popular are:

- mine-clearing line charge;
- mine plough, mineclearing rollers, flails;
- manipulators and excavator attachments;
- dozer and loader attachments;
- assault bridges.

Usually attachments and tools are grouped together creating specialized vehicles built on the basis of MBT (Main Battle Tank). Most commonly mine ploughs are grouped with mine-clearing line charge forming overcome mine barriers vehicles (mine-clearing vehicles) while manipulators and dozer or loader attachments create the vehicles making lines in other barriers.

Making line in extensive engineering obstacles therefore requires: mine-clearing vehicle, breaching vehicle, earthmoving vehicle and assault bridge vehicle. The weight

and the size of these vehicles is dictated by the need of the crew protection and it is not necessary for most of these tasks from point of view demanded capabilities and their stability. However large weight and dimensions limit their agility and mobility. Introduction of the remotely controlled combat engineer robots allows to reduce their weight, improve terrain mobility and also reduce the risk for crews [2,3,6].

Problems and restrictions of robotization. The limitation of robotization mainly depends from the current level of technology development [1,4,5,7]. Contemporary robots can successfully carry out repetitive activities – however they are not capable of autonomous actions requiring the robot to acquire new information, their analyses and decision making. These processes require the development of artificial intelligence. Currently used robots in order to fulfill unique tasks, requiring decision making must be controlled by man. If they work in direct operation's environment it is a sufficient solution to use remote control - the operator directly assesses the environment and controls all movements or its sequences. In case of operation at the greater distance or the occurrence of danger to the operator – the teleoperation is used. This means that the operator makes decisions and controls the robot based on the image obtained from the robot cameras. The remote control, especially teleoperation limited the operator's perceptual abilities in the area and of robot environment and location assessment and its working movements due to:

- delays occurring in the transmission path of the control signals;
- delays in image path of the robot's surroundings;
- limited viewing angle of the teleoperation system cameras;
- usually lack of stereovision - allowing quick distance assessment;
- too low image resolution due to the limited bandwidth output;
- no fillings of longitudinal and lateral inclinations of the robot and accelerations acting on the robot;
- no fillings contact between the robot and the ground;
- no fillings of vibrations and noise - allowing to assess the condition and load of the robot.

Limiting barriers requires the development of tele-presence technology.

Conclusion. Eliminating crews will allow to carry out the tasks by smaller and more mobile robots and it will increase the safety during completing tasks. Because in a remote control system, the productivity of machines in a teleoperation system is usually lower than in the case of direct control the tele-presence and new obstacle negotiation's technologies which make better use of the possibilities of relatively light robots should be developed. It is also necessary to develop the theory of managing of robot's teams, which will increase the efficiency of breaching the obstacles.

ACKNOWLEDGMENT

The work presented in this article has been supported by the Polis National Center for Research and Development – by grant DOBR -BIO4/083/13431/2013.

Keywords: combat engineer robot, mine field, engineer obstacle crossing, robot team

References

- [1] Allyn Daniel B.: The US Army Robotic and Autonomous System Strategy, US Army Training and Doctrine Command, March 2017.
- [2] Bogue Robert: Detecting mines and IEDs: what are the prospects for robots? The International Journal of Robotics Research and Application. Vol. 38 Issue: 5, pp.456-460
- [3] IED's, Mines, Route Clearance And Talisman. Think Defence. <https://www.thinkdefence.co.uk/2012/07/ieds-mines-route-clearance-and-talisman/>
- [4] Richardson Cedric: JIEDDO's Robotics Programs. Military Robotics Summit. 29 August 2012 *Washington DC, USA*.
- [5] Robotic and autonomous system strategy. U.S. Army Training and Doctrine Command 950 Jefferson Ave, Fort Eustis, VA 23604 March 2017
- [6] Rolenc Ota, Kopulety Michal: Engineer Devices for Obstacle Breaching in Offensive Operations and Possible Application of Engineer Robots. 2017 International Conference on Military Technologies (ICMT) May 31 – June 2, 2017, Brno, Czech Republic.
- [7] Unmanned Ground Systems Roadmap. Robotic Systems Joint Project Office, 6501 E 11 Mile Rd MS266, Warren, MI, 48397. JUL 2011

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Future Robots Using in C-Ied Detection

Marian Lopatka^a, Tomasz Muszynski^a

^a*Military University of Technology, 2 gen. W. Urbanowicza Street., 00-908 Warsaw, Poland*

Introduction. Modern military conflicts and actions, such as the conquering of Mosul in Iraq, Rakka in Syria and operations in Donbas, provide evidence to the rising role of using mine gropus, mine traps, as well as IEDs. In offensive actions IEDs and mines placed on roads and main communication routes prove to be of utmost importance, especially in cars and on roadsides (including buildings in direct proximity of streets). They are, however, the main source of losses in both combat techniques and live forces.

Recent years have witnessed a rapid development of engineering platforms (also known as engineering robots) and the range of their usage. It is currently predicted that they will be exploited in assymetrical actions, conflicts of low intensity and more classical combat actions. They are mainly used in following areas:

- engineering support of patrol actions of military subunits;
- engineering support of combat actions in urbanized areas;
- engineering patrol and maintenance of roads;
- realisation of EOD/IED tasks.

Investigation Results. The most complex tasks, possibly requiring whole groups of robots, are patrolling and maintaining roads – including clear-ups of mines and clearing the roads. That introduces the necessity of reconing and neutralizing any hazards on the road, the roadsides, as well as in the closest surrounding areas.

According to the conducted analyses, it is vital to be equipped with 3 types of engineering robots in the least:

- heavy engineering-recognizing robots;
- heavy engineering-intervening robots;
- light or medium-weight engineering-intervening robots of high mobility;
- UAVs (Unmanned aerial vehicle), used for scanning areas in front of motorcades and finding general hazards.

The task of the heavy engineering-recognizing robots is to find and mark points which are highly probable to be mines or improvised devices in either the crown of the road or its surroundings. An elementary kit of sensors/detectors should allow reckoning any threats in traffic lanes wider than 3 m. That task should be realized by integrated detection systems, using at least 2 types of mutually completing sensors, i.e. a georadar, cooperating with a magnet detector.

Finding threats on shoulders, in roadsides ditches, in culverts, under bridges or in

vehicles parked off the road should be facilitated by a special manipulator equipped with suitable cameras and sensors.

The area directly surrounding the road in a strip of 50-70 m width should be controlled by a special observation system. Its task is mostly finding threats EFPs or remote-controlled grenade-launchers.

It is advised for the robot to have systems allowing for activating explosive charges in front of vehicles, as well as certain elements of electronic combat, which can protect the robot from remote-controlled charges.

Considering the speed and efficiency of detection systems, the robot's speed is predicted to be 5-20 k/h. A low signature of the robot is highly desirable (volume, vibrations, ground pressure etc.), which will prevent from activating detonators. It is expected to allow, given favorable conditions, marking points of suspicion without the necessity of stopping the robot before a potential threat, thus increasing the speed of tasks completion up to 15-20 km/h.

Places marked by the heavy engineering-recognizing robots should then be verified by the heavy engineering-intervening robots. They should possess robotic abilities including:

- recognizing tensions (thin strings);
- recognizing antennae, cables, wires;
- recognizing explosive charges;
- picking up or pulling out objects, using a manipulator;
- excavating objects;
- removing cars and trucks (chassis, inside, trunk)
- checking culverts and bridges
- neutralizing IEDs, using different methods.

A light or medium-weight engineering-intervening high mobility robot is designed for completing intervention tasks in places inaccessible to a heavier robot. That can include places such as the insides of buildings in proximity of the patrolled road.

Conclusions. The battlefield of the future will be characterized by an increasing level of robotization. One should expect the introduction of entire groups of unmanned means, completing common tasks. For that to happen, though, there are still technical difficulties to be resolved. Those are mostly tied to mobility levels, detection systems, steering systems and manipulators. At the same time, new tactics should be developed alongside new technologies, in order to use them to their full potential.

ACKNOWLEDGMENT

The work presented in this article has been supported by the Polish National Center for Research and Development – (Grant No. DOBR -BIO4/083/13431/2013).

Keywords: mobile robot, engineer robot, Unmanned Ground Vehicle, UGV, EOD/IED tasks, C-IED.

References

Dąbrowska A., Konopka S., Przybysz M., Rubiec A.: *Ability to negotiate terrain obstacles by lightweight six-wheeled unmanned ground vehicles*. 10th International Conference ITELMS 2015, Panevėžys, Lithuania 2015

Dąbrowska A., Jaskółowski M., Krogul P., Spadło K.: *Mobility evaluation of a lightweight four-wheel unmanned ground vehicle with articulated steering system*. 10th

International Conference ITELMS 2015, Panevėžys, Lithuania 2015

Jaskółowski M. B., Konopka S., Łopatka M.J.: *Research of dynamic stability of articulated UGV*, Proceedings of 11th International Conference on Intelligent Technologies in Logistics and Mechatronics Systems ITELMS'2016, Medimond Publishing Company, Panevėžys, Lithuania 2016,

Patrick Lin, Ph.D. George Bekey, Ph.D. Keith Abney, M.A.: *Autonomous Military Robotics: Risk, Ethics, and Design*. Department of the Navy, Office of Naval Research, under awards # N00014-07-1-1152 and N00014-08-1-1209 December 20, 2008

Cedric Richardson : *JIEDDO's Robotics Programs. Military Robotics Summit. Washington* 29 August 2012 DC,USA, 2012

Robotic and autonomous system strategy. U.S. Army Training and Doctrine Command 950 Jefferson Ave, Fort Eustis, VA 23604 March 2017

Dr. Paul Rogers: *Future Ground Vehicle Robotics*. US Army Tank-Automotive Research Development and Engineering Center. 15 July 2015

Uran-6 Mine-Clearing Robot, Russia, Army Technology, May 29, 2016, <http://www.armytechnology.com/projects/uran-6-mine-clearing-robot/>

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Clausewitz's Trinity and Contemporary Low Intensity Conflicts (Theoretical Approach)

Leonas Lukoševičius

The General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius

Introduction. The Clausewitz's paradoxical Trinity, which, in simplified way, could be described as Army, Government and Population, from the first glance might be applicable mostly to the conventional warfare. When Clausewitz wrote this definition in his book *on War* in the nineteenth century, the battles were fought in linear manner of mass armies, if using nowadays terminology – in the First Generation Warfare. The war itself has been seen as a clash between the states. Even the following generations of warfare (Second, Third Generation) also were wars between or among the states as well. According to the military thinker Williams S. Lind, the Fourth Generation war: “seems likely to be widely dispersed and largely undefined; the distinction between war and peace will be blurred to the vanishing point... Success will depend heavily on effectiveness in joint operations as lines between responsibility and mission become very blurred.”

Clausewitz's ideas are still relevant in contemporary military campaigns. The successful military commanders and political leaders had to understand how the Trinity's entities are interconnected. This understanding allowed them to focus their efforts in order to achieve their political and military goals and their desired end-states.

The importance of the Trinity and the Centre of Gravity is clearly seen, due to their close link with one another. While the Trinity is more philosophical approach to the war, the Centre of Gravity is more practical tool, used by commanders in planning and designing of the military campaigns.

A war itself is not something static or easily understood by applying formulas or mathematical equations but is constantly changing action in time and space. Clausewitz's given definition of war in his book *on War* there are three entities of war: “primordial violence, hatred, and enmity;” “... the play of chance and probability;” “... and war's element of subordination to rational policy.” (Clausewitz C., 1989, p.89)

Even though, these three entities are different by their nature of actions, they never stand alone and are closely interconnected. They have to be balanced and have to be in support of each other in order to achieve the common goal.

The Centre of Gravity (*Schwerpunkt*): “is the hub of all power and movement upon which everything depends” (Clausewitz C., 1989, p.89). That means that the Centre of gravity is a source of all powers. The Centre of Gravity is closely linked to the Trinity.

The understanding of relations between the Clausewitz's Trinity and the Centre

of Gravity will allow commanders at all levels to achieve the desired end-state of the operation. During the campaign the Centres of Gravity may change and require commanders to change their focus and adjust their plans towards the new Centre of Gravity, otherwise the campaign may get extended in time and/or will lead to the failure or the heavy losses of the own troops.

Planning and designing campaigns commanders have to fully understand the operational environment: “How key groups in the society are organized, relationships and tensions among them, ideologies and narratives that resonate with the groups, group interests and motivations, means by which groups communicate the society’s leadership system.” (FM 3-24, 2006, pp. 1-18) Without this comprehension the commanders will be not capable to implement intelligence due to improper understanding. Proper intelligence is a key in the overall success of the operation.

Contemporary Low Intensity Conflicts are seen as the series of engagements with their latent phases and may last for decades; therefore, the Clausewitz’s Trinity is still relevant in low intensity conflicts due to their complexity. Its close link with Centre of Gravity as well as Operational Environment provides the understanding for the commanders and/or political leaders in the campaign planning.

The success of operation heavily lies on population trust and support of the government. To achieve this, every government has to assure population’s human rights, fulfilling its basic needs, such as food, water, shelter, healthcare, as well as freedom of worship and women rights. Those governments, which fulfilled those basic needs, were successful, due to population’s will to support government.

References

- [1] Clausewitz Carl – *On War*, Princeton University Press, 1989.
- [2] Lind William S., *The Changing Face of War: Into the Fourth Generation*, Marine Corps Gazette, 1989. (<http://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html> accessed on 15-03-18)
- [3] Department of Defence – *FM 3-24 Counterinsurgency*, Headquarters Department of the Army, 2006.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Visualization of Narrative Structure

Justina Mandravickaitė^{a,b1}, Tomas Krilavičius^{b,c}, Danguolė Kalinauskaitė^{b,d}

^a*Vilnius University, Faculty of Philology, Universiteto str. 5, LT-01513 Vilnius, Lithuania,*

^b*Baltic Institute of Advanced Technology, Saulėtekio av. 15, LT-10224 Vilnius, Lithuania*

^c*Vytautas Magnus University, Faculty of Informatics, Vileikos str. 8, LT-44404 Kaunas, Lithuania*

^d*Vytautas Magnus University, Faculty of Humanities, V. Putvinskio str. 23, LT-44243 Kaunas, Lithuania*

Introduction. The advantage of narrative structure over discourse is that narrative structure is specific to narrative. Discourse relations are common across domains. Thus narrative structure is well-suited to such tasks as narrative analysis and generation. Information about narrative structure could also be useful in education/teaching (e.g. automatic essay grading [8]) or detecting which blog posts (or Facebook, Twitter, online forum message, etc.) or news articles will become popular, get the most of reach or will spread the fastest. For example, if there are two Facebook posts about the same topic and written by equally well-connected persons, and one goes viral while the other does not, can we identify if there is something about the way the popular post was written that makes it a more effective narrative? Also, narrative structure could be useful for evaluating public opinion about certain ideas, events or people – their functions and roles as society perceives them.

We attempted to visualize the latent structure of narrative via sentiment analysis. Instead of shifts in narrative in terms of the topic or subject, we employed emotional shifts to mark the narrative movement [3]. In our research of narrative we follow Victor Shklovsky [2] and Vladimir Propp [8] who divided narrative into two components: the fable/story (“fabula”) and the plot (“syuzhet”). Plot refers to the technique of a narrative (structuring of the text) and fable (or story) is the chronological order of events [5]. Thus *plot* is concerned with the linear progression of narrative [1], [9]. Fable takes into consideration the specific events of a story. We focused on *plot* (the organization of the narrative) for visualization of narrative structure.

Method of investigation. We used variant of sentiment analysis for our experiment. Sentiment analysis uses natural language processing, statistics, or machine learning methods to extract, identify or characterize the sentiment content of a defined text unit. It determines a text is positive, negative or neutral. It's also known as opinion mining, detecting the opinion or attitude of a speaker/writer.

1 * Corresponding author.

E-mail address: justina@bpti.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

Our experimental setup and procedure followed the one described in [3]. For visualization of narrative structure we also used a dedicated R package for that purpose – *Syuzhet* [6]. *It was applied for the extraction of sentiment and sentiment-based plot arcs from text. This process involved a controlled vocabulary of positive and negative sentiment markers and a machine model trained to identify and score chunks of text as positive or negative. We also attempted to identify prevailing emotions (anger, anticipation, disgust, fear, joy, sadness, surprise, trust) in the text. For our experiments we constructed dictionary (work in progress) addressing sentiments and just mentioned emotions. It is based on online Lithuanian synonym dictionary² and Lithuanian Wordnet [4].*

Investigation Results. *Our experimentation included variety of text samples – fiction, news articles and transcriptions of parliamentary sittings of the Lithuanian Parliament. We had a success in detecting emotional shifts (from positive to negative and vice versa) in our text samples. Produced graphs allowed quick look into emotional valency at the sentence level as well as emotional representation of the text, i.e. generated diagrams allowed to look into emotions present in the given text as well as their prevalence (in percentage).*

Conclusions. *The results of our experiments using the above mentioned technique for visualization of narrative structure appeared promising for the more extended study in automatic narrative analysis. However, we our experimentation was limited by our dictionary developed for the purpose of narrative structure analysis that is currently work-in-progress. Thus our future plans include more comprehensive dictionary as well as adaptation of the experimental setup to be suitable for the texts in non-standard language, e.g. Facebook messages, internet comments, etc.*

Keywords: computational narrative analysis, visualization of narrative structure, sentiment analysis, narrative movement, emotional shift.

References

- [1] Aghaei, M. B. (2014). A Structural Semiotic Perspective on Narratology. *Studies in Literature and Language*, 9(2), 43.
- [2] Bann, S. (1977). Structuralism and the Revival of Rhetoric. *The Sociological Review*, 25(1_suppl), 68-84.
- [3] Gao, J., Jockers, M. L., Laudun, J., & Tangherlini, T. (2016, November). A multiscale theory for the dynamical evolution of sentiment in novels. In *Behavioral, Economic and Socio-cultural Computing (BESC), 2016 International Conference on* (pp. 1-4). IEEE.
- [4] Garabík, R. and Pileckytė, I. (2013). From Multilingual Dictionary to Lithuanian WordNet. In: *Natural Language Processing, Corpus Linguistics, E-Learning*. Ed. Katarína Gajdošová — Adriána Žáková. Lüdenscheid: RAM-Verlag, pp. 74–80.
- [5] Gervás, P. (2013). Propp's Morphology of the Folk Tale as a Grammar for Generation. In *OASICS-OpenAccess Series in Informatics* (Vol. 32). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
- [6] Jockers, M. (2017). Package 'syuzhet'.
- [7] Landauer, T. K. (2003). Automatic essay assessment. *Assessment in education: Principles, policy & practice*, 10(3), 295-308.
- [8] Propp V. (1968). *Morphology of the folktale* (1928). University of Texas Press, Austin.
- [9] Tomaščíková, S. (2009). Narrative theories and narrative discourse. *Bulletin of the Transilvania University of Braşov* Vol, 2, 51.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Design of Electromagnetic Rail Powered Missile for Penetrating Missile Defence System

Hari Prasanna Manimaran^{a1}, Naga Manikanta Kommanaboina^b, Mastan Raja Papanaboina^c.

^{abc}*Kaunas University of Technology, Studentų 56, Kaunas, Lithuania,*

Introduction. The idea of using electricity in place of gun propellant to launch projectiles is not new. It can be traced back at least as far as 1846, and there were short periods of productive research. One type of electric gun, the railgun, has demonstrated in the laboratory that it can achieve velocities of 2000-3000 m/s considerably above those normally achieved in conventional propellant guns. Such velocities can provide increased armor penetration and outmanoeuvre interceptors [1]. Each territory is protected by missile defence system (MDS). Entering the MDS is the challenging stage for any missile fired towards the target. As the launched cruise missile reaching the missile defence system shield, the heat signature of the exhaust captured by infrared (IR) satellite and the trajectory is sensed by the MDS radar. The velocity and flight path are measured and the interceptor missile are fired towards the cruising missile. The design of new kind of missile varying velocity and without heat signature can counteract the interceptor missile launched from MDS batteries.

Mission Design. The first stage is solid motor that propels the missile towards the target from the Launchpad. During the missile defence shield entering stage, onboard computer receives signal from Missile approach warning system (MAW) for the interceptor missile. The second stage of the missile is projectile launcher equipped with electromagnetic rail power by the electric power, pushes the projectile at high velocity towards the target. Flight control surface alter the attitude for the projectile trajectory. Solid motor acts as suicide missile for the incoming interceptor missile. The velocity of the projectile is higher than the velocity of missiles used in MDS makes it agile towards the target. Due to absence of exhaust, this high velocity projectile will not produce any heat signature.

Principal of working. Second stage projectile launcher works based on the Lorentz force created by the electromagnetic rail connected to the onboard power system. This rail makes the launcher behave as an electromagnet, creating a magnetic field inside the loop formed by the length of the rails up to the position of the projectile. In accordance

1 * Corresponding author. Tel.: 370-6-30-80-660.

E-mail address: hari.manimaran@ktu.edu

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

with the right-hand rule, the magnetic field circulates around each conductor. Since the current is in the opposite direction along each rail, the net magnetic field between the rails is directed at right angles to the plane formed by the central axes of the rails and the projectile. In combination with the current in the projectile, this produces a Lorentz force, which accelerates the projectile along the rails and accelerate forward with high velocity [2]. Electromagnetic rail converts electric power into kinetic energy by creating a magnetic field that accelerate projectile.

Conclusions. The following results of our design:

- Hyper velocity projectile launched towards target by electromagnetic rail mounted on the second stage of the missile;
- Projectile travels on kinetic energy produced by the electromagnetic rail avoids heat signature;
- Projectile escapes from interceptor missile and hits the target.

Acknowledgements. The design of this missile is inspired from the US navy railgun project designed by BAE SYTEMS and GENERAL ATOMICS. Authors thanks full to KTU online library and IEEE journals.

Keywords: electromagnetic rail; Lorentz force; right hand rule; missile defence system; interceptors; infrared signature.

References

- [1] McNab I. R, Stefani.F, Crawford.M.T, Erengil.M, Persad.C, Satapathy.S, Vanicek.H, Watt.T, and Dampier.C. *Development of a Naval Railgun*, IEEE EML 2004.
- [2] Harris, William. How Rail Guns Work, HowStuffWorks. Archived from the original on 17 March 2011. Retrieved 2011-03-25.
- [3] Lehmann.P, Peter.H, and Wey.J. *First Experimental Results with the ISL 10 MJ DES Railgun PEGASUS*, IEEE transactions on magnetics, vol. 37, no.01, January 2001.
- [4] Ian R. McNab, IEEE, Scott Fish, and Francis Stefani. *Parameters for an Electromagnetic Naval Railgun*, IEEE transactions on magnetics, vol. 37, no.01, January 2001.
- [5] Lehmann.P, Reck.B, Vo.M.D and Behrens.J, *Acceleration of a Suborbital Payload Using an Electromagnetic Railgun*, IEEE transactions on magnetics, vol. 43, no.01, January 2007.
- [6] Jerome T. Tzeng, IEEE *Dynamic Response of Electromagnetic Railgun Due to Projectile Movement*, IEEE transactions on magnetics, vol. 39, no.01, January 2003.
- [7] *Multiple stage Railgun*, United States Patent: 4,343,223, Aug. 10, 1982.
- [8] *Missile Defense System*, United States Patent: 5,400,688, Mar. 28, 1995
- [9] Andrew M. Sessler, John M. Cornwall, Bob Dietz, Steve Fetter, Sherman Frankel, Richard L. Garwin, Kurt Gottfried, Lisbeth Gronlund, George N. Lewis, Theodore A. Postol, David C. Wright. *A Technical Evaluation of the Operational Effectiveness of the Planned US National Missile Defense System*, April 2000.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Significant Impact of Cyber Threats to National Security

Svajone Bekesiene^{a1}, Emile Mazeikaite^b

^{ab}The General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius

Introduction. Lithuanian defence is a component part of national security. The main purpose is to create a favourable international security environment for Lithuania. Defence and security institutions system interaction, management and administration methods, the modern technology solutions – are doing big influence for making decisions and realization. Contemporary position to modern defence technology and their management is making a significant influence to the national security. These processes are controlled by defence policy principles.

The participation in democratic state creation is becoming more and more important to every citizen. The combat field and technological solutions are constantly changing. According to national cyber security, the problematic research field consist of: awareness, financial resources, technological solutions, government policy decisions and citizens' competencies. Only active, creative citizens, sustainable financing, state-of-the-art defence technologies, ability to manage these technologies in a timely and proper manner, non-confrontational policies can adequately secure the cyber security of the national security and NATO Alliance security.

Method of investigation. A qualitative study was carried out, to assess the cyber security integrity and cyber security enhancements. The empirical study of the tasks set out in the research was carried out using the expert assessment method. "The expert assessment method is a specially selected group of people who are skilled in a particular field, a specific type of survey." [1]. Depending on the requirements for the information received, expert evaluation can take various forms - from a group discussion of these individuals, to an anonymous questionnaire survey. In an empirical study, in order to assess the expert opinion in this aspect, an anonymous questionnaire survey was selected. This form has been chosen because it is the most appropriate method for getting a lot of missing information in a relatively short time.

Investigation Results. The results of the importance of cyber security for national security has shown that cyber security is directly related to national security and has a decisive influence over it. Analyzing the modern national security of cybernetics and assurance, the study found that modern technologies and cyberspace are integral parts of the direct functioning of national security of the countries, because the security of

1 * Corresponding author. Tel.: 370-6-86-48-000

E-mail address: Svajone.Bekesiene@lka.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

cyber space is protection of information from intruders, which is significant for the defence of cyber security, democracy, economy and state governance.

Conclusions. The results of our investigations show us that the national security is directly dependent on cyber security, which is supported by modern defence technologies and citizenship. Substantial further research is needed on strengthening the security potential of the cyberspace and the development, deployment and management of smart technologies use.

Key words: modern defence technology, national security, cyber security.

References

- [1] TIDIKIS RIMANTAS Socialinių mokslų tyrimų metodologija. Vilnius, 2003.
- [2] CREERY, A.; BYRES, E. J. (2005) Industrial cybersecurity for power system and SCADA networks. In: Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual. IEEE. p. 303-309.
- [3] DAVIDAVIČIENĖ V.; RAUDELĪŪNIENĖ J. (2003) Informacinių technologijų ir telekomunikacijų poveikis visuomenei. Verslas, vadyba ir studijos' 2002. II tomas : konferencijos, skirtos profesoriaus habilituoto daktaro Kazimiero Antanavičiaus (1937-1998) 65-osioms gimimo metinėms paminėti, straipsnių rinkinys. Vilnius: Technika, 2003. ISBN 9986056381, p. 125-130. [M.kr.:04S] [Aut.lankų sk.: 0.429]
- [4] DOMBROWSKI, Peter J., GHOLZ Eugene, and ROSS Andrew L.(2002.) Military transformation and the defense industry after next: the defense industrial implications of Network-Centric Warfare. Naval War College.
- [5] ISODA Vytautas, (2017) Visuomenės ontologinio saugumo samprata: Lietuvos nacionalinio saugumo ontologinė dimensija Mokslinių straipsnių rinkinys ISSN 2335_2035 (Online) VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA PUBLIC SECURITY AND PUBLIC ORDER (18)
- [6] JOHN B., STEVE S., PATRICIA O. (2011) The globalization of world politics: an introduction to international relations.
- [7] KAZLAUSKAITĖ-MARKELIENĖ, Rolanda. PETRAUSKAITĖ, Audronė. (2011). Civil Society and National Security: a Theoretical Survey of the Problem. Lithuanian annual Strategic Review. (2010–2011). P. 219–238
- [8] KAZLAUSKAITĖ-MARKELIENĖ, Rolanda. PETRAUSKAITĖ, Audronė. (2011). Pilietinė visuomenė ir nacionalinis saugumas: teorinė problemos apžvalga. Lietuvos metinė strateginė apžvalga. (2010–2011). Vilnius. LKA. P. 235–253
- [9] LIBICKI Martin, (2009) Cyberdeterrenceand Cyberwar, RAND.
- [10] LIBICKI, Martin C., (2007) Conquest in cyberspace: national security and information warfare. Cambridge University Press.
- [11] ROBSON COLIN (2007). How to Do a Research Project: A Guide for Undergraduate Students. Oxford, UK: Blackwell Publishing. Tamsin Shaw University of Leeds, UK.
- [12] SAKALAS, Algimantas. (2008). Human resources management as science and studies at KTU Economics and Management Faculty. Inžinerinė ekonomika. ISSN 1392-2785. (2008), Nr. 4 (59)
- [13] ŠTITILIS, Darius (2013) Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos.
- [14] WIENER, Norbert. (1961). Cybernetics: Or Control and Communication in the Animal and the Machine. Paris. (Hermann & Cie) & Camb. Mass. (MIT Press). (1961). ISBN 978-0-262-73009-9; 2nd revised ed.
- [15] Valvanis, K.; Vachtsevanos, G. Future of Unmanned Aviation. In Handbook of Unmanned Aerial Vehicles Springer: Dordrecht, The Netherlands, 2015; pp. 2993–3009.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Assessment of the Influence of RGO Content on the Static Strength of Silicone

Barbara Nasiłowska^{a1}, Piotr Wawrzyniak^b, Zdzisław Bogdanowicz^c, Paweł Bogusz^c, Aneta Bombalska^a, Wojciech Skrzeczanowski^a, Monika Mularczyk-Oliwa^a and Zygmunt Mierczyk^a

^a *Military University of Technology, Institute of Optoelectronics, st. Gen. Witolda Urbanowicza 2, 00-908, Warsaw 49, Poland,*

^b *TOPSIL GLOBAL, Graniczna 6, 96-321 Slubica B, Poland*

^c *Military University of Technology, Faculty of Mechanical Engineerin, st. Gen. Witolda Urbanowicza 2, 00-908, Warsaw 49, Poland*

Introduction. An inspiration for taking up a study on the plastic material issue were research in Military University of Technology on tires of road wheels for motor vehicles containing graphene. The tests showed improved adhesion and performance compared to the non-graphene tires. Currently research is being carried out in many scientific centers on the use of graphene properties i.a. microwave absorption properties) [1], high thermal conductivity and stretchability [2]. The goal of the conducted research was to determine the influence of the content of reduced graphene oxide (RGO) flakes on the structure and static tensile strength.

Method of investigation. The research on functional properties was subjected to silicone-graphene developed in cooperation with the Biomedical Engineering Center, Institute of Optoelectronics, Military University of Technology and Topsis Global company. Structural investigations were performed using the Quanta 3D FEG scanning electron microscope (FEI company). The experiment to determine the chemical composition was made by laser emission induction spectroscopy (LIBS) method. The laser beam was focused on the material samples causing its ablation, followed by heating and ionization of the occurring vapors and plasma generation. Created plasma was a source of strong continuous and discrete radiation, characteristic of atoms occurring in a given sample. Tensile strength tests were carried out on the Instron 8862 pulsator. Spectral analysis of Raman spectra was performed on a Nicolet iS50 spectrometer from Thermo Fisher Scientific company. This device is used to measure scattering spectra in the mid-infrared range and qualitative and quantitative analysis (resolution 4cm⁻¹, the range of measurements 4000-350 cm⁻¹).

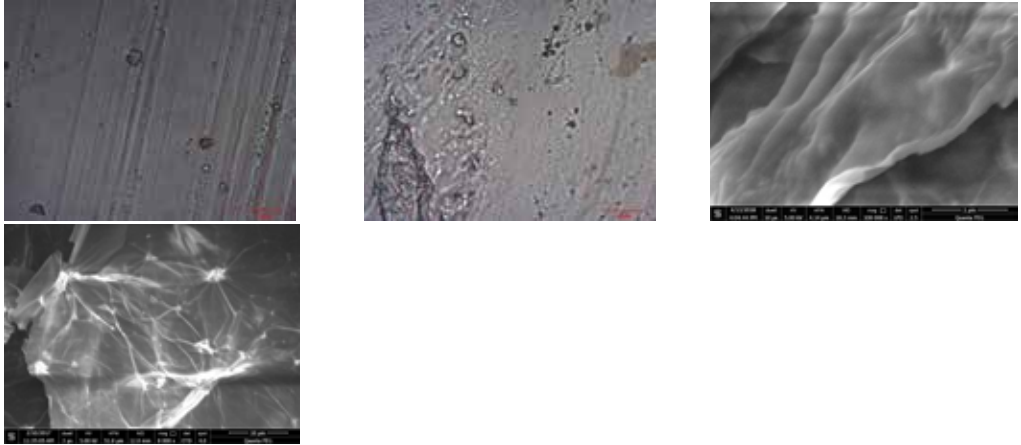
1 * Corresponding author.

E-mail address: barbara.nasilowska@wat.edu.pl

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

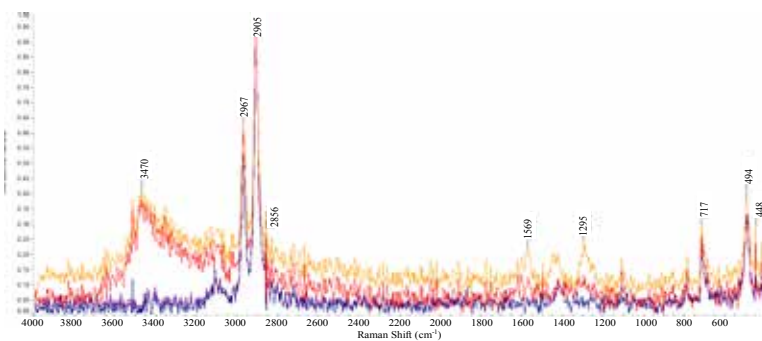
Investigation Results. The work presents structural, spectroscopic and strength tests as well as LIBS chemical composition analysis of a silicone-graphene composite. In the visual assessment, silicone-graphene was characterized by homogeneity, however, microscopic analysis performed using optical and scanning microscope showed numerous flakes of reduced graphene oxide (RGO) (Fig. 1 a, b), also located on its surface (Fig. 1 c, d).



Rys.1. Morphology of the silicone-graphene surface

Static tensile test of silicone containing reduced graphene oxide (RGO) flakes did not show any effect on static strength compared to non-RGO silicone.

All analyzed by Raman spectroscopy samples were characterized by typical spectral bands in the 2900-2970 cm^{-1} range, derived from the C-H cyclic alkanes stretching vibrations, which are part of the siloxane structure. In the 1590, 1350 cm^{-1} area, RGO bands were observed what is a confirmation of their presence in the silicone structure.



Rys.2. Raman spectra of the silicone-graphene

Analysis of the chemical composition made by LIBS spectroscopy also confirmed the presence of carbon from RGO bonds.

Conclusions Conducted structural and spectroscopic studies confirmed the presence of RGO in silicone-graphene. The static tensile test showed no negative influence of the reduced graphene oxide flakes on the tensile strength.

Keywords: Graphite/silicone composites, tensile strength, RGO, graphene

References

[1] Chen C, Pu N, Liu Y, Chen L, Wu Ch, Cheng T, Lin M, Ger M, Gong Y, Peng Y, Grubb P, Chen R, Microwave absorption properties of holey graphene/silicone rubber composites, *Composites Part B*. 2018; 135: 119-128.

[2] Song J, Chen C, Zhang Y. High thermal conductivity and stretchability of layer-by-layer assembled silicone rubber/graphene nanosheets multilayered films, *Composites Part A: Applied Science and Manufacturing*, 2018:105:1-8.

[3] Silva A, Correa M, Oliveira G, Florez-Rodriguez P, Costa C, Semaan F, Ponzio E, Development of graphite/silicone composites for use as flexible electrode materials, *Journal of Alloys and Compounds*; 2017: 691:220-229.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Undercarriage of Combat Tracked Vehicles

Vlastimil Neumann^{a1}

^aUniversity of Defence in Brno, Faculty of Military Technology, Kounicova 65, Brno, 66210, Czech Republic

Abstract. Combat tracked vehicles have an important position in the nowadays military operations. During last 15 years a battle field has changed. There is no regular army in the opposite side. The “war” has changed from the “regular battle” into a guerrilla and combat in the urban area. Improvement of the vehicle protection is current trend in construction of the combat vehicles because saving of the lives and reduction of casualties are the primary goals of commanders. Improvement of vehicle protection increases the vehicles weight and negatively influences a vehicle mobility. Increasing of the vehicle weight raises the stress of the power unit, transmission, suspension mechanism and vehicle propulsion track. From this point of view construction of the track line mechanism and suspension mechanism should keep up with the improvement of the protection.

Introduction. Combat tracked vehicles have an important position in the nowadays military operations. Massive protection, huge firepower and excellent obstacle negotiation are their main advantages. Direct combat support is their primary purpose, yet utilization of the tanks as escort vehicles of convoys was found very effective in the Afghanistan. Utilization of the combat tracked vehicles brings the “emotional” effect on the opponent units, too. On the other side the battle field has already changed. We do not expect tank battles like in 2nd world war. Nowadays we face up to terrorism. There is no regular army in the opposite side. The “war” has changed from the “regular” into the guerrilla and combat in the urban area. Assault rifles, RPGs (Rocket Propelled Grenade), mines, IEDs (Improvised Explosive Device) and suicide attacks are the main terrorist’s weapons.

Ally units had to change the tactics and the construction of the vehicles. Saving of the lives and reduction of casualties are the primary goals. Protection, firepower and mobility are the main vehicle capabilities. Improvement of the vehicle protection is current trend in construction of the combat vehicles. Utilization of the additional and slat armour are typical solutions in operations. On the other side utilization of additive armour increases the vehicles weight and negatively influences a vehicle mobility. Increasing of the weight raises the stress of the power unit, transmission system, undercarriage and vehicle propulsion track. This means that we have to focus

1 * Corresponding author. Tel.: +420 973 442 671.

E-mail address: Vlastimil.neumann@unob.cz

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

on the vehicle mobility change during the modernization process or during the vehicle improvement. Not only protection and firepower influence the vehicle survivability. Unfortunately nowadays the vehicle mobility change is not seriously take into account during the vehicle development, yet without the analysis of the vehicle mobility a producer is not able to manufacture a balanced vehicle.

Keywords: Suspension, track line, combat tracked vehicle, development.

References

[1] Neumann, V. Suspension mechanism of combat tracked vehicles. In: *Transport Means 2016*. Kaunas: Kaunas University of Technology, 2016, p. 48-53. ISSN 1822-296X.

[2] Neumann, V.; Krobot, Z. Analysis of track line parameters and their influence on track line stress. In: *Transport Means 2017*. Kaunas: Kaunas University of Technology, 2017, p. 788-793. ISSN 1822-296X.

[3] Neumann, V.; Krobot, Z.; Túró, T. Stress of a Vehicle Propulsion Mechanism. In: *International Conference on Military Technologies (ICMT)*. Piscataway, NJ 08854-4141 USA: Institute of Electrical and Electronics Engineers Inc., 2017, p. 179-184. ISBN 978-1-5386-1988-9.

[4] Ogorkiewicz, Richard M. *Technology of tanks*. Coulsdon, Surrey: Jane's Information Group, 1991, 2 v. (424 p.). ISBN 07-106-0595-1.

[5] Wong J. Z. *Terramechanics and off-road vehicle engineering: Terrain Behaviour, Off-Road Vehicle Performance and Design*, 2010, ISBN: 978-0-7506-8561-0

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

ARDL Models of Military Spending and its Security and Economic Determinants

Jiří Neubauer^{a1}, Jakub Odehnal^b

^aUniversity of Defence in Brno, Department of econometrics, Kounicova 65, 662 10 Brno, Czech Republic,

^bUniversity of Defence in Brno, Department of economics, Kounicova 65, 662 10 Brno, Czech Republic

Introduction. The NATO countries represent political and military Alliance covers 29 members. From the long term point of view, only a small group of the 29 countries fulfils the recommended values of allocating 2% of GDP at minimum in favor of defense. This paper has provided an empirical analysis of the determinants of military spending in the selected NATO countries for the period from 2001 to 2016. Empirical studies [1], [2] aimed at identifying military expenditure determinants classify those determinants into groups of economic factors, political factors and strategic factors. The first group of variables, marked as economic factors contains variables like the amount of GDP per inhabitant, GDP growth and fiscal variables. The political factors include variables like the quality of democracy, voting system, form of government, ideology and finally strategic factors covers variables describing security environment by civilian war risks, terrorism risk and by previous participation of countries in armed conflicts and participation of the country in a certain type of Alliance. We focus on modeling military expenditure in following 7 countries: Visegrad group countries (Czech Republic, Slovak Republic, Hungary and Poland) and Baltic states (Estonia, Latvia and Lithuania). Data from database SIPRI (Stockholm International Peace Research Institute) and PRS (Political Risk Service Group) are used. The aim of the contribution is to describe development of military expenditure (a percentage of GDP) by selected economic and security determinants, such as a risk for inflation, a risk for GDP per capita, a risk for foreign debt, a risk for terrorism and a risk for foreign pressures.

Method of investigation. We analyze data from 2001 to 2016. Time series under scope are too short for applying a vector autoregressive model, or a vector error correction model [10]. We employ autoregressive distributed lag model $ARDL(p, q_1, q_2, \dots, q_k)$, where p is the number of lags of the dependent variable Y_t , q_1, q_2, \dots, q_k are numbers of lags of explanatory variables X_{it} , $i = 1, 2, \dots, k$. The model can be written as

1 * Corresponding author. Tel.: +420 724 692 558.

E-mail address: jiri.neubauer@unob.cz

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

$$(1) \quad Y_t = \alpha + \sum_{i=1}^p \gamma_i Y_{t-i} + \sum_{j=1}^k \sum_{i=0}^{q_j} \beta_{j,i} X_{j,t-i} + \varepsilon_t,$$

where ε_t is a one-dimensional zero mean error term. It is possible to transform the model into a long-run representation showing the long run response of the dependent variable to a change in the explanatory variables. The long run estimates are given by [3]

$$(2) \quad \hat{\theta}_j = \frac{\sum_{i=1}^{q_j} \hat{\beta}_{j,i}}{1 - \sum_{i=1}^p \hat{\gamma}_i}.$$

The ARDL approach offers except for the dynamic description also testing of cointegration. The cointegrated system of time series can be estimated as ARDL model with the advantage that variables in cointegrating relationship can be either $I(0)$ or $I(1)$ without needing to specify which are $I(0)$ or $I(1)$ [4].

Investigation Results. Estimated parameters of ARDL models of 7 analyzed countries are summarize in the table 1. The strategy of model selection was based on AIC criterion and the parameters significance. The values of R^2 are close to 1, which means that all models are able to describe time series of military expenditures satisfactorily. It can be shown that long-run relationship exists, time series are cointegrated. Except for Poland, military expenditures are positively linked to previous value. One can see that estimated models differ, economic and security determinants are not the same.

Table 1 Estimated parameters of ARDL models

Variable	CZE	SVK	POL	HUN	EST	LVA	LTU
Milex _{t-1}	0.492	2.871	-0.349	0.730	0.512	0.273	0.415
Inflation _t	0.026	0.796	0.102	-0.054	-0.189	0.191	
Inflation _{t-1}	-0.158	-0.244	0.175	0.077			
GDP _t		-1.360					-0.248
GDP _{t-1}		0.402					-0.326
Debt _t		-1.155	0.066		0.207	0.169	0.183
Debt _{t-1}		0.482				0.234	-0.341
Terrorism _t		-0.685	0.404	-0.015		-1.796	-0.813
Terrorism _{t-1}		1.676	-0.120	-0.349		1.041	0.090
Foreign pressures _t	0.550	0.464			-2.416	-4.252	
Foreign pressures _{t-1}		0.473			-0.699	0.690	
Const.	0.130	-8.501	-1.263	1.504	10.107	11.973	5.673
R ²	0.970	0.997	0.867	0.958	0.809	0.986	0.983

Conclusions. The following results of our investigation were obtained:

- Autoregressive distributed lag model are able to describe analyzed time series of military expenditures and describe the relationship with other regressors, such as a risk for inflation, a risk for GDP per capita, a risk for foreign debt, a risk for terrorism and a risk for foreign pressures;
- Military expenditures are strongly correlated with their previous values;
- Estimated models reveal different determinants of military expenditures in analyzed countries.

Acknowledgements. This contribution was supported by FML Development Project AERO.

Keywords: military expenditure, security determinants, economic determinants, ARDL model.

References

[1] Sezgin, Y, Yildirim, J. The Demand for Turkish Defence Expenditure. *Defence and Peace Economics* 2002; 13(2), 121–128.

[2] Dunne, P, Nikolaidou, E. Military expenditure and economic growth: A demand and supply model for Greece, 1960–1996. *Defence and Peace Economics* 2001; 12 (1), 47–67.

[3] Pesaran, M H, Shin, Y. An Autoregressive Distributed Lag Modelling Approach to Cointegration Analysis. In *Econometrics and Economic Theory in the 20th Century: The Ragnar Frisch Centennial Symposium*, edited by S. Strom, Cambridge: Cambridge University Press, 1999.

[4] Pesaran, M H, Shin, Y, Smith, R J. Bounds Testing Approaches to the Analysis of Level Relationships. *Journal of Applied Econometrics* 2001; 16, 298–326.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

The New Trend - Environmental Data and Information Collection Using Unmanned Aerial Vehicles

Josef Novotný^{a1}

^aUniversity of Defence in Brno, Faculty of Military Technology, Kounicova.65, CZ-66210, Brno,

Introduction. To have the most precise possible knowledge about the area we aim to work in is one of the basic conditions and prerequisites for a successful completion of the assigned task. There is a large number of tasks, whose character determines not only applicable means for acquisition of relevant data, but also their limits. One of such means could be the unmanned aerial vehicles (UAV), a phenomenon that might present an altogether new platform for collecting a wide spectrum of environmental data. This ranges from creation of artistic photography, through online surveillance of a specific area, scanning of localities for the analysis in GIS interfaces or meteorological application. The widest employ of UAVs is in the photogrammetry field, controlling activities in places with difficult accessibility and for obtaining photo documentation e.g. during crisis management. The expansion of this domain is documented by the fact, that the International Civil Aviation Organization reacted through the issue of Annex 2, Appendix 4, which restricts (regulates) the use of UAV. There are also new programs in development that will enable processing of images from those vehicles. The outcomes may be of relatively high quality, even if a given UAV is not equipped with a cutting edge technology. And more importantly, the results can be available in a very short time comparing to the conventional technologies (aviation and satellite photography).

Acknowledgements. The work presented in this paper was supported within the institutional support for “Development of the methods of evaluation of environment in relation to defense and protection of the Czech Republic territory” (NATURENVIR) by the Ministry of Defense of the Czech Republic.

Keywords: environment, gathering data, unmanned aerial vehicles.

References

[1] De Melo, Roseneia Rodrigues Santos, et al. Applicability of unmanned aerial system (UAS) for safety inspection on construction sites. *Safety science*, 2017, 98: 174-185.

1 * Corresponding author. Tel.: 420-973445101.

E-mail address: josef.novotny@unob.cz

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

[2] Toschi, I., et al. A Survey of Geomatics Solutions for the Rapid Mapping of Natural Hazards. *Photogrammetric Engineering & Remote Sensing*, 2017, 83.12: 843-859.

[3] Adams, Stuart M.; Friedland, Carol J. A survey of unmanned aerial vehicle (UAV) usage for imagery collection in disaster research and management. In: *9th International Workshop on Remote Sensing for Disaster Response*. 2011. p. 8.

[4] Jakovels, Dainis, et al. Land cover mapping in Latvia using hyperspectral airborne and simulated Sentinel-2 data. In: *Fourth International Conference on Remote Sensing and Geoinformation of the Environment (RSCy2016)*. International Society for Optics and Photonics, 2016. p. 96881Q.

[5] Salvini, Riccardo, et al. Use of a remotely piloted aircraft system for hazard assessment in a rocky mining area (Lucca, Italy). *Natural Hazards and Earth System Sciences*, 2018, 18.1: 287.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Meteorological Application of UAV as a New Way of Vertical Profile of Lower Atmosphere Measurement

Josef Novotný^{a1}, Radek Bystřický^a, Karel Dejmala

^aUniversity of Defence in Brno, Faculty of Military Technology, Kounicova.65, CZ-66210, Brno,

Introduction. The knowledge of basic meteorological parameters such as vertical profile of pressure, temperature, humidity and airflow speed and orientation, that describe the state of atmosphere in lower levels, is crucial in terms of understanding the atmospheric behavior for a given period and consequently also for creating the weather forecast. There are several ways of obtaining such data. A majority of them, however, is in principle more complex and therefore more costly than measurements carried out on the ground within the terrestrial network of meteorological stations. In the past few years, the use of unmanned aerial vehicles (UAV) started to occur for other than camera related purposes. A broadening of measurement techniques through the aforementioned UAV is one of the newest trends of today. This way of data acquisition could be classified as a local measuring technique and direct method. Depending on the character of use of the unmanned platform, it could gather data from a significant part of low troposphere.

Method of investigation. Our unmanned vehicle falls into category of controllable vehicles heavier than air with rotary wings with electrical engine weighting less than 7 kg.

Due to its structure, the UAV Robodrone SuperHornet pertains to multi-engine vehicles (quadcopters). Besides the usual components, it also incorporates a telemetric module, suspension camera and meteorological data acquisition unit. Thanks to the used engines and accumulators, the stamina of our vehicle amounts to 20-25 minutes, 10 minutes of which would be a safety reserve. For practical application, it is therefore counted with a flight of around 15 minutes. The concept of the vehicle allows flying under conditions such as high air humidity (rain) or a wind no greater than 20 m/s. Its vertical speed had been limited to 5 m/s, taking into account the capacity and discharge rates of accumulator. Bearing that capacity in mind, the flights could be, theoretically conducted up until around 8200 ft (2500 m) above ground level (AGL). In respect of legislative limitations we can fly the vehicle in experimental mode in several designated areas up to 5000 ft (1500 m) above mean sea level (AMSL) provided a reserved air space of 3 km radius.

1 * Corresponding author. Tel.: 420-973445101.

E-mail address: josef.novotny@unob.cz

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

The aim of the experiments is to approximate to the measuring conditions of meteorological balloon probe. The flights consist of a simple constant-speed ascent to the maximum height and back, while holding the same geographical coordinates. Even at the designing phase, it was clear, that the air turbulence around propellers would cause diversions in measured values, especially in the case of temperature. In order to stave off this negative effect a cheap meteorological data acquisition unit had to be installed. It serves to determine the impact on each given sensor and to find an appropriate location so that the impact in the course of flight is minimal. The key point in the development stage turned to be the choice of sensors with a very small time constant, as only the proximity of ground before the take-off can heat up or cool down the sensors by several degrees.

At present, the drone is fitted with pressure and humidity sensor BME280 by Bosch, which communicates via I2C interface. It measures humidity from 0 % to 100 % and pressure from 300 hPa to 1100 hPa with definition 0,008 % for humidity and 0,18Pa for pressure. The precision in the case of humidity is $\pm 3\%$ and $\pm 1\text{Pa}$ for the pressure. Additionally, it comprises a platinum temperature sensor 701-101BAA-B00 by Honeywell with measuring range of $-70\text{ }^{\circ}\text{C}$ to $500\text{ }^{\circ}\text{C}$ and definition that thanks to the used processing chain amounts to $0,001\text{ }^{\circ}\text{C}$. At this point, the air direction and airspeed data are not usually available, but we try to obtain those experimentally through calculation from measured position angles. The preliminary results are quite promising.

Investigation Results. The comparison of temperature and relative humidity during flight was performed on three locations - airport Brno Medlánky, military training area Libavá and aerological station Prostějov. The testing focused on the different placement of sensors. When the measured data could not be compared to the real data and the tests were only limited to repetitiveness of value retrieval during different flight conditions, the tests pursued the accord between measurements taken during vertical ascent and descent with varying vertical speeds. Since there is usually no significant change of meteorological conditions in the course of minutes, the values obtained at the same position should correspond.

For a more precise comparison, however, it is necessary to perform the comparison with real data. This took place in Prostějov, where the drone and meteorological probe with sensors by company Vaisala placed on a balloon were made to take off simultaneously. Another advantage of this measurement was the fact, that an identical probe to the one placed on the balloon could have been placed on the drone too. A complication to such comparison though is constituted in the raw-data processing from Vaisala in software on a processing device. A limitation of the comparison with upper-air sounding is the interval: only twice a day (every 12 hours), while utilization of supplementary probes is financially very demanding.

Another possibility for comparison would be to use a 250 m high meteorological pole in Křešín (Pacov area), on which the sensors are positioned by every circa 50 meters. This distance is very rough, but the pole gives an advantage, that during one day several comparison measurements may be carried out. This possibility is though still in negotiation.

Conclusions. The development and comparison brought about the following results. The selected temperature sensors have a considerably lower inertia than the

ones originally tested. Instead of one, there are two sensors installed on the drone (one up, the other down), so that the varying influence of the drone on the temperature measurement during ascent and descent is eliminated. The development phase also exposed some software problems, which contributed to an incorrect determination of flight height. It appears (not only in comparison with Vaisala probe), that in order to get the real data with requested precision the collected data will have to undergo a post-processing. Another problem encountered during temperature measurement is a variable offset. Similarly, to the case of Vaisala probes, a calibration / temperature levelling will be necessary to do before the flight so that the corresponding values may be collected.

Acknowledgements. The work presented in this paper was supported within the institutional support for “Development of the methods of evaluation of environment in relation to defense and protection of the Czech Republic territory” (NATURENVIR) by the Ministry of Defense of the Czech Republic.

Keywords: unmanned aerial vehicles, aerological sounding, troposphere, meteorological parameters, accuracy of measurement.

References

- [1] Dejmál K, Hudec F, Kolář P, Novotný J. Evaluation of measurement quality of selected elements on the meteorological stations Meteos6 and Davis Vantage Pro 2 in the military quarters area of Černá Pole. In: Conference Proceedings of ICMT'17. Piscataway, NJ 08854-4141 USA: Institute of Electrical and Electronics Engineers Inc., 2017, p. 318-324. ISBN 978-1-5386-1988-9
- [2] Dejmál K, Almášiová L. The comparison of temperature and moisture characteristics of natural and artificial surfaces. In: Central Europe Area in View of Current Geography. Proceedings of 23rd Central European Conference. Brno: Masarykova univerzita, 2016, p. 141-148. ISBN 978-80-210-8313-4.
- [3] Bystrický R, Novotný J, Dejmál K. Use of the climatic chamber for meteorological drone validation. In: 17. International Scientific Conference „Measurement, Diagnostics and Dependability of Aircraft Systems 2017“. Brno: University of defense, 2017, s. 50-59. ISBN 978-80-7582-012-9.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Utilization the New Advanced Structural Materials in the Military Vehicles and Heavy Equipment

Tomasz Ślęzak^{a1}

^a*Military University of Technology, Faculty of Mechanical Engineering, ul. gen. W. Urbanowicza 2, 00-908
Warsaw, Poland*

Introduction. A force protection and preservation of the mobility are ones of the most important issues which must fulfill the military equipment within the battlefield or widely, on the combat zone. The combat vehicles, means of conveyance or equipment of supporting units must be designed with taking into account their destination and basic tasks that should be done. In each case they move through the combat zone on roads, tracks or cross-country, when the ability to move in the last one case is always necessary. Nowadays, the requirements of appropriate protection level are defined not only for combat vehicles, weapons carriers or personnel carriers but also as an option for logistic vehicles operating in areas when can be endangered by fragments from artillery indirect fire or rifle firing. Additional armor always increases the total weight of the unit and make worse the ability of forces to movement on the battlefield. For this reason, it is necessary to use on a ballistic armor protective system the novel lightweight materials like ceramics, composites or nanomaterials. They are characterized by higher level of protection simultaneously with decreased specific weight. On the other hand, these materials are very characteristic and cannot be joined by using welding technologies and other are insufficient. Therefore, full-sized elements of structure like crew hatches or ramp doors are manufactured, otherwise shaped protective panels are mounted by using screws, rivets or special mounting systems. The weight of military vehicles is increasing despite the use of new protective materials. For this reason, self-supporting structures of the vehicles or frames are designed and made of high strength steels. The usage of steel is necessary because it is much better weldable than other structural alloys.

Composites, ceramics and nanomaterials. The exigency to ensure suitable level of mobility and protection cause that many modern protective materials are developed. Homogenous steel armors occur nowadays mainly in old structures and they have low efficiency against kinetic energy penetrators and high-explosive anti-tank (HEAT) warheads. For this reason, the new layered armors were developed and they consist of a few different layers of steel, ceramic or composite. The ceramics are characterized by an extremely high hardness. Consequently, a penetrator is damaged through

1 * Corresponding author. Tel.: +48 261-837-685.

E-mail address: tomasz.slezak@wat.edu.pl

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania,
Engineering Managing Department

fragmentation or blunting but the ceramic elements crumble due their brittleness almost every time. What is important the ceramic is not used independently but always together with other materials, i.e. steel, aluminum or fibers composites creating composite armors [1-2]. Other group of protective materials is created by special steels. Except common known hard armor steels i.e. Armox [3] there were developed the grades of maraging or bainitic nanostructured steels [4-5]. These grades of steel have high hardness and what is more important ultra-high strength above 1.8 GPa with good ductility. The steels destroy or stop the projectile by absorption of kinetic energy and their dissipation in panels. Composites are the last group among the considered. They are mainly used in the body protection solutions or in lightweight military vehicles. The composites have different configurations from above mentioned ceramic-metallic system to compact nano-composites joining various materials to achieve lower weight and higher protection [6]. One of the specific solution of light materials with higher ballistic resistance are laminates from alloys of titanium and aluminum obtaining by explosive welding [7-8].

High strength steels. Higher weight of the military vehicles cause that the structure must be fabricated of steels with high strength and acceptable weldability. The yield stress of those steels reach the value of 1100 MPa or even above [9]. Besides the vehicles these grades of steels are utilized in special military structures i.e. the military assault and supporting bridges, extremely loaded elements and mechanisms or the trailers for heavy vehicles transportation [10-11]. Nevertheless, a production process exploiting welding technologies must be performed very carefully. There are numerous problems with connecting the high strength steel i.e. a choice of proper junction's shape and welding parameters, a quality of weldments and the properties of a parental material. All above factors are crucial for obtaining high quality product meeting all requirements.

Keywords: armour, ceramic, nanomaterials, high strength steel,

References

- [1] Cegła M. Ceramic materials for armor applications. *Problemy Techniki Uzbrojenia* 2014; 131: 19–25.
- [2] Matchen B. Applications of Ceramics in Armor Products. *Key Engineering Materials* 1996; 122-124: 333–344.
- [3] <https://www.ssab.com/products/brands/armox>
- [4] Wiśniewski A, Garbarz B, Burian W, Marcisz J. Composite space armours with the bainitic-austenitic and maraging steel layers. *Problemy Techniki Uzbrojenia* 2013; 128: 33–41.
- [5] Garbarz B., Marcisz J., Adamczyk M., Wiśniewski A.: Ultrahigh-strength nanostructured steels for armors. *Problems of Mechatronics. Armament, Aviation, Safety Engineering* 2011; 2 (1): 25–36.
- [5] Burian W, Marcisz J, Garbarz B, Starczewski L. Nanostructured Bainite-Austenite Steel for Armours Construction. *Archives of Metallurgy and Materials* 2014; 59(3): 1211–1216.
- [6] Ávila A F, Neto A S, Nascimento H Jr. Hybrid nanocomposites for mid-range ballistic protection. *International Journal of Impact Engineering* 2011; 38: 669–676.
- [7] Szachogluchowicz I, Sniezek L, Mierzynski J, Koperski W. Experimental

study on ballistic AA 2519 / Ti6Al4V laminate according to STANAG 4569 Level 1. *Proceedings of 11th International Conference Intelligent Technologies in Logistics and Mechatronics Systems* 28-29 April 2016, Panevėžys, Lithuania, pp. 155–163.

[8] Lazurenko D V, Bataev I A, Mali V I et. all. Explosively welded multilayer Ti-Al composites: Structure and

transformation during heat treatment. *Materials and Design* 2016; 102: 122–130.

[9] Gresnigt A M, Steenhuis C M. High strength steels. *Steel Construction* 1997; 1: 31–41.

[10] Raczyński Z. Badania parametrów wytrzymałościowych przęła mostu MS-40. *Szybkobieżne Pojazdy Gsienicowe* 2015; 36: 99-113 [in polish]

[11] Morada P. Examples and applications of high strength steel. *by webpage*: www.oakleysteel.co.uk/examples-applications-high-strength-steel

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Electronic Defence Systems Comparison: Nato and Russia Case

Jolanta Sabaityte^{a1}, Aušrius Juozapavičius^b, Pranas Karčiauskas^c

^{ab}*The General Jonas Žemaitis Military Academy of Lithuania, Šilo g. 5A, LT-10322 Vilnius, Lithuania*

Introduction. Electronic warfare (EW) is currently one of the most relevant ways of fighting. This is a fast developing fighting technique, since modern battles use modern weapons and technology. And most countries, realizing that they cannot catch up with the modernization of their military equipment by one or other country, are investing heavily in an electronic warfare, which is precisely counter the technology's advantage. Although the electronic warfare was used since before the First World War, this is quite new field in Lithuanian Armed Forces. But Lithuania should not be an exception, having a powerful and aggressive neighbor Russia. Electronic warfare is one of the areas that can help win against a more modern and powerful opponent. Therefore, it is very important to understand the capabilities of Russia and NATO in the field of electronic warfare. And further use this knowledge in order to evaluate current situation in this field in the Lithuanian Armed Forces and improve it. The object of the research is electronic defence systems capabilities. The aim of this research is to investigate the electronic warfare systems capabilities of NATO and Russia.

The Concept of Electronic Defence Systems. The electronic warfare is described as actions taken using the electromagnetic spectrum or weapons whose main destructive mechanism is based on electromagnetic spectrum or direct energy (lasers, directed-energy weapons), in order to control the electromagnetic spectrum, to use electromagnetic spectrum to damage the enemy's forces or to counter the enemy's electronic attack.

Although electronic warfare has been known for a while, but the most striking electronic fighters have become the British warriors during the first year of the Second World War, when they interfered the German bomber navigation (Thurbon, 1977). Later during this war Germans and British realized that electromagnetic spectrum control was the key to the successful end of the war. Also, it is worth to mention, that the main breakthrough in the Second World War was when the Allies landed in Normandy was due to the electronic fight – the electronic communication tools were used in order to deceive the opponents mistakenly providing information about the landing in Pa-de-Calais, northern France (Williamson, 2015). It can be argued that the

1 * Corresponding author.

E-mail address: Jolanta.Sabaityte@lka.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

electronic warfare tools were used more frequent in the army with the emergence of radio and radars, and eventually it was called electronic defense systems, which main goal is to disrupt the enemy's communication and to protect the communication of own forces, and to disrupt or deceive the radar data.

In order to get deeper understanding of electronic warfare, it is crucial to determinate the components of its system. The analysis of literature revealed that system consists of these elements: electronic attack, electronic protection and electronic warfare support

NATO's and Russia's Electronic Warfare System Capabilities. Most of the advanced EW equipment is currently implemented on ships and airplanes (such as AN/ALQ-99) and the capabilities of the land forces are lagging behind. Under the leadership of the United Kingdom the EW units of six NATO countries have been performing regular exercises in order to achieve interoperability: 14th signal battalion of UK forces, U.S. 103d MI Battalion, the Royal Netherlands Army's 102d EW Company, the Royal Danish Army's EW Company, and the German Army's 320th regiment. Taken together they amount to an estimated 3.5 thousand personnel. In general, standardization and interoperability issues remain a challenge within the 29 NATO nations.

A major reform of Russia's Armed forces from 2008 to 2015 put the EW capability development into focus. EW units became an integral part of all formations of the land forces including EW sub-units in assault divisions. Currently there are five EW brigades and two of them in the Western Military District (in Tula and in Kursk) [6]. Taken together this amounts to 15 thousand soldiers. As opposed to NATO forces, Russia does not need to deal with interoperability issues as all the EW units, tactics and equipment follow the same standard and can be integrated and interchanged.

Conclusions. The Electronic warfare is described as a system, consisting of electronic attack, electronic protection and electronic warfare support. The aim of the system it is to take actions using the electromagnetic spectrum or weapons whose main destructive mechanism is based on electromagnetic spectrum or direct energy (lasers, directed-energy weapons), in order to control the electromagnetic spectrum, to use electromagnetic spectrum to damage the enemy's forces or to counter the enemy's electronic attack. The main criteria for assessing EW capabilities should be: human resources, possibilities of integration into existing system and also possibilities of use, frequency range, mobility and operating distance.

The analysis of NATO Electronic Warfare System revealed that most of the advanced EW equipment is currently implemented on ships and airplanes and the capabilities of the land forces are lagging behind. The main issues within the 29 NATO nations remain standardization and interoperability. The analysis of main EW systems employed by NATO was carried out.

The analysis of Russia's electronic warfare capabilities revealed that the focus on this system was put by the major reform of Russia's Armed forces from 2008 to 2015. Comparison of NATO and Russia EW systems revealed that unfortunately, but Russia's EW systems are superior in human resources, possibilities to use and frequency range

Keywords: Electronic warfare, NATO, Russia, electronic attack, electronic defense systems.

References

- [1] Thurbon, M. T. (1977). The Origins of Electronic Warfare. *The RUSI Journal*, 122(3), 56–63. <https://doi.org/10.1080/03071847709428739>
- [2] Williamson, M. (2015). “Jamming” operations for D-Day. Retrieved November 30, 2017, from <https://weaponsandwarfare.com/2015/08/12/jamming-operations-for-d-day/>
- [3] Mj. McPeck. Electronic Warfare British Style. Retrieved from <https://fas.org/irp/agency/army/mipb/1996-1/mcpeek2.htm>
- [4] AN/PRD-13(V)2 Man-portable signals intelligence system. Retrieved from [http://www2.l3t.com/linkabit/pdf/datasheets/PRD-13\(V\)2_Datasheet_OSRAproved_Web.pdf](http://www2.l3t.com/linkabit/pdf/datasheets/PRD-13(V)2_Datasheet_OSRAproved_Web.pdf)
- [5] SMARTSCAN ° MEWS Modular Electronic Warfare System for Joint Operations. Retrieved from <https://www.cybertrl.com/Uploads/Brochures/cyber/Smartscan-Mews-Datasheet.pdf>
- [6] McDermott, R. (2017). *Russia’s Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. Retrieved from https://www.icds.ee/fileadmin/media/icds.ee/doc/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf
- [7] Clark B. et al. (2017). Winning In The Gray Zone: Using Electromagnetic Warfare To Regain Escalation Dominance, CSBA.
- [8] Donetsk. Russian “Torn” And “Taran” Radio Intelligence Systems at “Sparta” Base. Retrieved from <https://informnapalm.org/14245-radyorazvedka-ukv-dyapazona-na-baze-sparta/>.
- [9] 1L267 Moskva-1. Retrieved from <http://militaryrussia.ru/blog/topic-770.html>.
- [10] Automatic jamming station R-330BM. Retrieved from <https://topwar.ru/128706-avtomaticheskaya-stanciya-pomeh-r-330bm.html>

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Experimental Study on Ballistic AA 2519 –AA 1050 -Ti6Al4V Laminate According to STANAG 4569 Level 2

Ireneusz Szachogluchowicz^{a*}, Lucjan Sniezek^a, Marcin Wachowski^a,
Volodymyr Hutsaylyuk^a, Wojciech Koperski^a

^a*Mechanical, Military University of Technology, gen. W. Urbanowicza 2 str., 00-908 Warsaw, Poland*

Introduction. In case of specialized and civilian structures operated in environments with high risks of appearing dynamic effects of foreign particles it is extremely important for the material used to have the highest ballistic resistance as possible. One of the methods of obtaining these types of materials is to combine materials with different properties. Composites acquired this way are amongst the most promising materials with potential applications in the industry [1,2]. One of the intensively developed modern methods of producing layered composites (laminate) is explosive bonding. Composites obtained this way consist of two or more materials and often have unique application properties, including substantial ballistic resistance [3,4]. The aim of this study is to evaluate the applicability of the explosive welding technology for the production of a new material in the form of a laminate of titanium alloy (Ti6Al4V) and aluminum (AA2519) and to investigate the ballistic resistance of base materials and sandwich panels designed to small caliber and rifle fire during dynamic tests (shooting) [5-7].

Dynamic tests were carried out on plates with a thickness of 7.5-15,0 mm which were fired upon from Bz-7.62 mm projecting system with adjustable kinetic energy. The analysis of samples was carried out in accordance with the approved program and research methodologies, according to current standards, including the STANAG 4569 standard [8].

Method of investigation. The concept of research of dynamic (firing) base materials and panels made of composite material developed assumed testing sandwich panels made by putting together panels AA2519-Ti6Al4V combined method of explosive. Shelling samples followed from the titanium-type missiles BZ rifle cartridge 5,56x45 mm in conditions complying with the class II STANAG 4569.

The concept includes research:

- testing during the shelling of base materials AA2519 and Ti6Al4V,
- 2) testing during the shelling of triple layered panels. Each layer of the panel is composed of a laminate of AA2519-Ti6Al4V thickness of 11 mm. The

combination of materials of AA2915 and Ti6Al4V was executed by the method of explosive bonding the interlayer using an alloy AA1050 with a thickness of about 0.8 mm. The distance between the layers for the first ballistic tests was 15 mm. This study assumed fire panels from the Ti6Al4V alloy. These results enabled to estimate the number of layers of the panel, necessary to avoid the puncture.

- testing fire base materials and firing double sheets and sextuple panels made of a laminate AA2519-Ti6Al4V where the distance between the plates was 15 mm. The panels are configured with a laminate layer of dimensions 200x120x20 mm and 200x120x7 mm. Stand for testing ballistic resistance basis materials and developed layers panels shown in Fig.4.Fig.5. This position used to fire the samples in the laboratory missiles BZ (7,62x39 mm) rifle cartridge.

Rifle 7.62mm model 1944 was placed on the bench in order to ensure that you get hit in the designated area of the sample. Before each test checks for proper mounting arms and putting the barrel axis relative to the sample. During the shot distance of the muzzle of the sample was 2.5 m.

Investigation Results. The mechanism of material penetration by the projectile is the same for each case. On the surface of the aluminum alloy around the inlet opening creates a crater with the effect of flaking resulting from the ejection of the material. During the tests, it was found that the laminate AA2519-AA1050-Ti6Al4V presents the characteristics of materials used for ballistic shields. Panels made of laminates in the initial condition show greater ballistic resistance than panels subjected to additional heat treatment. It has been noticed that in one and the other variant laminates due to multiple shots tend to delaminate. Therefore, the microstructure of bullet holes was investigated. Damage to the AA2519 alloy panel is characterized by the occurrence of local deformations of the face of the panel layers due to the penetration of the ogive penetrator. The result is the occurrence of outflows at the edges of the crater formed resembling flower petals called frontal petalling. It is caused by the occurrence of high radial and circumferential tensile stresses after passing the instantaneous wave of stresses generated in the vicinity of the penetrator.

Acknowledgements. The project is carried out under Project PBS2/A5/35/2013 funded by the National Research and Development Centre and PBS applied research program.

Keywords: explosive welding, cladding, composites, alloy, aluminum, 2519, titanium, Ti6Al4V, ballistic resistance, STANAG.

References

- [1] Nasilowska, B.; Slezak, T.; Sniezek, L., Torzewski J., Mechanical Properties of Laser-Welded Joints in the Difficult-to-Weld Steels, *Intelligent technologies in logistics and mechatronics systems itelms* 2013, 173-178p.
- [2] Slezak, T., Sniezek, L., A Comparative LCF Study of S960QL High Strength Steel and S355J2 Mild Steel, *International Conference on Structural Integrity ICSI*

2015, Vol.114, 78-85 p.

[3]. Szachogluchowicz, I., Sniezek, L., Gocman, K. The mechanical properties of composites AA2519-Ti6Al4V obtained by detonation method. – Intelligent Technologies in Logistics and Mechatronics Systems ITELMS'2014, Proc. of The 9th International Conference edited by Z. Bazaras and V. Kleiza, 2013, p. 214–219 .

[4] Szachogluchowicz, I., Sniezek, L., Hutsaylyuk, V. Research of Property Fatigue Advanced Al/Ti Laminate. – Intelligent Technologies in Logistics and Mechatronics Systems ITELMS'2014, Proc. of The 9th International Conference edited by Z. Bazaras and V. Kleiza, 2014, p. 232–238.

[5] Abrahamson, G. R. Residual periodical deformations of surface under action of moving jet. – Proc. of ASME, Ser. E, Appl. Mechanics, 1961, Vol. 28, No. 4, p. 45–55.

[6] Cowan, G.R., Holtzman, A.H. Flow configuration in colliding plates: explosive banding. – J. Appl. Phys. 1963, Vol. 34, No. 4, p. 928–939.

[7] Cowan, G.R., Bergmann, O.R., Holtzman, A.H. Mechanism of Bond Zone Wave Formation in Explosion Clad Metals. – Metallurgical Transactions, 1971, V. 2, No. 11, p. 3145–3155.

[8] Szachogluchowicz, I; Sniezek, L.; Mierzynski, J., Koperski, W., Experimental study on ballistic AA 2519 / Ti6Al4V laminate according to STANAG 4569 Level 1, 11th International Conference on Intelligent Technologies in Logistics and Mechatronics System (ITELMS), 155-163p. , 2016.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Knowledge Management in Military: a Systematic Review

Rasa Smaliukiene^{a1}, Vidmantė Giedraityte^a

^aThe General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius

Introduction. Information management for decision making already exist within military for many years. However, the conversion where information becomes knowledge remains fracture. The most valuable implicit knowledge resides in the heads and offices and is not always converted to retrievable formats. At the same time, it should be noted the growing amount of current studies within an emphasis on knowledge management in military. The studies take different paradigms and represent perspective of management, social networking, organizational psychology, information technology and other fields towards phenomena of knowledge in military and its management practices.

The objective of this study is to review current research on knowledge management in military and to identify the main streams where research is performed. Although previous studies on knowledge management in military have presented some literature overviews, this study is the first to provide a systematic analysis using term mapping.

Method. Systematic literature review is used as a method for this study. The data consist of theoretical, analytical and research papers retrieved from Web of Science (Clarivate Analytics) and Scopus databases up to 2018. The only articles covering knowledge management issues in military are selected for the analysis. The data are analyzed using the software tools for constructing bibliometric networks. These networks are visualized and interpreted using general trends in knowledge management development.

Results. Three streams (conceptual categories) are identified in the analysis. The first and the biggest stream of research embodies management sciences and is represented by papers in leadership, strategic management as well as other field of military management. The papers analyze how knowledge management is used in planning and executing military operations. This stream provides new approaches developed by investigating the emerging trends for knowledge exchange in military decision superiority (Bannister & Byrne, 2013), as well as classical military theories are reexamined using knowledge management perspective (see Boe, 2014). The second

1 * Corresponding author. Tel.:

E-mail address: rasa.smaliukiene@lka.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

stream consists of papers from highly diverse fields where emphasis is made to integrate different approaches and develop new attitude in military knowledge management. The researchers take the most challenging issues in military and provide new solutions. As sense making, decision making and learning are identified as a major activities where knowledge creation take place in military (Mattila, 2016), an integration of these activities are a primal focus of the research. The third stream represents studies performed in the paradigm of system management. The stream reflects a range of technical solutions and best practices in knowledge management system development. Multiagent system to combat terrorism (Galka et al., 2009), fuzzy cognitive maps as a mediator in decision making (Perusich & Mcneese, 2006) and other solutions are presented in the papers of this stream.

Conclusions. We conclude that knowledge management research in military is performed in three streams where new ideas and solutions are developed. The largest stream represents management science paradigm. The second largest stream is created by researchers from diverse disciplines. This stream represents interdisciplinary perspective. The last and the smallest stream is predominated by technical solutions in military knowledge management.

References

Bannister, F., & Byrne, B. (2013). Knowledge Management in Defence. In *PROCEEDINGS OF THE 14TH EUROPEAN CONFERENCE ON KNOWLEDGE MANAGEMENT (ECKM 2013), VOLS 1 AND 2* (pp. 106–116).

Boe, O. (2014). Changing Knowledge Management Strategy in the Norwegian Armed Forces: A Discussion of Effects-Based Thinking as an Alternative Method in the Planning and Execution of Military Joint Operations. In *2v. Proceedings of Knowledge Management International Conference, 12-15 august 2014, Langkawi* (pp. 814–818). Sintok: College of Art and Sciences, Universiti Utara Malaysia.

Galka, A., Jarema, P., Krasowski, K., Kosinski, A., Chmielewski, M., Nguyen, N. T., Kowalczyk, R. (2009). Semantic Knowledge Representation in Terrorist Threat Analysis for Crisis Management Systems. In N. T. Nguyen, R. Kowalczyk, & S.-M. Chen (Eds.), *Lecture notes in computer science, 0302-9743: Vol. 5796. Computational collective intelligence: Semantic web, social networks and multiagent systems. first international conference, ICCCI 2009, Warsaw, Poland, October 5-7, 2009. proceedings / Ngoc Thanh Nguyen, Ryszard Kowalczyk, Shyi-Ming Chen (eds.)* (1st ed., Vol. 5796, pp. 460–471). Berlin: Springer.

Mattila, J. (2016). Military Knowledge Management: Sense-Making, Decision Making and Knowledge Creation. In *PROCEEDINGS OF THE 17TH EUROPEAN CONFERENCE ON KNOWLEDGE MANAGEMENT* (pp. 1053–1062).

Perusich, K., & Mcneese, M. D. (2006). Using Fuzzy Cognitive Maps for Knowledge Management in a Conflict Environment. *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, 36(6), 810–821. <https://doi.org/10.1109/TSMCC.2005.855509>

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Postmodern Threats for National Security in Postmodern World

Audronė Petrauskaitė, Rolanda Kazlauskaitė Markelienė

The General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius

Introduction. The process of globalization, rapid development of technologies and transformations in the identity and worldview of an individual has drastically changed structure of the society, collective and individual identity as well as it brought about many problems and difficulties for governmental and educational institutions. Per contra, the process of globalization has raised the opposite process of society fragmentation based on the idea of individualization and localization. These processes have introduced some misunderstanding and confusion into the consciousness of both - individuals and society, at the same time affecting the decision making process of governmental institutions and military as well.

The *National security strategy* of the Republic of Lithuania (2017) identifies 15 dangers, threats and risks. Contemporary threats for national security are becoming more complex and have more hybrid character. As the rule they are targeting the consciousness of individuals and of the societies because of their moral weakness. The human factor is the main risk and main threat for the national security conditioned by moral decline of consumer society. It is the biggest challenge for national states and their governments because of complexity and diversity of postmodern world.

It has forced the democratic society to rethink traditional understanding of warfare and moral war standards expressed by the International Humanitarian Law. Traditional forms and methods of warfare were based on professional knowledge and professional moral standards which guaranteed a success in conventional war. The 2nd World War and war conflicts of the 20th century helped the democratic society to understand of “good” or “bad” warfare and “right” or “wrong” behavior of the militaries in the armed conflicts. Postmodern threats came out of the frames of conventional war and denied a traditional understanding of war. As the result, it has led the society and the military to some confusion: irregular warfare has erased the bounds between war and other military operations as well as principles of warfare and traditional understanding of security and defence.

It became evident that Postmodernism has changed personal identity and as the consequence the balance between personal identity of the individuals and the institutional identity of an organization: how to maintain individuality and construct a personal identity in the context of such a strong organizational identity as military one? Now it is not so evident what is right and what is wrong because contemporary

threats does not keep traditional rules and “traditional” moral standards of warfare. The question for the majority of people is whether we really need to keep the rules fighting against the terrorists, against the unmanned aerial vehicles and other postmodern threats.

Methodology. This scientific research is based on the structuralism and post-structuralism as philosophical theoretical background (Zygmunt Bauman, Michel Foucault), postmodern paradigm of the military (Charles C. Moscoso) and the concept of network society (Manuel Castels).

Conclusions. Mutable character of postmodern identity and the diversity of identities is at variance with traditional understanding of this phenomenon. The process of transformations and reconstruction of the identity in contemporary society has become the problem for individuals, society and every institution as well.

The construction of postmodern identity has encountered two mutually supportive and determinant phenomena - fragmentation and fixation of identity which became the main threat for national security and defence in postmodern world.

Key words: postmodernity, identity, postmodern society, postmodern Armed Forces, hybrid threats.

References

- Bauman Z. From Pilgrim to Tourist - or a Short History of Identity. / Questions of Cultural Identity. Ed. Stuart Hall and Paul du Gay. London: Sage Publications, 1996, p.18-37.
- Battistelli F., Peacekeeping And The Postmodern Soldier, *Armed forces & Society*, Vol. 23 no. 3, Spring 1997, p. 467-484.
- Castels M., *The Power of Identity*. UK. Blackwell Publishing, 2010.
- Eriksen, T. H. *Globalization. The Key Concepts*. London: Bloomsbury. 2007.
- Friedman, J. *Globalization, Transnationalization, and Migration : Ideologies and Realities of global Transformation.*/ Friedman, J., Randeria, S. (eds.) *Worlds on the Move. Globalization, Migration and Cultural Security: 63–90*. London: I. B. Tauris, 2004.
- Foucault M., *Discipline and Punish. The Birth of the Prison*. USA, Second Vintage Book Edition, 1996. Hall St. *The Question of Cultural Identity./ Modernity. An Introduction to Modern Societies./ Edited by Stuart Hall, David Held, Don Hubert, and Kenneth Thompson*. Oxford. The Open University press, 1996. p. 596-632.
- Hall St. *The Question of Cultural Identity./ Modernity. An Introduction to Modern Societies./ Edited by Stuart Hall, David Held, Don Hubert, and Kenneth Thompson*. Oxford. The Open University press, 1996. p. 596-632.
- Kellner Douglas. *Popular culture and constructing postmodern identities.*/ Scott Lasch and Jonathan Friedman (eds). *Modernity and Identity*. Oxford: Basil Blackwell, 1992.
- Manville B., Ober J. *Beyond Empowerment: Building a Company of Citizens.*/ *Harvard Business Review*, January 2003.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Composites Containing Ag Nanoparticles for X-ray Protection

Rita Plaipaitė-Nalivaiko^{a*}, Diana Adlienė^b, Igoris Prosyčėvas^{b,c},
Valery Luhn^d, Tomas Gadišauskas^e

^a*Kaunas University of Applied Engineering Sciences, Tvirtovės Ave. 35, LT – 50155, Kaunas, Lithuania;*

^b*Kaunas University of Technology, Studentų Str. 50, 51368 Kaunas, Lithuania;*

^c*Institute of Materials Science, Kaunas University of Technology, K. Barsausko Str. 59, LT-51423 Kaunas, Lithuania;*

^d*Belarusian State University of Technology, Sverdlova Str. 13a, 220050 Minsk, Belarus;*

^e*The General Jonas Žemaitis Military Academy of Lithuania, Silo Str. 5A, LT-10322 Vilnius, Lithuania*

Introduction. The colossal attention towards nanostructured materials containing nanoparticles (NPs) is increasing every day due to their unique size-related properties as compared to bulk materials [1]. Whatever they are made of, the properties, structure and composition of nanoparticles [2, 3] are highly important since NPs are employed in electronics, biotechnology, optics, catalysis and etc [3, 4]. Metal nanoparticles play a special part among all nanoparticles and are the most explored in nanotechnology. The fortunate application of nanoparticles depends upon both the synthesis and the surface modification of particles [1, 4]. Surface modification can improve the intrinsic features of nanoparticles and allow the fabrication of nanocomposites and other structures inexistent in nature [4, 5].

Exposure to high-energy radiation may be hazardous as well as accumulated radiation dose from either particle emission or high-energy electromagnetic waves such as X-ray or γ -ray [2, 3]. Modeling the effect of ionizing radiation on various materials is one of the important preparation stages aimed at development of new compositions for protective shields [3]. To attenuate the radiation from these kinds of exposure traditionally heavy metals, aluminum or aluminum-alloy are used. Nevertheless, protective coatings made of heavy metals or aluminum are not only bulky but also are capable to produce higher penetrating secondary radiation. Such radiation requires additional shielding, increasing the cost and the weight. Hence, at present time research works focused toward designing efficient, lightweight and flexible shielding materials for protection against radiation. Therefore, polymer-based composites are attractive for developing materials that can effectively attenuate radiation. In past years, the growing attention is paid to the employment of nano- and micropolymeric composites that able effectively absorb high-energy radiation [4]. These requirements are performed by the new optically transparent polymer nanocomposites, produced by the embedding the Ag nanoparticles into polymer matrix. Fabricated polymeric nanocomposites are used

for the formation of radiation protective coatings that in turn will cover the dielectric layer to secure optical transparency [4].

The main purpose of this investigation was to study optically transparent polymeric nanocomposites containing metal nanoparticles, to analyze X-ray attenuation properties in these composites and to investigate the stability of their optical properties after irradiation.

Method of investigation. Nanocomposites with Ag nanoparticles were produced by in-situ polymerization technique. Synthesis of Ag nanoparticles was carried out using photocatalytic reduction of silver atoms directly in a thin layer of deposited polymer. UV light source (Hibridas Exposure Unit MA4) used for this goal. Applied UV exposure time of 5 min. was enough for photoreduction of Ag ions and formation of silver nanoparticles. The successful incorporation of Ag nanoparticles has been approved and properties of the layers were examined performing UV-VIS and FTIR measurements. The morphology of the samples and bulk composition were examined in a scanning electron microscope (JSM-5610 LV) with attached energy dispersive X-ray analysis (EDX JED-2201; JEOL, Japan) and using optical microscope Optika B-600 MET. Properties of the nanocomposites were analyzed based on the following characteristics: the absorbed dose, mass attenuation coefficient.

Investigation results. Exploration of the optical properties of polymer composites has shown that Ag nanoparticles were successfully embedded in the PMMA matrix. The size of synthesized Ag nanoparticles was X-ray dose dependent. Though, not particles formation but polymer chain scission was the main process contributing to the deterioration of the nanocomposites optical properties. This suggestion was supported by the results of surface morphology examinations. X-ray radiation induced changes in nanocomposites are linked to the reconfiguration of their bonding structure. Chemical bonding structure of experimental films was investigated before and after their irradiation of infrared spectroscopy, which allows detection of functional groups and characterization of chemical bonds in a molecule. Mass attenuation coefficients were evaluated for the experimental samples. Estimated lead equivalent values differed not significantly as compared to the averaged lead equivalent.

Results. Performed research shows potential application of Ag NPs containing polymer composites in the implementation of surface functionalization strategy: analyzed and discussed X-ray induced modification processes in Ag/PMMA composite layers are easily transferable for the analysis of other nanocomposites containing metal nanoparticles. Also assessment of nanocomposites behavior upon dose rate irradiation might be of value in applications related to materials that are used in moderate radiation environment.

Acknowledgement. This research is partially funded by a grant (Reg. No. MIP-091/2012 „Optically transparent polymeric nanocomposite shields for radiation protection”) from the Research Council of Lithuania.

*Corresponding author: +37067454287
E-mail address: rita.plaipaitė@gmail.com

Keywords: Nanocomposites, nanotechnologies, defence applications, polymer-based nanocomposites.

References:

- [1] Telegin S.V., Draganyuk O.N., The heterogeneous anti-radiation shield for spacecraft: *Materials Science and Engineering* 122 (2016) 012033; doi:10.1088/1757-899X/122/1/012033;
- [2] Zeynali O, Masti D. and Gandomkar S., Shielding protection of electronic circuits against radiation effects of space high energy particles; *Advances in Applied Science Research*, 2012, 3 (1): 446-451;
- [3] Singho N.D., Che Lah N.A., Johan M.R., Ahmad R., FTIR Studies on Silver-Poly(Methylmethacrylate) Nanocomposites via *In-Situ* Polymerization Technique, *Int J Electrochem Sci* 7 (2012) 5596 – 5603;
- [4] Singho N.D., Che Lah N.A., Johan M.R., Ahmad R.; Enhancement of the Refractive Index of Silver Nanoparticles in Poly (Methyl Methacrylate), *International Journal of Research in Engineering and Technology (IJRET)* 1 (4) (2012) ISSN 2277 – 4378;
- [5] Coates J., Interpretation of infrared spectra, a practical approach, *Encyclopedia of analytical chemistry* 2005, pp. 10815-10837, doi:10.1002/9780470027318.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Influence of Social Media on National Security

Dalia Prakapienė^{a1}, Romas Prakapas^b, Gitana Dudzevičiūtė^c

^{ab}*The General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius,*

^b*Mykolas Romeris University, Ateities 20, LT-08303, Vilnius*

Introduction. The spread and penetration of social media into everyday life are perceived as self-evident and natural phenomena. Generation Z is often identified with mobile technology, which, according to Ozkan & Solmaz [12], they use to interact with each other, maintain social relationships, etc. On the other hand, Facebook, Twitter, Instagram, etc. have become the inseparable elements of everyday social contacts for the representatives of previous generations, too. As Conti and Passarella [3] point out, today's media world is in close contact with the real model of human social behaviour. Such a close interaction between real and virtual worlds that helps solve everyday problems is often seen as a given that makes not only personal but also public life (e.g., e-government [6], business world [7], tourism [11] easier. However, despite these advantages, social media users irresponsibly use personal information, revealing it not only to friends or family members but also to other social network users [14]. Such, at first glance, innocent personal information display creates preconditions for a potential violation of privacy. As Thompson, McGill & Wang [15] point out, personal computer users are among the most vulnerable because of information security threats, as individuals often lack knowledge of technology as well as consequences of its use and have no ability to identify threats. The problem of the research is to see how social media through personal use are related to national security. The object of the research is the impact of social media on national security. The purpose of the research is to reveal the impact of social media on national security.

Research method. The research was modelled on the methodological approaches of quantitative research. The cross-sectional design model [5] was used to carry it out as it is the most commonly used one for research in a particular group. The construct of the research instrument was designed on the basis of theoretical considerations of the analysis of social networks [13]. The choice of the research model was conditioned by the peculiarities of the analysed phenomenon - as Carolan [2] notes, in the case of social network analysis, it often involves both the method and the theory, thus combining the aforementioned theoretical considerations of social network analysis and combining them with social constructivism [1] and knowledge management [9]. A questionnaire survey method was chosen for the empirical research. Indicators of measurement of

1 * Corresponding author. Tel.: 370-5-210-3557.

E-mail address: Dalia.Prakapiene@lka.lt

the instrument used in the research were selected based on the meta-analysis data of scientific sources and the specific context of the legal environment characterizing the situation in Lithuania [10]: national security interests, contribution of conscious citizens to the development of the country's security and prosperity, information and cyber threats, etc. Young people (18-29 years old) born and / or raised in the digital age of Generation Z [4] and studying in different Lithuanian higher education institutions (Vilnius, Kaunas, Klaipėda) were interviewed for the research. The subjects were selected by simple random sampling ($n = 152$)². The research involved 32.24% men and 67.76% women, 51.97% of the participants were studying at universities and 48.03% at non-university higher education institutions at the time of the research. It was conducted in March and April, 2018. Descriptive and inferential statistical research methods were used to analyse the collected data using SPSS 22 software package.

Research results. Young people that use social media are analysed from the perspective of different disciplines, but in the context of this research, the research data was analysed from the perspective of knowledge management (what, why, why, where and when). Research data shows that young people (aged 18-29), who were born and / or raised in the digital age of Generation Z, enjoy a wide range of social media benefits - most often social networks are necessary for them to communicate with their friends (95.39%), to search for information (84.87%) and spend leisure time (81.58%), for studies (66.45%), to communicate with family members (66.45%) and share photos (50.66%), for work (or business) (44.08%) and discussions (35.53%), to share experience (25.00%) and videos (19.74%), to look for new friends (15.79%) and play games (10.53%). Research data shows that the prioritization of some goals is related to gender (e.g., communication with family members, $r = -0.246$, $p < 0.005$) or age (e.g., communication with friends, $r = 0.281$, $p < 0.001$). On average, young people use four social networks ($M = 3.6$), the most popular of which are Facebook (98.68%), Youtube (93.42%), Instagram (73.03%), Google+ (43.42%).

Almost all young people (95.39%) who participated in the research have indicated their real name and post their personal photos (90.79%) on social networks. Also, most social network users have provided their exact birth date (74.34%) and email address (53.95%). One third has indicated their interests, a place of residence as well as a social status; a quarter has published their personal telephone number. 4.61% of the participants indicated that they have provided the exact address of their place of residence. Almost all young people connect to their social networking accounts with smartphones (99.34%) or personal computers (65.13%). A significant proportion (14.47%), however, regardless of any security requirements, uses public facilities in their education or work institutions. It turned out that only 48.03% of all the participants while connecting to social networks pay attention to the security of public and unprotected networks. Half of them refrain from joining such networks and the rest rely on their connection passwords. 94.74% use a password to protect their personal profile, the rest state that it is not necessary when using a personal device that only he/she alone uses.

A much more problematic situation emerges when a stranger sends a friend request - 2.63% accept all requests and 38.82% do that sometimes. The magnitude

2 Limitations of the research - the generalization of findings due to a relatively small sample of research is not possible; the results of the research show only a trend.

of the problem is highlighted by the fact that only more than half of all participants have heard about some of national security threats and risk factors (67.11% have heard of information threats, 64.47% of corruption, 63.16% of cyber-terrorism, 59.21% of terrorism, 55.26% of social exclusion, poverty, etc.). The findings of the Mann-Whitney test show that women know about the identified national security threats and risk factors statistically better than males ($p < 0.05$); in terms of educational institutions, college students know about the threats statistically better than university students ($p < 0.03$). Of all the participants in the research who have heard something of possible threats to national security and risk factors only 74.34% associate the spread of information threats and 65.79% of cyber threats with the use of social networks. More than 60% do not see any possible links between all other national security threats and risk factors and the use of social networks. In this regard, there are no differences between male and female opinions. However, regarding educational institutions, the findings of the Mann-Whitney test show that college students statistically see potential links more often ($p < 0.01$).

Conclusions. Young people actively use social networks for various purposes (personal, learning, work, recreation). A statistical person, aged 18-29, has personal profiles on four social networks, yet most often does not adequately evaluate and link the use of social networks with possible national security threats and risk factors: relatively often accepts friend requests from little-known people, posts a lot and various personal information, does not deter from using public computers and unsecured networks. Less than two-thirds of young people have heard something of possible threats and risk factors; however, the impact of social media on national security is not considered significant. Thus, it seems that young people lack information about real threats presented by social networks to both personal data storage and national security.

Keywords: social media, national security, Generation Z

References

- [1] Allen, M. *The sage encyclopedia of communication research methods*. Thousand Oaks, CA: SAGE Publications Ltd, 2017.
- [2] Carolan, B. V. *Social network analysis and education: Theory, methods & applications*. Thousand Oaks, CA: SAGE Publications Ltd, 2014.
- [3] Conti, M., Passarella, A. Online Social Networks and Media. *Online Social Networks and Media* 2017; 1: iii–vi.
- [4] Dabija, D.-C., Babut, R., Dinu, V., Lugojan, M. I. Cross-Generational Analysis of Information Searching Based on Social Media in Romania. *Transformation in Business & Economics* 2017; 16(2): 248–270.
- [5] Edmonds, W. A., Kennedy, T. D. *An Applied Guide to Research Designs: Quantitative, Qualitative, and Mixed Methods*. London: SAGE Publications, Inc, 2017.
- [6] Gao, X., Lee, J. E-government services and social media adoption: Experience of small local governments in Nebraska state. *Government Information Quarterly* 2017; 34(4): 627–634.
- [7] Grizane, T., Jurgelane, I. Social Media Impact on Business Evaluation. *Procedia Computer Science* 2017; 104: 190–196.
- [8] Yasin, A., Liu, L., Li, T., Wang, J., Zowghi, D. Design and preliminary evaluation

of a cyber Security Requirements Education Game (SREG). *Information and Software Technology* 2018; 95: 179–200.

[9] Mittelmann, A. Personal Knowledge Management as Basis for Successful Organizational Knowledge Management in the Digital Age. *Procedia Computer Science* 2016; 99: 117–124.

[10] Nacionalinio saugumo strategija. *TAR* 2017; 1424.

[11] Narangajavana, Y., Callarisa Fiol, L. J., Moliner Tena, M. Á., Rodríguez Artola, R. M., Sánchez García, J. The influence of social media in creating expectations. An empirical study for a tourist destination. *Annals of Tourism Research* 2017; 65: 60–70.

[12] Ozkan, M., Solmaz, B. Mobile Addiction of Generation Z and its Effects on their Social Lives: (An Application among University Students in the 18-23 Age Group). *Procedia - Social and Behavioral Sciences* 2015; 205: 92–98.

[13] Prell, C. *Social network analysis: history, theory & methodology*. London: Sage Publications, 2012.

[14] Rathore, S., Sharma, P. K., Loia, V., Jeong, Y.-S., Park, J. H. Social network security: Issues, challenges, threats, and solutions. *Information Sciences* 2017; 421: 43–69.

[15] Thompson, N., McGill, T. J., Wang, X. “Security begins at home”: Determinants of home computer and mobile device security behavior. *Computers & Security* 2017; 70: 376–391.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Grenade UAV for Reconnaissance and Rapid Combat Assistance (GURRCA) Project

Sathvik Sathyanarayana Rao¹

Kaunas University of Technology, Faculty of Mechanical Engineering and Design, K. Donelaičio g. 73, LT-44249, Lithuania, India

Introduction. The UAVs in the recent history have established their significance in multi domain fields and has gained priority higher than ever. One of the most important application of the UAVs focuses on Military requirements and capabilities. At present, the use of UAV for military operations has accelerated development. However, in most cases, long endurance (Global Hawk, Predator, etc., Class III according NATO classification) or tactical (RQ-7 Shadow, RQ-11 Raven, vertical landing, etc., Class II) UAV are used. However, such UAVs are not always suitable for use in real conditions. As operations in Afghanistan, Iraq, and others have shown, very often it is necessary to have UAVs capable of carrying out operations much closer to the ground, easy to carry, operate under complex conditions (in the battlefield, in the event of a fire, etc.), rapid launch without any preparation, capable to perform the same functions as larger UAV, and the servicemen do not need special skills [1-3]. The existing quickly launchable military mini UAVs require the certain preparation of personal, a special container for transportation and does not operate under any weather or environmental conditions. One of the solutions could be UAV launched by grenade launcher. The first attempts to use the grenade launchers or other firearms for the UAV launcher have already been completed [4, 5]. The Project “GURRCA” meets almost all the requirements of a military mini UAV in weight, size, rapidly launchable, semi-autonomous. In addition, it is not need the separate container for the delivery, the personal do no need special skills for the control and management, it is useable for reconnaissance and other combat assistance. Although there are similar technological developments, The GURRCA will feature a long duration descent system with a real time data transmission for the combat personal on ground assisted with a light weight On Screen Display (OSD) mounted to the primary launch system. This gives the GURRCA an added advantage in the current military needs, especially for counter terrorism operations which is of greater concern. With all the above configurations, The GURRCA is one of its kind and holds great significance in the modern Combat technological developments and peace for mankind. This system would be useful also in nonmilitary operations carried out by the police or firefighters

¹ * Corresponding author. Tel: +37063050081
E-mail address: sathvik30@gmail.com

Method of investigation. The project is faced with two challenges:

- the availability of appropriate electronic equipment to resistant to vibrations and to high levels of acceleration (High-G);
- UAV landing method.

The first challenge is solving by choosing the appropriate elements and their composition (fig. 1).

The second challenge is solved by comparing the theoretical estimates of various landing methods (landing times). For this purpose, well-known formulas and methods suggested in the works [6, 7] were used.

Investigation Results. GURRCA is a Grenade type UAV which would be a 40mm grenade and can be launched from a light gun (as an automatic rifle), with add on grenade launcher. The principle of launch would be same as the regular 40mm grenades but unlike the ones filled with explosive substance, this 40mm grenade would feature small electronic components including replaceable propulsion and slow descent system, AV camera, gyroscope, and replaceable components based on the combat requirements such as gathering intelligence.

At present, such work has been carried out:

- Proposed concept and initial requirements for such UAV;
- Carry out evaluation of different landing methods and according it's the landing method chosen;
- An elements composition scheme and a system operation algorithm are proposed.

According to theoretical comparison of different landing methods, a landing method with the propeller was chosen.

The UAV composition and operational algorithms are shown in Fig. 1 and Fig 2.:

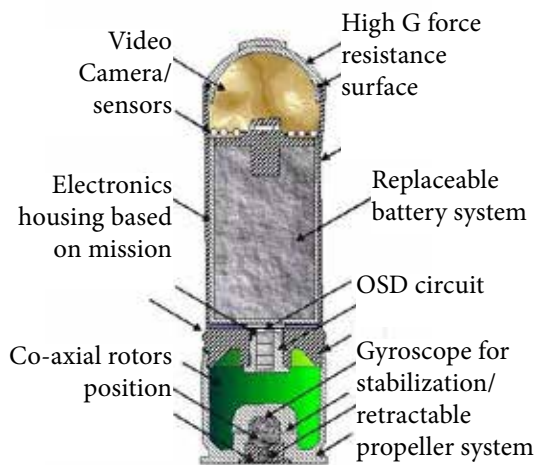


Fig. 1. Basic Grenade UAV abstract composition

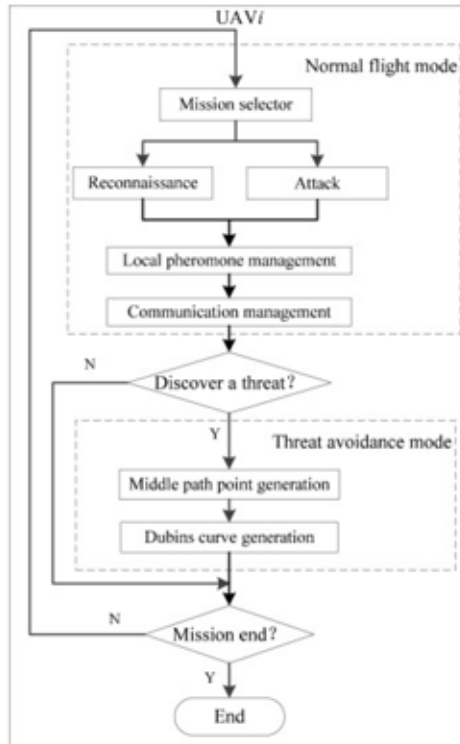


Fig. 2. Basic UAV operational flowchart

Figure 1: The figure represents a simple composition of the planned Grenade UAV which will consist of electronic components and the co-axial rotor descent system

Figure 2: The figure 2 represents a typical UAV mission design and for the GURRCA project, the flowchart would be similar but will be based only for the reconnaissance system in the preliminary stages

Conclusions. At this stage of the project, such results are obtained:

- Various types of landing system are being analyzed such as Parachute descent, winged system, coaxial rotor system, single rotor descent system and Streamer descent system. It was noted that Coaxial rotor descent has long duration descent advantages.
- Suggested UAV composition allows to change the power supply and to have the opportunity to install additionally other micro sensors;
- Proposed algorithm that describes the operation of a UAV.
- Soon, we will continue to develop this project, focusing on the information transfer system.

Keywords: unmanned air vehicles; grenade launcher; explosive detection; quick launch; slow descent; replaceable;

References

- [1] Coffey T, Montgomery J A. The Emergence of Mini UAVs for Military Applications. *Defense Horizons* 2002; 22; 1–8.
- [2] Miller P M. Mini, micro, and swarming unmanned aerial vehicles: a baseline study. *Federal Research Division, Library of Congress*. 2006; 58 p.
- [3] Atcioglu B. Micro unmanned air vehicles formation process and models. *International Journal of Mechanical and Production Engineering*. 2016; 4 (6); 91–95.
- [4] Zhang M. Hackers create a DIY flare gun camera. Available at: <https://petapixel.com/2011/08/09/hackers-create-a-diy-flare-gun-camera/>. 2011.
- [5] 155mm Ballistic Sensor Fuzed Munition. *Think Defense*, Available at: <https://www.thinkdefence.co.uk/2014/07/105mm-155mm-something/155mm-ballistic-sensor-fuzed-munition/>. 2018.
- [6] Eriksson M, Ringman P. Launch and recovery systems for unmanned vehicles onboard ships. A study and initial concepts. *KTH university Central of Naval Architecture*. 2013; 96 p.
- [7] Wagner N, Boland S, Taylor B, Keen D, Nelson J, Bragley T. Powertrain design for hand-launchable long endurance unmanned aerial vehicle. *America, institute of aeronautical and astronautics*. 2010; 1-16.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Peculiarities of ICT in Securing Energy Sector in Lebanon

Youssef El Tabsh^aVida Davidavičienė^{b1}, Jolanta Sabaitytė^c

^a Vilnius Gediminas Technical University, Department of Business technologies and Entrepreneurship, Sauletekio al.11, LT-10222, Lithuania,

^b Vilnius Gediminas Technical University, Department of Business technologies and Entrepreneurship, Sauletekio al.11, LT-10222, Lithuania,

^cThe General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius

Introduction. The information and communication technologies (ICT) cause technological improvement of products, services and processes. ICT providing solutions for the business, society and for the countries development. The ICT importance in the energy management sector was emphasized by [1]. ICT for energy management systems and resource incorporation should be taken into consideration in order to increase the productivity and to sustain the resources used on daily bases. ICT surely will have an essential yet positive effect on energy production, direct and in indirect ways [2,3,4].

The various challenges are facing in the different countries, such as: aim to reduce the energy consumption, the aim to lower costs and carbon emission, the aim to replace the current fuel producing power plants to alternative fuel and sustainable energy resources; the aim to implement new technologies. Since most of the developing countries including Lebanon are facing problems with the energy sector, the problem raised in this article is to analyse information and communication technologies integration in the energy sector for ensuring the security and sustainability. The developmental approach must include all major technology breakthroughs in power sources, grids, energy storage, and ICT [5]. The results of the technological developments should focus on the productivity of the power sources, manage the distribution process and finally keep the system error and problem free. Social responsibility in addition to the political obligations appear to be the primary motivation for the futuristic developmental approach [6]. Then the governments should work to put all of the political problems aside and work together in order to achieve a policy that will lead to the implementation of the development of the energy sector. The social actors should also collaborate and put their efforts with the governments not only for supporting the process rather than to find applicable solutions and provide studies to choose the best option that might the governments choose for implementation.

1 * Corresponding author. Tel.: 370-699-699-71.

E-mail address: vida.davidaviciene@vgtu.lt

The purpose of this article is to analyze possibilities to use ICT for securing Energy sector at Lebanon.

Method of investigation. For reaching such methods as literature analysis, synthesis, survey and descriptive data analysis was employed. A survey was conducted by the authors in Lebanon (Beirut), during the fall of 2017. The aim of the research was to identify the Lebanese citizen's awareness about renewable energy available and what causes slow implementation of new technologies in the energy sector. Sample size of 386 calculated taking 61.3 percent (age 15-65) of inhabitants from all 6 million populations with confidence level 95 percent, confidence interval 5. In total 200 completed questionnaires were collected in Beirut.

Investigation Results. The solutions for the energy supply deficiencies vary, every solution can depend on the country geographical location and its' nature. The key areas of innovation in the sustainable energy production include wind, solar, ocean power, distributed generation, and other renewable energy technologies [5]. The investments in the sustainable energy solutions can have a major impact on the development of the countries that are lacking the energy power supply, or still using the oil to produce energy [7,8,9]. Modern countries and cities are developed and managed basically taking into consideration the significance for sustainable development, several inventiveness have emphasized how ICT can be used to achieve cities' powering targets by using effectively and efficiently the scarce sources of energy [10]. The sustainability in developing countries opens a statement about the possibility to improve the lives of the people living in these countries. Not to forget the financial, educational and psychological problems that are main factors facing these implementations. Information and communication technologies are the way of which we should use to successfully complete any sustainable development project, the main reason for that is communication is determining the world widely and rapidly. Once a specific information and communication technology (ICT) innovation has been decided on, it is usually in everyone's interest to make it work as efficient as possible, and a crucial part of the knowledge concerning how to do so is usually dispersed among people working with the ICT innovation in their daily routine.

Lebanon, since the war against Israel in the summer of 2006, is facing a catastrophic situation in the electricity provided by the Ministry of Electricity, because during the war, the major electrical power generator plants were destroyed. Lebanese government nor the municipalities are unable to fulfill their duties in implementing the renewable energy systems due to legal constraints and financial dependency. The two major financial resources for municipalities - the Independent Municipal Fund (IMF) and the local taxation - are not sufficient to promote community development and sustainability initiatives [11]. Forty years ago, Lebanon used to produce enough power to be able to export a part of it to Syria, the largest neighbor. Currently, Lebanon is barely able to cater for its national energy demands, there is hardly enough electricity to keep street lamps on at night. The governmental paralysis and the corruption affecting the developmental strategies in Lebanon has started since the civil war and it is continuing till present times.

In a country where the gross national income per capita is \$9,800, according to the latest World Bank estimates, the Lebanese families spent on average of \$1,300 on electricity, around \$900 on generators owned by locals in the neighborhoods during the year of 2016.

The first factor was the Lebanese participants were unaware of the renewable energy supplies available in the market and the second factor was that the participants have hesitancy in having these new devices for many reasons.

Research revealed that the majority of the respondents 52% are little aware of the solar energy technologies, this because the solar energy technologies entered the Lebanese market very recent, people in general are curious about anything new but they are afraid of trying this technology, the government is not helping the suppliers in doing enough marketing campaigns to attract customers, so ICT solutions for informational purposes could be helpful. 43% are very aware because we are living in a technological era where everything is available online, so these people tend to read and search about it to have more knowledge.

The second question was about the factors that preventing the customers to have the solar energy power systems at their places. The affordability came first, then the lack of awareness. The majority of the participants 43% can't have solar energy technology at their homes because they can't afford it, the prices of this technology is very high in Lebanon and the government is not helping that much in supporting the citizens to have solar energy at their homes. People are interested in the solar energy technology, 96% gave the acceptance for the solar energy technology if it was cheaper, more convenient, the suppliers and the government make intensive awareness campaigns about it and finally try to build the trust between the participants and the suppliers about the solar energy technology and how useful to install it at their homes.

From the above results we see that the Lebanese are willing to have a new innovative technology, that's because the majority of the Lebanese society is composed of youth and educated people who are willing to invest money in an energy management system that will save their environment and their money on the long term and secure the households from electrical energy shortages. In order to evaluate the full consequence of implemented ICT solutions in the energy management systems, it is significant to take into consideration all the direct and the indirect transformations caused by this implementation, including the effect from the ICT solutions through the entire lifecycle. This can lead to the result of the importance of merging the ICT's to the energy management system implementation with policy and planning procedures, to make sure that the efficiency and effectiveness gains actually lead to a reduced use of energy have also been proved.

There are many used prototypes to solve the energy management sector problems in the world, due to the bad economy factors, corruption and regional position, the Indian example can be implemented in Lebanon with some minor adjustments. In India the energy sector was facing a lot of problems, due to several factors that played a negative role in the innovation and in the development of the sector. Thus, Lebanon is facing a lot of these problems yet there is a good hope in doing developmental strategies to the energy management sector in Lebanon by using the Indian prototype. Recent studies showed that India is in the 13th position in using the renewable energy systems [12, 13,14] (Monforti et al. 2014; Hazarika et al. 2017; Zhang, Xuan 2017).

Conclusions. The ICT's generally depend on innovation, and with the era of wireless communication and information sharing, the innovation management will play a major role in keeping the ICT's on the right and correct track when it comes to monitor and control the energy management systems. When connecting the innovation to the information and communication technologies, a lot of positive results will be linked

to the success of the energy management sector, the positive aspects will be counted, such as, creation of innovative solutions for solving the electricity problems for the developing countries, connecting similar projects together to serve the need of the communities for electricity and finally empowering the citizens and the municipalities in adapting and creating new energy management projects and try to implement them on the national level with the help of the government and the help of the ministry of water and power supply.

Nowadays, less than 10 percent of all of the energy used worldwide comes from renewable energy resources, so governments should have the ability to encourage the citizens to use these solution, provide support and educate the citizens about the positive aspects of using these solutions and involve ICT solutions for this purpose.

Keywords: renewable energy, energy security, Information and communication technologies, ICT, Lebanese case.

References

- [1] Jáñez Morán, A.; Profaizer, P.; Herrando Zapater, M.; Andérez Valdavida, M.; Zabalza Bribián, I. Information and Communications Technologies (ICTs) for energy efficiency in buildings: Review and analysis of results from EU pilot projects, *Energy and Buildings* 2016; 127: 128–137. <https://doi.org/10.1016/j.enbuild.2016.05.064>
- [2] Ollo-López, A.; Aramendía-Muneta, M. E. ICT impact on competitiveness, innovation and environment, *Telematics and Informatics* 2012; 29(2): 204–210. <https://doi.org/10.1016/j.tele.2011.08.002>
- [3] Røpke, I.; Christensen, T. H. Energy impacts of ICT - Insights from an everyday life perspective, *Telematics and Informatics* 2012; 29(4): 348–361. <https://doi.org/10.1016/j.tele.2012.02.001>
- [4] Bekaroo, G.; Bokhoree, C.; Pattinson, C. Impacts of ICT on the natural ecosystem: A grassroot analysis for promoting socio-environmental sustainability, *Renewable and Sustainable Energy Reviews* 2016; 57: 1580–1595. <https://doi.org/10.1016/j.rser.2015.12.147>
- [5] Liu, Z.; Liu, Z. Chapter 6 – Innovation in Global Energy Interconnection Technologies. *Global Energy Interconnection* 2015; Source in the internet: <https://doi.org/10.1016/B978-0-12-804405-6.00006-3>
- [6] Ngar-yin Mah, D.; Wu, Y. Y.; Ronald Hills, P. Explaining the role of incumbent utilities in sustainable energy transitions: A case study of the smart grid development in China, *Energy Policy* 2017; 109(June): 794–806. <https://doi.org/10.1016/j.enpol.2017.06.059>
- [7] Buracas, A. ICT Impact on Competencies and Innovations: Regional Applicability of Global Indicators, *TEM Journal* 2016; 5(4): 550–559. <https://doi.org/10.18421/TEM54-20>
- [8] Mosannenzadeh, F; Bisello, A.; Vaccaro, R.; D'Alonzo, V.; Hunter, G. W.; Vettorato, D. Smart energy city development: A story told by urban planners, *Cities* 2017; 64: 54–65. <https://doi.org/10.1016/j.cities.2017.02.001>
- [9] Silvast, A. Energy, economics, and performativity: Reviewing theoretical advances in social studies of markets and energy, *Energy Research and Social Science* 2017; 34(October 2016): 4–12. <https://doi.org/10.1016/j.erss.2017.05.005>
- [10] Tabsh, Y.; Davidavičienė, V. Information and Communication Technologies in Energy Management, *Journal of System and Management Sciences* 2016; 6(4): 67–81.

[11] Khoury, R. Recommended National Sustainable Urban and Energy Savings Actions. Lebanon 2012.

[12] Monforti, F.; Huld, T.; Bódis, K.; Vitali, L.; Isidoro, M. D.; Lacal-arántegui, R. Assessing complementarity of wind and solar resources for energy production in Italy. A Monte Carlo approach, *Renewable Energy* 2014; 63: 576–586. <https://doi.org/10.1016/j.renene.2013.10.028>

[13] Hazarika, D.; Gogoi, N.; Jose, S.; Das, R.; Basu, G. Exploration of future prospects of Indian pineapple leaf, an agro waste for textile application, *Journal of Cleaner Production* 2017; 141: 580–586. <https://doi.org/10.1016/j.jclepro.2016.09.092>

[14] Zhang, J.; Xuan, Y. Performance improvement of a photovoltaic - Thermoelectric hybrid system subjecting to fluctuant solar radiation, *Renewable Energy* 2017; 113: 1551–1558. <https://doi.org/10.1016/j.renene.2017.07.003>

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

The Influence of Substitutions on the Explosive Properties. N-(2,4,6-trinitrophenyl)- 1H-1,2,4-triazol-3'-amine

Jelena Tamuliene^{a1}, Jonas Sarlauskas^b, Svajone Bekesiene^c

^aVilnius University, Institute of Theoretical Physics and Astronomy, Sauletekio al. 3, LT-10222, Lithuania,

^bVilnius University, Institute of Biochemistry, Sauletekio al. 7, LT-10222 Vilnius, Lithuania

^cThe General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius

Introduction. Currently, the research has been carried out into the synthesis of new explosive materials aiming to couple high density with high energy. The detonation pressure approaching kilo bars (kbar), a specific impulse and/or enhanced stability, and insensitivity to such stimuli as impact, friction, and electrostatic discharge should also be considered [1]. Additionally, energetic materials could not be quite sensitive and hydrolytically unstable. Hence, the research is in progress worldwide searching for explosives with the combination of properties such as safety, reliability, stability, cost-efficiency and eco-friendliness. For the synthesis of thermally stable explosives, nitro compounds have received special attention because of their ability to withstand high temperatures and the low pressures encountered in space environments [2].

We intend to present the results of our study on an investigation of the influence of nitro group and $-\text{CH}_3$, $-\text{N}_3$ and $-\text{Cl}$ substituents on the thermal and chemical stability as well as the explosive performance of N-(3,5-dimethyl-2,4,6-trinitrophenyl)-1H-1,2,4-triazol-3-amine (HEM-I). This study is performed to exhibit that the stability, explosive properties and resistance to accidental stimuli (thermal, impact, friction) of the explosive materials could be increased when the substitutions and their place in the molecule are properly selected.

Method of investigation. The structure of the molecule and its fragments has been studied by the Becke's three-parameter hybrid functional applying the non-local correlation provided by Lee, Yang, and Parr (B3LYP) [6], – a representative standard DFT method.

The analysis of the thermal stability based on the comparison of the binding energy per atom was performed. The highest occupied molecular orbital (HOMO) and lowest unoccupied molecular orbital (LUMO) gap chemical hardness and softness were investigated to determine chemical stability. Detonation velocity and oxygen balance

1 * Corresponding author. Tel.: 370-6-89-12-133.

E-mail address: Jelena.Tamu.liene@tfai.vu.lt

© 2018 The Authors.

Peer-review under responsibility of the General Jonas Žemaitis Military Academy of Lithuania, Engineering Managing Department

were investigated to compare explosive properties.

Investigation Results. The results of our investigation show that the additional nitro groups increase resistance of the new explosive material to react with other materials and the explosive properties (strength detonation pressure and velocity), but decrease possibility to degradation, toxicity and thermal stability. We also found that only $-NH_2$ substitution position in the core molecule is appropriate to achieve our aim both to increase the stability and improve explosive performances of HEM-I. The experimental measurement proves high thermal stability and resistance to stimuli of HEM-I. The theoretical and experimental investigations of the IR and UV spectra and structural and optical properties of HEM-I with various groups were investigated taking into consideration solvent influence. The results obtained indicated some difficulties to recognize the new materials by spectroscopic analysis. Thus, we suggested and checked theoretically and experimentally the colour test of HEM-I recognition.

Conclusions. The results of our investigations show us that the new material could be used as new unknown explosives. The new explosive materials could be recognized by colour test suggested by us.

Acknowledgements. This work was conducted within the framework of the LMA scientific project “A theoretical and experimental investigations of new potentially explosive materials using quantum mechanical methods (NSPROG-I4)”. The authors are thankful for the high performance computing resources provided by the Information Technology Open Access Center of Vilnius University

Keywords: explosive materials; explosive-based terrorism; explosive detection; calculations; DFT method.

References

- [1] Wilson W. S. NAWCWPNS Technical Publication 8188, Published by Technical Information Department, 1994.
- [2] Agrawal J. P. Central European Journal of Energetic Materials, 2012, 9, p. 273-290.
- [3] Senesac L, Thunda T G. Nanosensors for trace explosive detection. *Materials Today* 2008; 11: 28–36.
- [4] Hwang J, Namhyun Choi N, Aaron Park A, Park J-Q, Chung J.H, Baek S, Cho S G, Baek S-J, Choo J. Fast and sensitive recognition of various explosive compounds using Raman spectroscopy and principal component analysis. *Journal of Molecular Structure* 2013;1039: 130–6.
- [4] Moore D. Instrumentation for trace detection of high explosives. *Rev. Sci. Instrum.* 2004; 75: 2499–2512.
- [5] Izake E L. Forensic and homeland security applications of modern portable Raman spectroscopy. *Forensic Sci. Int.* 2010; 202: 1–8.
- [6] Tamuliene J, Sarlauskas J, Bekesiene S, Kleiza V. ITELMS'2014: Proceedings of the 9th international conference, May 23-24, 2014, Panevėžys, Lithuania. Kaunas: Technologija, 2014.
- [7] Steinfeld J I, Wormhoudt J, Explosives detection: A Challenge for Physical Chemistry. *Annu. Rev. Phys. Chem.* 1998; 49:203–32

- [8] Becke A.D. Density-functional thermochemistry. iii. The role of exact exchange. *J. Chem. Phys.* 1993; 98:5648-52.
- [9] Zhao Y, Pu J, Lynch B J, Truhlarand D G. Tests of Second-Generation and Third-Generation Density Functionals for Thermochemical Kinetics. *Phys. Chem. Chem. Phys.* 2004; 6:673–676.
- [10] Kendall R A, Dunning Jr. T H, Harrison R J. Electron affinities of the first-row atoms revisited. Systematic basis sets and wave functions. *J. Chem. Phys.* 1992; 96:6796–6806.
- [11] Scalmani G, Frisch M J, Mennucci B, Tomasi J, Cammi R, Barone V. Geometries and properties of excited states in the gas phase and in solution: Theory and application of a time-dependent density functional theory polarizable continuum model. *J. Chem. Phys.* 2006;124:094107: 1-15.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Societal Security in Poland

Maciej Tołwiński^{a1}

*^aSiedlce University of Natural Sciences and Humanities, Faculty of Humanities,
Institute of Social Sciences and Security, 39 Żytnia st.,
08-110 Siedlce, Poland*

The main aim of the paper is description and explanation of societal security in Poland, especially scientific theory of societal security. Theoretical approach to societal security is not homogenous. Until the early 90s, societal security has not been considered in Poland as a part of national security disciplines. Owing to the fact that emerging societal unrest in the state are primarily public administration bodies responsibility, societal security may be studied in the field of internal security and therefore it can be associated with the tasks of public authorities, their competences and scope of activities within the state.

Nowadays societal security is represented in Polish national security system. It can be proved by records in Polish White Paper of National Security (pol. *Biała Księga Bezpieczeństwa Narodowego*), where societal needs are presented. What is more, state guarantees societal services for citizens. It is inextricably connected with state guardianship function. Societal security system is societal subsystem, supporting national security system.

Societal security can be divided into two dimensions: social security and psychosocial security. Social security refers to every form of state's activities, orientated onto providing stabile economical situation citizens, ensuring equality and sustainability. Psychosocial security is more subjective, referring to own self-welfare and own security aims perception. The paper will discuss both dimensions of societal security in Poland, presenting available research data related to the subject.

Keywords: national security system in Poland, psychosocial security, societal security.

References

- [1] M. Brzeziński, Bezpieczeństwo społeczne z perspektywy bezpieczeństwa wewnętrznego, „Zeszyty Naukowe WSO WL” Nr 3 (169) 2013
- [2] J. Czaputowicz, Bezpieczeństwo międzynarodowe. Współczesne koncepcje, Warszawa 2012

1 * Corresponding author. Tel.: +48 517788378.
E-mail address: maciej.tolwinski@uph.edu.pl

[3] A. Kołodziejczyk, Bezpieczeństwo jako fenomen społeczny : pojęcie bezpieczeństwa, jego interpretacje i odmiany, „Saeculum Christianum : pismo historyczno-społeczne”, 2017 14/1.

[4] S. Koziej, Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja, „Bezpieczeństwo narodowe”, 2011/18.

[5] M. Leszczyński, V. Mika, Bezpieczeństwo społeczne w nowym pojmowaniu bezpieczeństwa państwa, „Acta Scientifica Academiae Ostroviensis”, 33/2010

[6] M. Leszczyński, Wybrane obszary zagrożeń dla rozwoju społecznoekonomicznego i bezpieczeństwa społecznego, „Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne”, 2012 tom 1.

[7] A. Skrabacz, Bezpieczeństwo społeczne – podstawy teoretyczne i praktyczne, Warszawa, 2012.

[8] K. Szewior, Bezpieczeństwo społeczne jednostki. Założenia i polska rzeczywistość, Warszawa 2016.

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Information Security in Poland

Stanisław Topolewski^{a1}

^aSiedlce University of Natural Sciences and Humanities, Faculty of Humanities, Institute of Social Sciences and Security, 39 Żytnia st., 08-110 Siedlce, Poland

Permanent increase of the role and significance of information is characteristic to modern civilization; it's one of its features. Information resources are the most valuable tools on the capital and investment markets, but also are a great political weapon. Therefore, they are exposed to various types of threats. Threats to information security can be divided into threats resulting from: intentional, accidental, random and other actions, e.g. appointing persons without appropriate knowledge to responsible positions, poor knowledge of applicable laws or inconsistencies of law. Therefore, to maintain the stability of the state and give a sense of security to citizens, the most important task and duty of the government and its specialized services in this area is to protect them. It can be provided by a properly organized and efficiently functioning system that will guarantee restrictions on the access of people, especially to sensitive information, and their proper processing. For this reason, the system requires state-specific precisely defined rules and norms to be legally enforceable.

The article describes nature of information security in Poland. By critical source analysis it introduces framework of Polish legal acts that guarantee information security. Polish legal system guarantees information security in various ways. One of them is Classified information protection Act (05/08/2010, Dz.U. 2010 nr 182 poz. 1228). The article relates to four secrecy clauses and their impact on national security and protection of information. Requirements of information physical protection are discussion taking into account organization and requirements for infrastructure construction and accessibility. Security clearance is another element discussed in the article in relation to information security in Poland. Verification proceedings are also described and their impact on information security is discussed. In conclusion, Polish information protection system has various methods and instruments implemented for increasing information security. What is more, it still evolves, to rise to new challenges of contemporary world.

Keywords: information protection, information security, Polish information protection system

1 * Corresponding author. Tel.: +48 697140629.
E-mail address: stanislaw_topolewski@wp.pl

References

- [1] E. D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa, 2002
- [2] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013
- [3] K. Liderman. *Bezpieczeństwo informacyjne*, Warszawa 2012
- [4] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2010 nr 182 poz. 1228
- [5] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997 nr 133 poz. 883
- [6] S. Topolewski, *Ochrona informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Siedlce 2017

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

The Value of Staff Loyalty at Security and Defence Institutions: A Case Study of the Public Security Service Vilnius Unit

Vladas Tumulavičius^a, Karolis Kriaučionis^b

^{a,b} *The General Jonas Žemaitis Military Academy of Lithuania, Silo g. 5A, LT-10322 Vilnius*

Introduction. The article presents and analyses the current issues and latest trends of the definition of loyalty of public servants and the problem of employers loyalty at Public Security Service of Lithuania. Authors reveals the indicators which influence and encourage the loyalty or organizational commitment while working in certain organization. It's emphasized that the loyal employer is useful in any kind of organization, as it can easily increase the productivity at several work [1]. Meanwhile, organizational commitment is important to keep the membership of employers at certain organization and charge them by more relevant targets [2]. Job satisfaction appears as technical kind of value which provides the possibility to evaluate how the typical workplace matches with the targets which employers is charged to accomplish [3,4].

The authors found that loyalty, organizational commitment and job satisfaction are the indicators which are closely related and can be analyzed all at once at the same perspectives. When working conditions are being improved, the jobs satisfactions grows automatically also, organizational commitment increases as well, which provides the possibility to increase the career or be charged by more specific tasks. Committed employee is mentally and physically liable to increase the work productivity at the organization which influences loyalty [4].

Consequently, due to the complicated circumstances organization stands assured the loyal employees keep the membership at the organization until the hard times are over and the balance restored. The aim of work – analyse the employees' loyalty at organizations, its impact and factors which influence loyalty. Investigate the problems and conditions of occurrence due to the process of research, the main targets have been formulated: 1) to examine the concept of loyalty and its impact; 2) identify and highlight key factors of importance of loyalty; 3) evaluate employee satisfaction with certain organization; 4) analyse the importance of employees' organizational commitment.

* Corresponding author.

E-mail address: Vladas.Tumulavicius@lka.lt

Method of research. The authors applied general scientific methods of studying objective reality, peculiar to social sciences: systematic document analysis, meta-analysis, structural-functional analysis, teleological, comparative, critical approach, generalisation and prediction. To complete the results and formulate conclusions of research questionnaire method has been used.

Results of research. As the result both male and female, are very similar and completely independent from the level of job satisfaction at Public Security service. However, when comparing the age-group commitment of officials, it becomes clear that the senior officials of the group continue to have a higher commitment than, for example, officers aged 18 to 25 years. Also, having a long record of work, the employees' commitment to the organization arises.

Conclusions. As a result in this research is emphasised that the higher the satisfaction of the officers with the work (both internal factors and external factors), the higher the normative commitment to work; the main guidelines of modernisation in this field are presented.

References

[1] Antoncic, J. A.; Antoncic, B. (2011) Employee loyalty and its impact on firm growth. *International Journal of Management and Information Systems*, vol. 15(1), p. 81-87. DOI: <https://doi.org/10.19030/ijmis.v15i1.1598>

[2] Elegido, J. M. (2013) Does it make sense to be a loyal employee? *Journal of Business Ethics*, vol. 116(3), p. 495–511. DOI: 10.1007/s10551-012-1482-4

[3] Raišienė, A. G.; Vanagas, R.; Žuromskaitė, B.; Stasiukynas, A.; Dromantaitė, A.; Girčys, A. P.; Tamošiūnaitė, R.; Bileišis M. (2014) Veiksmingos vadybos gairės: teorinės išvalgos ir Lietuvos organizacijų atvejai. Vilnius: MRU, p. 430. eISBN 9789955196198

[4] Rajput, S., Singhal, M., Tiwari, S. (2016) Job Satisfaction and Employee Loyalty: A study of Academicians, p. 1–2. Available in Internet: https://www.researchgate.net/publication/305516797_Job_Satisfaction_and_Employee_Loyalty_A_study_of_Academicians

International Conference and Live Firing Show-2018 (LFS'2018)



The 1th International Conference Challenges to Nacional Defence in Contemporary Geopolitical Situation (CNDCGS'2018), 25-27 April 2018, Pabrade, Lithuania

Implications of the Fragmentation of Lithuanian Uniformed Services

Svajūnė Ungurytė-Ragauskienė^a, Mantas Bileišis^b

^a*Mykolas Romeris University, Public Management Innovation Laboratory, Didlaukio 55, room 201, LT-08303 Vilnius, Lithuania,*

^b*General Jonas Žemaitis Military Academy of Lithuania, Šilo g. 5A, LT-10322 Vilnius, Lithuania*

Introduction. The scope of impact of EU integration on national governance structures is minimal. Member states need only to comply with standards of democratic governance, whereas the exact means how to achieve results remains specific to a member state. Prior to the Eurozone crisis, there was a belief that economic convergence would lead to institutional convergence among EU member-states and thus strengthen integration. However, the crisis has showed that the causal link might be the opposite – differences in how policy is implemented may lead to divergence between the member states, and those differences may act to impede integration.

Uniformed services form the core of the coercive capacity of a sovereign state. On the one hand in EU these organizations need to be overseen by democratically elected civilian leaders, and act on the basis of the rule of law; on the other – the management of these services is highly contingent on national contexts. The impact of international best practices is patchy at best and local political consideration constantly risk trumping the adoption of such practices.

The Lithuanian case is of particular interest in this context, as its civil, and uniformed service regulation and structure is highly complex, and does not correspond to the organizational structure, and even the constitutional division of power between branches of governments. A small state with a about 70.000 service-members has a structure of a dozen laws that regulate different aspects of different service. This internal fragmentation means that there is a diffusion of managerial practices even at the national level. We hypothesize that this lowers the capacity to perform the tasks presented to uniformed services.

Method of investigation. The constitutional models of checks and balances create additional costs to the operation of governments in both time and money, but they are expected to yield positive results from the point of view of decision sustainability and compliance to political intent and values. These models tend to separate regulation, oversight, and implementation elements. Further, the agencification process of governance in the past four decades has created new structures that implement narrowly

defined functions, and also have a large degree of autonomy from central government, e.g. regulation and competitive r&d (or similar) funding. Agencification and a complex checks and balances mechanism has created a system that duplicates a multitude of general functions in the uniformed services of Lithuania. We used regulation analysis to demonstrate these process, and identify points where complexity may be reduced in the management of uniformed services.

Investigation Results. Uniformed service in Lithuania develop along divergent paths, as all of them have separate regulations passed by the parliament. As such, it becomes difficult to coordinate or adopt best practices at the level of the institution due to various procedural inconsistencies. On the surface, this appears to be in-line with New Public Management ideology, but there is no evidence to support this notion. The fragmentation is more likely a result of low capacity of political leadership to manage large institutions, and fragmentations reduces the complexity of management from their standpoint, while shifting the burden to institutions themselves, creating complicated separation of functions and mutual oversight mechanisms.

Conclusions. We contend that national coherence of uniformed services is essential for Lithuania to achieve better governance outcomes. The categories of military, police, and corrections are sufficient to achieve all the regulatory goals of oversight among the uniformed services. We believe that sufficient oversight may be achieved by having no more than two institutions in each of these categories, which is not the case now. Meanwhile, such changes would lead to significant decision-making time and overhead cost savings.

Keywords: uniformed services, agencification, institutional fragmentation

Authors' index

A	
Adamonis J.	9
Adlienė D.	105
B	
Bakšys T.	40
Bausys R.	12
Bekesienė S.	12, 15, 33, 77, 121
Bileišis M.	130
Bogdanowicz Z.	79
Bogusz P.	79
Bombalska A.	79
Bystřický R.	89.
C	
Ciburienė J.	24
Cieslak E.	27
D	
Davidavičienė V.	116
Dejmal K.	89
Dobržinskij N.	15
Dubauskas G.	29
Dudzevičiūtė G.	108
E	
Eidukynas V.	19
F	
Fedaravičius A.	37
G	
Gadišauskas T.	19, 22, 105
Gailevičius D.	22
Giedraitė V.	101
Guscinskiene J.	24
H	
Hošková-Mayerová S.	33
Hutsaylyuk V.	98
J	
Japertas S.	40, 45
Juodkasis S.	22
Juozapavičius A.	19, 95
K	
Kalinauskaitė D.	73
Karčiauskas P.	95
Kazlauskaitė Markelienė R.	103
Kelemen M.	48, 51
Kommanaboina N. M.	75
Korecki Z.	54
Koperski W.	98
Kriaučionis K.	128
Krilavičius T.	73
Kubiak M.	56
L	
Lietuvnikė M. M.	57
Łopatka M. J.	59, 62, 65, 68
Luhin V.	105
Lukoševičius L.	71
M	
Malinauskas M.	19, 22
Mandravickaitė J.	73
Manimarana H. P.	75
Matuzas J.	9
Mazeikaite E.	77
Mierczyk Z.	79
Mizeikis V.	22
Molis G.	9
Mularczyk-Oliwa M.	79
Muszynski T.	62, 68
N	
Nasiłowska B.	79
Neubauer J.	84
Neumann V.	82
Novotný J.	87, 89

O
Odehnal J. 84

P
Padolskytė V.22
Papanaboina M. R.75
Petrauskaitė A. 103
Plaipaitė-Nalivaiko R.....19, 105
Prakapas R. 108
Prakapienė D. 108
Prosyčėvas I. 105

R
Rao S. S. 112

S
Sabaitytė J.57, 95, 116
Sarlauskas J.121
Skrzeczanowski W.79
Smaliukiene R.101
Staliunas K.22
Survila A.37
Szabo S.48, 51
Szachogluchowicz I.98
Sniezek L.98

Š
Šakirzanovas S.22
Ślėzak T.92

V
Vajdova I.48, 51
Vasilienė-Vasiliauskienė V.57
Vasilis Vasiliauskas A.57

T
Tabsha Y. El 116
Tamuliene J. 121
Tołwiński M. 124
Topolewski S..... 126
Tumalavičius V. 128

U
Ungurytė-Ragauskienė S..... 130

W
Wachowski M.98
Wawrzyniak P.79

CHALLENGES TO NATIONAL DEFENCE
IN CONTEMPORARY GEOPOLITICAL SITUATION

CNDCGS`2018

ABSTRACTS OF THE 1TH INTERNATIONAL SCIENTIFIC CONFERENCE
EDITED BY S. BEKESIENE AND S. HOŠKOVÁ-MAYEROVÁ

ISBN 978-609-8074-77-2

Chief Editor Svajonė BEKEŠIENĖ
Cover Design by Laima Adlytė

Publishing by
The General Jonas Žemaitis Military Academy of Lithuania
Šilo g. 5 A, LT-10322 Vilnius