Armed Forces Academy
of General Milan Rastislav Štefánik

V4 Group Students' Scientific Conference 2015

ABSTRACTS

Liptovský Mikuláš, Slovak Republic
26th May 2015

The Armed Forces Academy of General Milan Rastislav Štefánik is the non structured faculty state military college. The Academy is situated in Liptovský Mikuláš, Slovak Republic. It is a school that has international acceptance and its main mission is to educate, improve skills and train students in higher and lifelong career education. Its mission is to develop good personality, knowledge creativity and motivation in students to prepare them for service to the country and to be effective within national and international environment.

In addition to education and training, the Armed Forces Academy focuses on development of science and research to support security and defence of the state and development of capabilities within the Armed Forces of the Slovak Republic. The Academy participates in project solution of basic and applied research, in international research projects in terms of EDA as well as in scientific and professional committees. The research results are applied into teaching process and thus the Academy has become a unique base that enhances the quality of personnel training for the Armed Forces of the SR and for the state security community.

V4 Group Students' Scientific Conference 2015

Organizer:

THE ARMED FORCES ACADEMY OF GENERAL MILAN RASTISLAV ŠTEFÁNIK
Liptovský Mikuláš, Slovak Republic
Department Science and Foreign Affairs

Edited by:

PhDr. Jana VITOVSKÁ

ISBN 978-80-8040-507-6

© The Armed Forces Academy of General Milan Rastislav Štefánik, Liptovský Mikuláš, Slovak Republic, 2015

CONTENS

SECTION: MECHANICAL ENGINEERING

SECTION: ELECTRONICAL ENGINEERING

SECTION: INFORMATICS

SECTION: MANAGEMENT, ECONOMICS AND LOGISTICS

SECTION: SOCIAL SCIENCES; NATIONAL AND INTERNATIONAL SECURITY

SECTION
MECHANICAL ENGINEERING

THE DESIGN OF THE ECCENTRIC GEAR FOR UTILIZATION IN AIRCRAFT ENGINEERING

Ondřej FLÁŠAR

Consultant: Assoc. Prof. Eng. Juraj HUB, Ph.D.

University of Defence, Czech Republic, 661 10 Brno, Kounicova 65, ondrej.flasar@unob.cz

Abstract: One of the well known group of wave gears is an eccentric gear. The most important parts of this gear are wave generator, gears and coupling as is usual for this gears.Even if the eccentric gear provides very good properties to its users it has not been already applied in aircraft engineering for higher power transmission. However, its utilization is capable to reduce the weight of structures where the very high reduction ratio is needed. Therefore the eccentric gear has capability to replace the common gear with several stages or multi-staged planetary gear.

This project endeavours to deal with a new design and difficulties which are inherently connected to this structure. Accordingly to last progress, the work will focus on design of a shaft coupling and analysis of a model in this design phase. The shaft coupling represents the most important and the most complicated part of the whole gear. The coupling has to transmit high power and torque while it is dealing with eccentric movement of the gear. Next to the construction of the coupling the project is also focused on the design of apparently common gear parts. The compiled eccentric gear design is furthermore investigated to confirm the strength requirements. The calculation of all gear components is based on verified sources of the calculation methodology.

The outcome of the project should be the design of eccentric gear for an aircraft power plant with a power of 200 kW and with input speed 4500 RPM and output speed 300 RPM. Such eccentric gearbox could consequently replace ordinary reducer in a small class helicopter and serve as a pattern for further improving and designing of the gear with even higher speed.

Keywords: eccentric gear, speed reducer, wave gear, gearbox, coupling

BIBLIOGRAPHY

1. FLÁŠAR, Ondřej. *The design of the eccentric gear for utilization in aircraft engineering. University of Defence.* Brno, 2015.

INSENSITIVE MUNITION

Mário HNÁT

Consultant: Assoc. Prof. Eng. Peter LISÝ, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Mechanical Engineering, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The aim of this workisto introduce the problem with the technology insensitive munition. The insensitive munition means the munition with reduced sensitivity on temperature, impact of bullets and fragments and close blast. Due to wide problem this work will solve only the munition which will be use in small weapon. The first step at the development of the insensitive ammunition was the development the caseless ammunition –CL. Therefore cartridge was without the case the propellant has to fulfil demands which were putted on the case. That means, propellant has to resist temperature in loading chamber, humidity, mechanical damage and has to keep shape and bullet together like the cartridge with the case. The most famous producers in development and production the caseless ammunition and weapon are Heckler&Koch with weapon model G11 and after the program LSAT (Lightweight Small Arms Technologies) Ardec USA. During development of weapon model G11 was introduce new high ignition temperature propellant (HITP) by firm Dynamit Nobel (DNAG). This prototype was not to introduce to German Army due to that this propellant has low temperature cook-off-effect. Nowadays is the caseless ammunition development under program LSAT and here was problem with cook-of-effect solved by introduce the plastic case for the machine gun. The idea of small weight for the cartridge was maintain. The reduction of the cartridge weight is up to 50 % to compare with the brass case. From obtain knowledge my idea is to improve HITP ammunition proper modification and thereby achieve bigger resistance against cook-off-effect. This means, that new HITP will be on the base of HMX and adhesive. The main idea is that only for outer case will be use more thermostable second explosive, which will fill function as protective layer of propellant.

Keywords: insensitive ammunition, caseless ammunition, LSAT

BIBLIOGRAPHY

1. SCHATZ, J. Caseless Ammunition Small Arms. In *NDIA Joint Armaments Conference Seattle, Washington, 2012.* Available on the Internet: http://www.forgottenweapons.com/.../Caseless-Ammunition-Small-Arms.pdf>
2. PATRICIA M. - O'REILLY, M. P. – HARDMEYER, E. – SENSENIG, CH. – ASHCROFT, B. – CLEVELAND, D. - ENGEL, B. – SHIPLEY, P. *Caseless Ammunition & Advances in the Characterization of High Ignition Temperature Propellant.* Available on the Internet: http://www.dtic.mil/ndia/2005smallarms/wednesday/oreilly.pdf>
3. SPIEGEL, K. – SHIPLEY, P. *Lightweight Small Arms Technologies*. http://www.defensereview.com/.../Army%20Science%20Conf%20_3A_.pdf>
4. HARDMEYER, E. K. – ASHCROFT, B. CaselessAmmunition and Advances in the Characterization of High Ignition Temperature Propellant (HITP). In: *NDIA 22nd International Symposium on Ballistics, November 14-18, 2005 Vancouver BC, Canada.* Available on the Internet: http://www.dtic.mil/ndia/22ndISB2005/thursday/shipley.pdf>

5. SHIPLEY, P., PHILLIPS, K. *Lightweight small arms technologies.* May, 2009. Available on the Internet: http://www.dtic.mil/ndia/2009infantrysmallarms/wednesdaysessioniv8536.pdf >
6. PAUL A. - SHIPLEY, P. A. – COLE, B. T. – PHILLIPS, K. *Cased Telescoped Small Arms Systems. US Army ARDEC, May 2014.* Available on the Internet: http://www.dtic.mil/ndia/2014armaments/Wed16533_Shipley.pdf>
7. BRUCE, R. *LSAT – the future of small arms.* Available on the Internet: http://defenceforumindia.com/forum/land-forces/16455-modern-battlefield- technologies.html>
8. Available on the Internet: http://en.wikipedia.org/wiki/Heckler_%26_Koch_G11>
9. Available on the Internet: http://en.wikipedia.org/wiki/Lightweight_Small_Arms_Technologies>

PROPOSALS FOR INCREASE THE TENSILE CHARACTERISTIC OF THE VEHICLE ALIGÁTOR 4X4

Štefan KUNÁŠ

Consultant: Prof. Eng. Peter Droppa, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Mechanical Engineering
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The objective of this work is through the various proposals to point to an increase in the tensile characteristics of the vehicle Aligator 4x4. The work is divided into two parts. The first section describes the technical data of vehicle Aligator 4x4 and the calculation procedure tensile characteristics. The second part focuses on the evaluation of the calculation of four proposals to increase the tensile characteristics of the vehicle Aligator 4x4. The proposals are based on the exchange of original gear groups such as the engine and transmission for more modern and more powerful units. One proposal is based on retaining the original motor-gear system, complemented by a parallel connected electric drive.

Images of mechanisms and graphs of calculations are referred in work. The calculated values are placed in tables in the Attachment of this work. In conclusion there is a summary of the results, which were obtained by comparing the tensile characteristics of the original vehicle with each proposal.

Keywords: aligator 4x4, tensile characteristics, tactical and technical data, gear mechanism, propulsive system, operational data, electrical branch, hybrid

BIBLIOGRAPHY

1. DROPPA , P. *Usporiadanie a popis vozidla Aligátor 4x4 PVS.* 1. vydanie. Akadémia ozbrojených síl gen. M. R. Štefánika v Liptovskom Mikuláši, 2005, 47 s, ISBN 80-8040-265-5.
2. HANZELKA, B., OBERMANN, F. *Teória pohybu kolesových vozidiel*. Časť druhá, Brno, 1981, 172 s.
3. LEJKOVÁ, L. *Rozbor hybridných pohonov a možnosti ich využitia v bojovej technike*, Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika, 2006.
4. Available on the Internet: http://www.yasamotors.com/wp-ontent/uploads/2014/07/Datasheet-YASA-750_en-ID-15637.pdf

POSSIBLE WAYS OF MODERNIZING DRIVE SYSTEM OF IFV-2

Michal MOKRÝ

Consultant: Prof. Eng. Peter Droppa, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Mechanical Engineering
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: In the first part of my work I have stated the basic tactical and technical parameters of BMP-2 and the method of calculating the tensile characteristics. Thanks the tensile characteristics we can determinate the maximum speed of the vehicle,, identify running resistance or determine the ratio of the drive power to the vehicle speed. Then I calculated the tensile characteristics of BMP – 2 with and without involving reduction and Russian BMP - 3 which is ownd by Russina armed forces which is currently one of modern infantry fighting vehicles. It has good ballistic protection, more powerful engine, and also modernized weapon system. Its production was based precisely on IFV - 2 and modernized concept Jackal which was presented at the exhibition IDET Brno in 2013. I compared the tensile characteristics and resulting graphs I mentioned in the Attachments. I prerequisite increase weight appears from increased ballistic protection, especially against mine. Therefore, the original engine and transmission space must be replaced with modern more powerful. In the second part I have used alternative engines how engines from the TATRA company and Cummins company. Instead I used the clutch torque converter. Manual gearbox I swapped for planetary gear. I made various combinations of engines and transmissions in the concept of BMP - 2 and the individual results I stated in graphs that are listed in the Attachments. My work should especially point out the possibility of upgrading IFV – 2. When upgrading, it has to be considered that with increasing vehicle weight, the performance of its engine is decreasing. Thanks to powerful new engine and using a torque converter can reduce the number of gears of maintaining the measuring propulsion power. Even through the torque converter increases the nominal propulsion power for the first two speed steps. The vehicle is able to overcome more challenging terrain than with conventional clutch and allows the full automation. In modern times, requires automatic gear changes.

Keywords: infantry fighting vehicle, tensile characteristics, modernization, tactical and technical data, propulsive power

BIBLIOGRAPHY

1. DROPPA, P. (2003). *Teória pohybu pásových vozidiel*. Liptovský Mikuláš : Vojenská akadémia, ISBN 8080402116, 171 s.
2. MIKLOŠKO, J. (2005). *Návrh elektromechanického pohonu pre vozidlo IFV – 2*. Liptovský Mikuláš : Vojenská akadémia, 81 s.
3. JANUŠEK, J. (2001). *Návrh modernizácie prevodového mechanizmu vozidla BPV – 2*. Liptovský Mikuláš : Vojenská akadémia, 103 s.
4. DROPPA, P. (2003). *Teória pohybu pásových vozidiel*. Liptovský Mikuláš : Vojenská akadémia, ISBN 8080402116, 171 s.

SECTION

ELECTRONICAL ENGINEERING

IMPLEMENTATION OF THE STEGANOGRAPHIC ALGORITHM IN THE SOFTWARE VOIP INTERNET TELEPHONE

Damian BACHMAT

Consultant: Col. Prof. Eng. Zbigniew Piotrowski, DSc., Ph.D.

Military University of Technology, gen. S. Kaliskiego 2 str., 01-476 Warsaw, Poland, babel90@gmail.com

Abstract: The paper describes implementation of the steganographic method based on the least significant bits (LSB) in a program Internet phone VoIP. In the developed program Internet phone VoIP a library PJSIP has been used. Selected technology – LSB is characterized by easiness of implementation and high bit rate and perceptional transparency of a signal with embedded steganographic sequence. In case of the LSB method a change in the least significant bits in a datagram takes place after quantizer of an analog-digital converter circuit. This solution enabled simple implementation of the embedding algorithm by modification of a source code of a codec G.711. One of the advantages of the method is the fact that for determined number of the least significant bits it does not cause an audible speech degradation and therefore, modified speech signal is perceptually transparent for a subscriber at the receiver side. The paper includes results of tests of developed steganographic phone, among others, subjective audible tests based on signal fidelity estimation standard - ITU-R BS 1116-1, tests of minimal, required time of transmission and integrity tests of steganographic sequence.

Keywords: VoIP, LSB, VoIP handset, steganography, data hiding.

BIBLIOGRAPHY

1. MAZURCZYK, W. - SZYPIORSKI, K. - LUBACZ, J. Available on the Internet: http://www.secure.edu.pl/historia/2008/docs/Mazurczyk_Szczypiorski_Lubacz.pdf
2. LIULihua, LI Mingyu, LI Qiong, YAN Liang. *Perceptually Transparent Information Hiding in G.729 Bitstream, Conference onIntelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International*, 2008, pp. 406-409.
3. HUANG, Yongfeng - LIU, Chenghao - TANG, Shanyu – BAI, Sen. *Steganography Integration Into a Low-Bit Rate Speech Codec.* IEEE Transactions on Information Forensics and Security, 2012, pp. 1865-1875.
4. WANG, C. – WU, Q. *Information Hiding in Real-Time VoIP Streams.* Ninth IEEE International Symposium on Multimedia, 2007, pp. 255-262.
5. DHOBALE, D. – GROPHADE, V. – PATIL, B. – PATIL, S. *Steganography by hiding data in TCP/IP header.* Conference on Advanced Computer Theory and Engineering, 2010, pp.: 61-65.
6. *RFC 791*. Available on the Internet: https://www.ietf.org/rfc/rfc791.txt
7. *ITI-T G.107.* The E-model, a computational model for use in transmission planning, 2005, pp. 8.
8. MUHAMMAD, A. – JUNAID, G. - ADNAN, K. *An Enhanced Least Significant Bit Modification Technique for Audio Steganography.* IEEE, 2011 International Conference onComputer Networks and Information Technology (ICCNIT), pp.: 143-147.
9. Available on the Internet: http://www.pjsip.org

10. Available on the Internet: http://www.twt.wt.pw.edu.pl/download/telekol/TK-VoIP.pdf

11. BERITELLI, F. - CASALE, S - RUGGERI, G. *Performance evaluation and comparison of ITU-T/ETSI voice activity detectors.* IEEE, Conference on Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International, 2001, pp. 1425-1428.

CIRCUITS CHANNEL OF SIGNALS AND BRANDS OF INDICATORS TYPE A

Tatiana BAJOVÁ

Consultant: Assoc. Prof. Eng. Bohuslav Lakota, CSc.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Electronical Engineering
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The work presents a proposal of the measuring plate of the time base channel to be useful for measurements in the laboratory conditions. Content of the work is divided into three main chapters. The first chapter consists of a general overview of display systems. This chapter specifically indicating incorporation of the structure of the radar station, along with the schemes of active, semi-active and passive radiolocation. The second point is the identification and it also contains all kinds of display systems, where is also their further division. The third point is their exploitation. Fourth point includes characteristic of indicator and formula for the calculation of the light spots and coefficient of observability. There is an explanation of the distance indicators and their simplified block diagram at the end of the introductory chapter.

The second chapter dealing with an issue of electron-optical display elements. At the beginning of the chapter, imaging element is defined and subsequent division of display elements. In the second part of the chapter there is a general overview of electron-optical imaging elements, as well as the principle of their operation. For better understanding the principle of operation it is also shown in attached figure. Subsequently there is a description of the types of screens with electrostatic focusing and electrostatic deflection. Motion of charged particles and basic shapes of the lenses are expressed in the part of electrostatic focusing. In the part dealing with electrostatic deflection it is briefly mentioned how this could be achieved by the deflection and consequently the movement of the electrons between the deflection plates is shown.

The third chapter includes the design of the measuring plate, where is at the beginning illustrated a simplified block diagram of a type indicator A and simple description of it. In the following part there are listed components that are necessary for constructing of the measuring plate.

A short characteristics is mentioned by each component, its layout and formulas needed for calculation. Measuring table suggested this way is designed especially for laboratory use.

Keywords: indicator, measuring plate, display systems

BIBLIOGRAPHY

1. STANÍK, P. *Rádiolokační indikační systémy.* VVTŠ-ČSSP, Liptovský Mikuláš, 1985.

CIRCUIT OF THE TIME BASE OF INDICATORS A TYPE A

Samuel BUC

Consultant: Assoc. Prof. Eng. Bohuslav Lakota, CSc.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Electronical Engineering
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: My work deals with the problems of indicator systems that are used as indicators of radar information for operators. The work is divided into three chapters, the first two are addressing to issue at the theoretical level and the last third chapter is a practical part of the work, which confirms the correctness of our theory and its applicability in practice.

The first chapter is entitled Overview of radar and indicator systems. In this chapter we incorporate indicator systems into the radar structure as an output device. Indicator systems are subdivided according their types and destination, and on this distribution are discussed different types of indicators bases and types of display indication with the relevant graphic examples. The last part of the first chapter is devoted to the characterization of indicators, especially coefficient of observability, light spot diameter, distinction ability and precision of indicators are analysed.

The second chapter deals with the principle of type A indicator, so it is the indicator with one channel screen, which shows us only one coordinate - distance to target. This principle is explained on a scheme and time courses. Furthermore, the scheme describes the operating principle of the indicator with dual-channel screen, which gives us a more accurate reading of distances of screen.

The third chapter is devoted to the circuit channel of signals and brands of indicator type A. This is a proposal of the measuring plate. On the measuring plate we will be able to track activity of circuit of indicator, where are produced signals and signs of target. The individual outputs are displayed on an oscilloscope. Plate is constructed from integrated micro components and it is supplied with 5 V.

Keywords: indicator, measuring plate, signals

BIBLIOGRAPHY

1. STANÍK, P. *Rádiolokační indikační systémy.* VVTŠ-ČSSP, Liptovský Mikuláš, 1985.

SOFTWARE MODEL OF SOLID STATE RADAR TRANSMITTERS

Martin GEROČ

Consultant: Assoc. Prof. Eng. Ján Ochodnický, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Electronical Engineering
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: My work is focused on area of radio engineering, specifically in radar transmitters. In the past, transmitters were constructed in base of using vacuum tubes but now we are using modern solid state technology to construct more effective transmitters. Solid state transmitters are based on using semiconductor tranzistors because of better properties toward vacuum tubes. Solid state transmitters has longer mean time between failures which can provide longer operation of transmitters without need to repair.

In this work I would like to present software model of solid-state radar transmitter which I made. It is a model which can be helpful for construction of real solid-state transmitter. This tool can simulate influences of same amplitude but different phase on power synthesis or influences of same phase but different amplitude on power synthesis of transmitter. In this tool, designer can make his own model with different parameters. Main advantage is that designer does not have to spend lot of money for different types of construction, but he can try it in simulation area. This software can save money and provide realistic simulation of designed transmitter with minimal deviation. I simulated both types of different phase or amplitude. In case with different phase but same amplitude I simulated phase shift up to ninety-five percent efficiency at output. In case with different amplitude but same phase I made model when amplitudes are the same, when first amplitude is equal to zero and the second is higher than zero and at the end I simulated situation when the difference between first and second amplitude is equal to thirty decibels.

Keywords: solid state, transmitter, simulation, phase shift, different amplitude

BIBLIOGRAPHY

1. HU, BEI - FENG, YANMIN. *"The 1000W microwave solid state power amplifier at Ku band*," *Radar (Radar*), 2011 IEEE CIE International Conference *on* , vol.2, no., pp.1211,1214, 24-27 Oct. 2011 doi: 10.1109/CIE-Radar.2011.6159773.

MATHEMATICAL MODELS OF MODULATION SIGNAL TYPES

Jana KOCHJÁROVÁ

Consultant: Assoc. Prof. Eng. Zdeněk Matoušek, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Electronical Engineering
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: In my work I focused on mathematical description of functions and construction of several different types of modulators and demodulators. According to the mathematical descriptions I decided to create an application program, which could be used for simulation and analysis of the chosen modulators and demodulators. The application program was created in Matlab 2013b and in Matlab´s graphical extension for modeling and simulation of systems named Simulink. The result of my work is a set of eight different, dynamic systems based on programmed block diagrams. Individual blocks are made by a tool called Embedded Matlab Function Block, whose characteristics could be programmed in Matlab language (m-code). The created programmed application consists of two parts. The first part is created in Matlab-Simulink where I programmed several kinds of different modulators and demodulators. Due to these mathematical models it is possible to simulate radio transmission and reception of signals with chosen type of modulation. The second part of the application program is aimed on analyzing various kinds of signals according to graphical displays of signal in time, frequency or time-frequency domain. There is also a possibility of testing by programmed test created mostly by using Matlab objects called uicontrol. During the test the user is able to look again at the graphical displays of used signal in time, frequency or time – frequency domain. According to the mentioned graphical displays of signal the user is supposed to answer on test questions. Whether the user succeeded or not it is automatically evaluated in the end of the test by giving a percentage score.

The application program could be used like a study tool during studying different modulation signal types. Furthermore, it could be used by teachers to check up student´s knowledge from the subject.

Keywords: modulator, demodulator, modulations, simulation and analysis of signal

BIBLIOGRAPHY

1. DOBEŠ, J. – ŽALUD, V. 2006. *Moderní radiotechnika*. 1 vyd. Praha : BEN – technická literatura, 2006. ISBN 978-80-7300-293-0.
2. ZAPLATÍLEK, K. – DOŇAR, B. 2004. *MATLAB tvorba užívatelských aplikácí.* 1 vyd. Praha : BEN – technická literatura, 2004. ISBN 80-7300-133-0.
3. *MATHWORKS-Accelerating the pace of engineering and science: Simulink Simulation and Model-Based Design* [online]. Web mathworks.com. [Dátum: 25.04.2015]. Available on the Internet: <http://www.mathworks.com/products/simulink/

SIMULATION OF SIMPLEX RADIO COMMUNICATION IN LAN NETWORKS

Marek LIPTÁK

Consultant: Eng. Marián Babjak, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Electronical Engineering
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The paper presents a software tool for simulation of simplex radio communication in LAN network. The aim of the simulator is to provide tool for training radio communication procedures, which can be used in the classroom without radiation of electromagnetic power and without using of radios. Proposed simulator is also suitable for simulation of radio communication in simulation center for training of command and control procedures, where radios cannot be used.

Simulator consists of two applications, server and client. Server application is used to configure radio networks parameters. Each radio network is simulated as multicast group, so multicast address and port have to be defined. For visualization purposes, for each network name and frequency is defined. Configuration of the clients is done from server automatically over unicast TCP connection. The protocol for communication between server and client is also presented.
Simulator enables configuration of 9 radio networks with unlimited number of radios inside each network. Server application allows recording and listening-in.There is a possibility to select recording for all radio networks. All records are saved in selected destination folder. Name of recorded file is generated automatically and it consists from network name, date and time. Only one radio network can be selected for listening-in.

Client application user interface is designed as front panel of radio. Information about selected radio network, name and frequency are displayed on the display in upper part. One of nine radio networks can be selected by click on the buttons. Push to talk (PTT) button is used to switch between the functions, transmitting when pressed, receiving when released.

Keywords: training of radio operators, multicast for voice broadcasting, TCP UDP, IP.

BIBLIOGRAPHY

1. *RFC1122, Requirements for Internet Hosts - Communication Layers.* Internet Engineering Task Force, 1989.
2. *DE GOYENECHE, J. M. Multicast over TCP/IP HOWTO.* Available on the Internet: http://www.tldp.org/ HOWTO/Multicast-HOWTO.html

CHAFF EMPLOYMENT

Maria-Mădălina NICOLAE

Consultant: Lt. Col. Eng. Laurian Gherman

„Henri Coanda" Air Force Academy, Brasov, Romania 500187 Braşov, Mihai Viteazul street
sekretariat@afahc.ro

Abstract: The paper deals with defensive mechanism employed from military aircraft to avoid detection and/or attack by adversary air defense system, known as "chaff". This consists of small fiber that reflect radar signals and when dispensed in large quantities from aircraft, form a cloud that temporarily hides the aircraft from radar detection. When ejected from an aircraft, chaff forms the electromagnetic equivalent of a visual smoke screen that temporarily hides the aircraft from radar.

The principal ingredient of foil type chaff and of the coating on the fiber chaff is aluminum metal, one of the most abundant metals in the earth's crust, water, and air. Although unlikely, humans and animals may be exposed to aluminum from chaff through ingestion or inhalation. In general, aluminum is regarded as relatively nontoxic. Aluminum compounds are often found as food additives and used in the treatment of potable water.

Chaff also serves to decoy radar allowing aircraft to maneuver or egress from the area. Modern armed forces use chaff to distract radar-guided missiles from their targets and most military aircraft and warships have chaff dispensing systems for self-defence. The materials in chaff are generally nontoxic except in quantities significantly larger than those any human or animal could reasonably be exposed to from chaff use.

Keywords: chaff, radar countermeasure, self-protection tactics, radar Cross Section

BIBLIOGRAPHY

1. FRANKLAND, N - WEBSTER, C. 1961. *The Strategic Air Offensive Against Germany.* 1939-1945, Volume II: Endeavour, Part 4, London : Her Majesty's Stationery Office, pp. 260-261.
2. WIEGAND, R. J. *Radar Electronic Countermeasures System Design*. Artec House, Inc., Norwood, MA, 1991.
3. *Electronic warfare fundamentals.* November 2000.
4. *Environmental effects of self-protection chaff and flares.* Prepared for: U.S. Air Force Headquarters Air Combat Command Langley Air Force Base, Virginia, August 1997.

POSIBILITIES OF THE SOFTWARE-DEFINED RECEIVERS IN THE COMMUNICATIONS INTELLIGENCE

Juraj ONDREK

Consultant: Mjr. Eng. Roman Berešík, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Electronical Engineering
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The use of a modern communications and informations technologies in military applications is characterized by using of software defined radios. At this fact is necessary to respond in sector of the communications intelligence, where the analog scanning receivers are substituted by the modern software-defined receivers. These receivers are able to not only carry out a reconnaissance in the bandwidth of several to tens MHz, but also to perform the signal analysis. The goal of work was to perform an analysis of the issue of software-defined receivers and the applications of software-defined receivers, which are useful in a military environment. Analysis of the software-defined receivers producers' products points out that, the certain subgroups of these devices arise according to the customer requirements, whose parameters are specific from viewpoint of required applications. Practical outputs of work are functional simulation models of software-defined receiver, that are usable for the needs of the communications intelligence. Receiver model is conceptually designed as a software-defined receiver with sampling of the baseband signal. The model consists of two parts, the hardware and the software parts. The hardware part consists of a software-defined receiver of Terratecs brand , that contains a tuner E4000 and a demodulator RTL2832 in its structure. Software-defined receiver is connected to PC via USB. The software part is executed in Matlab Simulink. The outcome of this work are two models of software-defined receiver. The first model provides a receiving and monitoring of the communications operations with frequency modulation. The second model is able to analyze the received communications operations in the frequency and time-frequency domain using the method of calculation a periodogram and Welch's algorithm in the whole band of software-defined receiver's retuning .

Keywords: software defined receiver, communications intelligence, posibillities, analysis

BIBLIOGRAPHY

1. ŽALUD, V. *Modern radioelectronics*. BEN, Prague, Czech Republic, 2000.
2. Available on the Internet: http://www.mathworks.com

IR (INFRARED) MISSILE SEEKERS FUNDAMENTALS

Marius ȘTEFĂNESCU

Consultant: Lt. Col. Eng. Laurian Gherman

„Henri Coanda“ Air Force Academy, Brasov, Romania 500187 Braşov, Mihai Viteazul Street
sekretariat@afahc.ro

Abstract: The paper is dedicated to presenting some information about infrared energy and infrared seeker based missiles. More exactly, it contains details about basic infrared theory, infrared seekers main components and infrared seeker types. The first part contains data about infrared frequency, infrared energy wavelengths and groups of infrared energy created on different criteria. This chapter is designed to familiarize the readers with some abbreviations and specific terms related to infrared energy. There is also information about infrared spectrum and characteristics of each subgroup, atmospheric infrared transmission in different conditions, absorption and scattering, along with causes and molecules responsible for each of them. Some environments are compared based on criteria mentioned before in order to present the best conditions for using infrared energy. The first part includes important facts about the infrared signature and intensity of an aircraft, related to its components, viewing angles, environment and flying conditions. The middle part is dedicated to presenting the main parts and characteristics of an infrared seeker. It also details each part and establishes its role and special characteristic, but also describes its functionality, advantages and some disadvantages. There are also presented two types of infrared missile seekers, each of them having some distinctive components made to improve their responsiveness and compatible infrared spectrum. All their components are presented and the second infrared seeker type is compared to the first one regarding its accuracy and advantages. The conclusion refers to some related topics that must be studied in order to have a complete image of infrared missiles, but also to topics that are continuously developing.

Keywords: infrared Energy, IR signature, IR Missile, IR seekers;

BIBLIOGRAPHY

1. *Electronic Warfare Fundamentals.* ACC Training Support Squadron Det 8, ACC TRSS/RA, 4349 Duffer Dr., Nellis AFB, NV 89191-7007, 2000.
2. JACK, R. W. *Aircraft Infrared Principles, Signatures, Threats, and Countermeasures*. Naval Air Warfare Center Weapons Division, Point Mugu, CA 93042, 2012.
3. YATES H. W. - TYLOR J. H. *Infrared transmission of the atmosphere.* US Naval Research Laboratory, Washington DC, 1960.
4. VIAU, C. R. *Expendable Countermeasure Effectiveness against Imaging Infrared Guided Threats.* Tactical Technologies Inc., 356 Woodroffe Ave., Ottawa, ON Canada, 2012.
5. *Infrared.* Available on the Internet: http://en.wikipedia.org/wiki/Infrared (last visit 21 April 2015)
6. *Infrared homing.* Available on the Internet: http://en.wikipedia.org/wiki/Infrared_homing#cite_ref-brevco_1-0, (last visit 22 April 2015)
7. *Electronic warfare.* http://en.wikipedia.org/wiki/Electronic_warfare (last visit 23 April 2015)

IMPLEMENTATION OF THE IEEE 802.11 STANDARD BASED ON THE ETTUS-USRP PLATFORM

Ernest SZCZEPANIAK

Consultant: Col. Prof. Eng. Zbigniew Piotrowski, DSc., Ph.D.

Military University of Technology, gen. S. Kaliskiego 2 str., 01-476 Warsaw, Poland, ernest_szczepaniak@wp.pl

Abstract: This paper is devoted to the hardware implementation of a receiver device, working in accordance with the IEEE 802.11 a/g/p standard with the use of the ETTUS-USRP prototyping platform and the Matlab/C++ environment. The presented module , working on the basis of the OFDM technique allows for full interference of the user both in the physical layer (PHY) and the medium access control layer (MAC) of the OSI [1] model. The document contains a detailed description of the applied algorithms as well as the test results which are aimed to verify the hardware demonstrator both in term of its operating parameters and the correctness of detection procedure.

Keywords: software defined radio, wireless communication, Wi-Fi standard

BIBLIOGRAPHY

1. *ISO standard 7498-1:1994 Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.*
2. BLOESLL, B. - SEGATA, M. - SOMMER, C. – DRESSLER, D. F. *An IEEE 802.11 a/g/p OFDM Receiver for GNU Radio.* Proceedings of ACM SIGCOMM 2013, 2nd ACM SIGCOMM Workshop of Software Radio Implementation Forum (SRIF 2013), Hong Kong, China, August 2013.
3. PELLEGRINI, V. – BACCI, G. – LOUISE, M. *Soft-DVB: A Fully-Software GNURadio-based ETSI DVB-T Modulator.* University of Pisa - Dip. Ingegneria dell'Informazione - Via Caruso - 56122 Pisa, Italy.
4. RONDEAU, T. W. - MCCARTHY, N. - O'SHEA, T. *SIMD Programming in GNU-Radio: Maintanable and User-Friendly Algorithm Optimization with VOLK.*
5. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 2012.
6. LIU, C. H. *On Designing of OFDM Signal Detection Algorithms for Hardware Implementation*. Wireless Communication Technology Lab. Chunghwa Telecomm Laboratories 12, Lane 551, Min-Tsu Road Sec 5.
7. KNAPP, C. H. - CARTER, G. C. 1976. *The generalized correlation method for estimation of time delay.* IEEE Transactions on Acoustics, Speech and Signal Processing ASSP-24(4), 320-327.
8. SCHMIDL, T. – COX, D. *Robust frequency and timing synchronization for OFDM*. IEEE Transactions on Communications, vol. 45, no. 12, pp. 1613–1621, 1997.

INFRARED COUNTERMEASURES

Erik-Sebastian TOTH

Consultant: Lt. Col. Eng. Laurian Gherman

„Henri Coanda“ Air Force Academy, Brasov, Romania 500187 Braşov, Mihai Viteazul Street
sekretariat@afahc.ro

Abstract: The paper deals with aerial infrared countermeasures used by airplanes or helicopters to intercept an infrared homing missile, known as "flares". They are used to make the guided missile seek out the heat signature from the flare rather than the airplanes or helicopters engine. There are various and different kinds of flares, based on the aircraft size or weight and on the type of the missile lauched toward it. Also, the present paper lay emphasis on the most common and most advanced infrared countermeasure systems which are used nowadays, not only by the fighting aircrafts, but by medical, supply and transport aircrafts too. The continuous development of the infrared countermeasure systems and of the seeking missiles, the importance of the flare deployment and the reactions of the pilot with the exactly right maneuvers will be counting in order to save aircrafts from crashing or even the lives of the crew on bord.

Keywords: infrared countermeasures, decoy flare, missile, advanced threat, radar

BIBLIOGRAPHY

1. DEYERLE, C. M. *Advanced Infrared Missile Counter-Countermeasures.* Journal of Electronic Defense, January, 1994, Vol. 17, No 1, pp. 47-70.
2. HUDSON, R. *Infrared System Engineering*. Hoboken, New Jersey, John Wiley & Sons, 1969.
3. WIEGAND, R. J. *Radar Electronic Countermeasures System Design.* Artec House, Inc., Norwood, MA, 1991.
4. *Electronic warfare fundamentals.* November, 2000.
5. Available on the Internet: http://www.globalsecurity.org/military/systems/aircraft/systems/ircm.htm
6. Available on the Internet: http://www.laserfocusworld.com/articles/print/volume-47/issue-8/features/photonics-applied-defense-ir-countermeasures-aim-for-safer-flights.html
7. Available on the Internet: http://www.militaryaerospace.com/articles/2013/11/circm-emd-phase.html
8. Available on the Internet: http://science.howstuffworks.com/guardian2.htm

SECTION

INFORMATICS

LINUX LIKE A FULL-FLEDGED DESKTOP OPERATING SYSTEM

Rudolf BUXA

Consultant: Eng. Miloš Očkay, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The work deals with the use of operating systems based on Linux as a fully-fledged operating system. Linux based operating systems provide free solution for wide variety of users. Biggest problem is to choose the appropriate distribution. Those are many kinds, with or without graphical user interface, free or paid, for basic or advanced users.

My goal in this work, was to find the suitable distribution for desktop PC and compose a set of applications which can run on Linux and meet the requirements of average user on operating system. The first section is devoted to user needs investigation, research of the way in which they use their personal computers, of the situation on the OS market and of software requirements on the desktop system.

The second part is devoted to the selection and characterization of specific applications. I composed a set of applications with information gained from research. This set covers all work which typical user do on his computer. All of these applications are free and can be downloaded from various internet sites

In the third part of the work I focused on the choice of Linux distribution most appropriate to use for average users. Conditions were: graphical user interface (GUI), free, low hardware requirements, simple installation, simple to use and compatibility with my set of applications.

My set of applications and choice of Linux distribution is not the only right and same as entire Linux is highly customable according to a taste of a user.

Keywords: linux, operating system, desktop system, user system, Unix, Ubuntu

BIBLIOGRAPHY

1. VALADE, J. *Linux - Jdi do toho.* Grada, Praha, 2006.
2. GAGNE, M. *Přejděte na Linux - Dejte sbohem modré obrazovce!* SoftPress, Praha, 2004.
3. Available on the Internet: http://www.linux.cz/

ACCESS MONITORING AND ITS UTILISATION FOR SECURITY

Bohumil ČERVENKA

Consultant: Assoc. Prof. RNDr. Ľubomír Dedera, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: In recent years we have been witnessing violation of human rights regarding privacy. Ordinary people find it really difficult to protect themselves against stalking. These facts force us to resolve this complicated problem. There are more solutions and applications which focus on helping us protect our privacy. But we can´t find any complex solution with necessary level of protection. So this is the reason, why this solution has been created– an application based on .NET platform. .NET platform is a virtual machine and provides possibility to start applications on different operating systems where.NET is installed. This platform allows higher level of protection and helps keep application protected from other processes. It´s important because all applications with similar functionality require Admin rights. This solution built on .NET uses low-level API to obtain information about files used by the system. Low-level API provides higher level of safety, because the application doesn´t access directly into the kernel core. Obtained information is analyzed in a few steps for detecting potential viruses and dangerous applications. The results of the analysis contain information about processes, files, access times, and other. This solution isn´t universal and can´t create ideal defense, because it can't detect inactive viruses or dangerous pieces of code, but, in some cases, it can help detect system violations and keep data safe.

Keywords: security, privacy, data protection, basic system analysis

BIBLIOGRAPHY

1. ROBINSON, S. *C# Programujeme profesionálně*. Computer Press, Brno, 2003.
2. JEROME: *How to suspend and resume processes in C#*. Available on the Internet: < http://psycodedeveloper.wordpress.com/2013/01/28/how-to-suspend-and-resume-processes-in-c/>.
3. *Listing Used Files*. Available on the Internet: http://www.codeproject.com/KB/shell/OpenedFileFinder.aspx?fid=422864&df=90&mpp=25&noise=3&sort=Position&view=Quick&fr=26&select=2277170>

ANONYMITY AND PRIVACY DURING UTILIZATION OF INTERNET SERVICES

Ivana HUDECOVÁ

Consultant: Eng. Miloš Očkay, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The purpose of this bachelor's thesis is to highlight the important aspects of anonymity and privacy of the user in the use of selected Internet services. The aim of the thesis is also to verify the fact, that the user is the only one who is responsible for anonymity and privacy in the Internet environment. In this way, it is not possible to rely on service providers or legislation.

In the first part, there is basic terminology such as personal information, data, privacy and their legislation protection. This part also focuses to show legislative protection in the Internet environment. It also includes definitions of the set of services that are used by regular users almost on a daily basis as well as their objective characteristics.

The next part is aimed to analyse the relation between users and the Internet service provider as far as the invasion of privacy and anonymity is concerned.

In the final chapter, there are outlines of the possible threats arising from the identified facts. It also shows the possible defence mechanisms to maximize the level of the user's privacy and anonymity during utilization of Internet services.

Keywords: anonymity, privacy, Internet services, personal information, threats, defence mechanisms, user, service provider, relation

BIBLIOGRAPHY

1. BUCKO, J., MIHÓK, P. 2008. *Elektronické služby v bankovníctve.* Košice : Technická univerzita, 2008. 125 s. ISBN 9788055300528.
2. MAISNER, M. a kol. 2013. *Základy práva informačných technológií*. 1. vyd. Bratislava : Iura Edition, 2013. 317 s. ISBN 9788080785949.
3. MAKULOVÁ, S. 1995. *Sprievodca po Internete*. Bratislava : Easy Learning & Teaching, 1995. 144 s. ISBN 80-88812-00-3.
4. MUSA, H. a kol. 2011. On-line bankové služby a ich využívanie v podmienkach Slovenskej republiky. In *Zborník recenzovaných príspevkov z II. medzinárodnej vedeckej konferencie FIN STAR NET.* Bratislava : Ekonomická univerzita, 2011. ISBN 970-80-970244-4-4.
5. *Ústava SR*. Bratislava : Remedium, 1992. 139 s. ISBN 8085352060.

VULNERABILITY ASSESSMENT AND PENETRATION TESTING OF WEB SERVERS

Ján KIMÁK

Consultant: Eng. Július Baráth, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The objective of this research is to process a study about vulnerability assessment and penetration testing of web servers. Vulnerabilities are holes in a system which allow hackers to attack and gain access to the system. It describes the difference between a white box test and a black box test. The paper explains vulnerabilities of web servers, which we can test to find out how dangerous these vulnerabilities are and how could they impact the service. We practically demonstrate the most common attacks on a vulnerable server. Based on results, we can deduct possible measures to minimize the risk of a succesfull attack.

Keywords: penetration testing, vulnerability assessment, web server

BIBLIOGRAPHY

1. ENGEBRETSON, P. – KENNEDY, D. *Basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. 02. vyd. S.l. : Syngress Media, U S, 2013. ISBN 0124116442.
2. WEIDMAN, G.. *Penetration testing: a hands-on introduction to hacking*. xxviii, 495 pages. ISBN 1593275641.

EVERYTHING COMES WITH A PRICE

Jozef KOSTELANSKÝ

Consultant: Assoc. Prof. RNDr. Ľubomír Dedera, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: During last few years Android became one of the most used OS in the world. This is the reasons while mobile device security is becoming increasingly important. All mobile applications can be hacked. A group of hackers with enough time and dedication can gain access to, and reverse engineer, even the most secure application environment. Android hacks come in all shapes and sizes, but the following are most common exploits: Application Piracy, Repackaging, Memory Hacking, Payments Verification Manipulation, Server Data Interpretation, Attack Application Creation. Known proverb says that everything comes with a price. Android ecosystem is not different. Generally , it is possible to divide Android applications into four main categories:

1. Paid applications
2. Applications with adverts
3. Malicious applications
4. FOSS

This paper will be mostly focused on third category, and more specifically on android applications downloaded from other sources than Google Play, such as unofficial markets, personal google drives, or sites like uloz.to. Paper will mostly consist of static code analysis of samples. This mean, to find out if they are malicious or not, usually using reverse engineering.
In the conclusion, paper tried to advice user not to install applications from unofficial markets and also conclude with, that Windows crack for games or Office are usually also malicious.

Keywords: android, security, reverse engineering

BIBLIOGRAPHY

1. DRAKE, Joshua J. *Android hacker's handbook*. xxix, 545 pages. ISBN 11-186-0864-X.

ANALYSIS OF NETWORK COMMUNICATION

Michal KOVÁČ

Consultant: Mjr. Eng. Michal Turčaník, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: Packet analysis is one of the basic methods of implementing network firewalls and analyzing network problems. The aim of this thesis is to analyze communication in a packet-switched computer network using an FPGA board. The theoretical part of the thesis focuses on packet filtering and field programmable gateway arrays (FPGAs). The practical part describes the research platform we built and the process we used to analyze network communication. The research platform was composed of two main parts – Virtex 5 programmable FPGA board and a program running on a computer. The board was used to sniff packets traveling over the network in order to record various statistical data. The software was used to communicate with the board and to collect the evaluated packet data. The data was collected in two sessions. The first session monitored student traffic and recorded over 1,6 million packets of varying types. The second session monitored controlled traffic and recorded over 160 thousand packets, mostly of HTTP protocol. The research serves as a starting platform for future application in hardware packet filter firewalls.

Keywords: packet filtering, FPGA, firewall

BIBLIOGRAPHY

1. STROM, D. *The Packet Filter: A Basic Network Security Tool.* Available on the Internet: http://www.giac.org/paper/gsec/131/packet-filter-basic-network-security-tool/100197 2002 (2002)
2. FERGUSON, P. – SENIE, D. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing : RFC2827.* Available on the Internet: https://www.ietf.org/rfc/rfc2827.txt (2000-05-01)
3. MAXFIELD, C. *FPGAS : Instant Access.* Oxford : Newnes, 2008. 216 s. ISBN 978-0-7506-8974-8.
4. *XILINX DS100 Virtex-5 Family Overview*. Available on the Internet: http://www.xilinx.com/support/documentation/data_sheets/ds100.pdf (2009-06-02)
5. *ML505 User Guide.* Available on the Internet: http://www.xilinx.com/support/documentation/boards_and_kits/ug347.pdf (2011-05-16)
6. *Virtex-5 Embedded Tri-Mode Ethernet MAC Hardware Demonstration Platform*. Available on the Internet: http://www.xilinx.com/support/documentation/application_notes/xapp957.pdf (2008-10-08)

VISUALIZATION OF THE RESULTS OF RISK ANALYSIS ACCORDING TO THE STANDARD STN ISO/IEC 27005

Tomáš MAŤKO

Consultant: Assoc. Prof. RNDr. Ľubomír Dedera, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: Regarding to the rapid development in the information and communication technologies is ensuring of information security in the organization one of the most difficult task. There were created standard technical tools with standard procedures which can reduce the impact of risks to the organization, so organization did not solve their security problems separately. To protect information security is being used set of standards ISO/ IEC 27000, which are one of the most popular tools in the management of information security. In my work i focus on visualizing risk analysis according to the standard STN ISO/IEC 27005, which contain recommendations for risk management within the organization. Visualization of risk analysis should serve as a basis for decision-making processes in companies or the implementation of standard STN 27001, which provides support for monitoring, improving of ISMS (Information Security Management Systems). In the first chapter, i have described the basic terms of my work for example: assets, threats, vulnerabilities, information security and so on, because of understanding the overall work. In the second chapter i have mentioned basic methods of creating risk analysis according to standard STN ISO/IEC 27005 and also i have shown some examples of calculating the level of risk if we know basic value of assets, threats which act on assets or the likelihood of incidents and so on. In the last chapter i have created own organisation, in which i showed the use of standard ISO/IEC 27005. To prove the usage of standard i have created own application which automatically visualizes results of risk analysis.

Keywords: ISMS, risk, risk Analysis, threat, asset, information security STN ISOC/IEC 27005

BIBLIOGRAPHY

1. MAŤKO, T. *Visualization of the results of risk analysis according to the standard STN ISO/IEC 27005.* AFA, Liptovský Mikuláš, Slovak Republic, 2015.

USING ARTIFICIAL INTELLIGENCE IN CRYPTOGRAPHY

Jaroslav PETRÍK

Consultant: Mjr. Eng. Michal Turčaník, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The main aim of this bachelor thesis is to provide brief introduction into methods of artificial intelligence and cryptography algorithms. Moreover, this thesis provides possible view of using methods of artificial intelligence in the area of cryptography, more specific in the area of elliptic curves. The thesis is divided into two main parts. In the first part are stated following chapters: Artificial intelligence, Cryptography and The basics of theory of elliptic curves. Each chapter contains its subchapters. The first chapter Artificial intelligence is divided into four main parts. Each part briefly describes one of the methods which are being used in the area of artificial intelligence. Names of those methods are: The expert systems, Fuzzy logic, Genetics algorithms and the last method stated in this thesis, Neural networks. The second chapter of this thesis is devoted to cryptography. This chapter contains basic information about basic communication model and its brief description, division of cryptographic systems from several points of view and few samples of symmetrical and asymmetrical ciphering such as DES and AES algorithms or RSA and DL ciphering systems. The last chapter of the first part of this thesis contain the basic knowledge about elliptic curves arithmetic and description of several algorithms based on elliptic curves, such as ECDH for key exchange and ECDSA for electronic signatures. Also it includes part about algorithm ECIES, which is meant to be a ciphering algorithm, but this thesis reveals, that it is not. The second part of this thesis provides possible view of using methods of artificial intelligence in the area of cryptography, more specific in the area of elliptic curves. This view serves as one of many possible techniques that can be used in area of implementation of methods of artificial intelligence in elliptic curves based cryptography.

Keywords: artificial intelligence, elliptic curves, neural networks, cryptography, ciphering

BIBLIOGRAPHY

1. LEICKÝ, D. 2005. *Kryptografia v informačnej bezpečnosti*. Košice : Elfa, 2005. 274 s. ISBN 80-8086-022-X.
2. SINČÁK, P. - ANDREJKOVÁ, G. 1996. *Neurónové siete: Inžiniersky prístup.* 1. diel. [online]. 1996. 117 s. Dostupné na internete : http://neuron-ai.tuke.sk/cig/source/publications/books/NS1/html/all.html
3. SINČÁK, P. - ANDREJKOVÁ, G. 1996. *Neurónové siete: Inžiniersky prístup.* 2. diel. [online]. 1996. 117 s. Dostupné na internete : http://neuron-ai.tuke.sk/cig/source/publications/books/NS2/html/all.html
4. BLAKE, SEROUSSI, SMART. 2005. *Advances in Elliptic Curve Cryptography* [online]. Cambridge University Press, 281 p. [cit. 2015.29.03] Available on the Internet: http://www.google.sk/books?hl=sk&lr=&id=E3hVu5ZjbxQC&oi=fnd&pg=PR9&dq=elliptic+curves+encryption+algorithm+%2BECIES&ots=GAJhUKzewy&sig=En5PV3sG7XPRTpiSQl6C9tE9HtA&redir_esc=y#v=onepage&q=elliptic%20curves%20encryption%20algorithm%20%2BECIES&f=false

INCREASE SECURITY OF VOIP SYSTEM BASED ON CISCO UNIFIED COMMUNICATIONS MANAGER TECHNOLOGY

Kristián SIMEONOV

Consultant: Eng. Miroslav Ďulík, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: In my student´s scientific thesis, I will try to introduces VOIP (Voice over Internet Protocol) system, its security challenges, and potential countermeasures for VOIP vulnerabilities. At the beginning of the work there are described the basic features and principles, which are implemented in the transmission of data communications technology. It also offers an overview of hardware components used to implement VoIP within IP networks. Then followed by a section describing protocols that are used in VoIP environments. Specifically, the standards of H.323, SIP, MGCP and SCCP used for signaling, managing and terminating connections, plus introduction to RTP protocol which provide end-to-end network transport function intended for applications with real-time requirements. In the next part of my thesis there is basic description of Cisco Unified Communications Manager technology. Another part of my thesis speaks about security threats which can attack on VoIP network, specifically DoS attacks, evansdroping, Man-in-the-Middle attack, voice SPAM and others and some recommendations how to mitigate vulnerabilities of VoIP networks. In the last part are used findings from the study of previous sections and offers propostal of solution to corporate VoIP phone structure.

Keywords: security, VoIP, IP Telephony, Cisco Unified Communications Manager

BIBLIOGRAPHY

1. WALLACE, K. *Cisco VoIP.* Computer Press, Brno, Czech Republic, 2009.
2. FINKE, J. - HARTMANN, D. *Implementing Cisco Unified Communications Manager.* Part 1, Part 2, Cisco Press, Indianapolis, 2012.
3. CIOARA, J. D. *Authorized Self-Study Guide Cisco IP Telephony (CIPT).* Cisco Press, Indianapolis, 2006.

IMPLEMENTING A CRYPTO DEVICE

Péter SZEGEDI

Consultant: Lieutenant Colonel Dr. Lajos Muha, Associate professor

National University of Public Service, Hungary, 1083 Budapest, Ludovika tér 2.,peter.szegedi92@gmail.com

Abstract: My thesis focuses on the field of cryptography, both in theory and in practice. Firstly I explain the relevance of information security nowadays, and the necessity of it. I proceed by explaining the cryptography's part in the information security field. I specially explain RSA, a cryptographic algorithm, which will be implemented later on. On the second part of my thesis, I focus on a practical way to create a cryptographic system. I explain the device I chose to implement on, the Raspberry Pi, its operating system the Raspbian. I proceed with networking and a socket communication knowledge, required for the system build up. I focus on the programming language used as well, the Python, and the way it implements crypto. Finally I point out the major point in my script required for the secure communication. I end the thesis with a conclusion, including my results, possible uses, and future research plans.

Keywords: cryptography, RSA, raspberry Pi, python, network

BIBLIOGRAPHY

1. VÁNYA, L. *Cyber Warfare - valóban korszerű kihívás a haderőkkel szemben*. Kommunikáció 2004. ZMNE, Budapest, 2004.
2. BUTTYÁN, L. - VAJDA, I. *Kriptográfia és alkalmazásai*. Typotex, 2004.
3. BRUEN, A. A. - FORCINITO, M. A. *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century.* John Wiley & Sons, 2011.
4. DIFFIE, W. - HELLMAN, M. E. *New directions in cryptography*, IEEE Transactions on information theory, vol. it-22 no. 6.
5. PAAR, C. - PELZL, J. *Understanding Cryptography*. A Textbook for Students and Practitioners (11. fejezet: "11: Hash Functions"), Springer, 2011.
6. MASON, S. *Electronic Signatures in Law 3rd edition*. Cambridge University Press, 2012.

METHODS OF DETECTING MALWARE AND EXPLOITS IN JAVA CODE

Radovan ŠTELBASKÝ

Consultant: Cpt. Eng. Michal Vangorík

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: This paper characterizes methods used in systems to detect and analyze malicious code and it describes the current security status of Defense Department's data network. The thesis is systematically divided into five chapters. The first chapter discusses the options in malicious code detection, including detection, prevention and protection systems. It describes the phases of forensic analysis and methods of static and dynamic analysis. The second chapter characterizes obfuscation. The third chapter describes encryption of Java code. The fourth chapter shows practical difficulties when analyzing Java code. The fifth chapter describes the current security status of Defense Department's data network and it presents a set of actions to increase the security of endpoint devices.

The main aim of the research is to describe the importance of each system and method used in malicious code detection and to show the necessity of securing each system against potential dangers.

Keywords: malware, Java, antivirus, obfuscating Java Code, forensic Analysis

BIBLIOGRAPHY

1. TEICHMANN, Radek. VsadNaJavu.cz. *ProGuard - obfuskace kódu v praxi.* [Online] MoroSystems, 22. August 2011. [Dátum: 2. December 2014.] Dostupné na internete: http://vsadnajavu.cz/2011-08/java-j2ee/proguard-obfuskace-kodu-v-praxi/.

2. SZOR, Peter. *Počítačové viry, analýza útoku a obrana.* Brno : Zoner Pres, 2006. ISBN 80-86815-04-8.

3. PROVOS, NIELS. HONEYD. *Developments of the Honeyd Virtual Honeypot.* [Online] 16. Júl 2008. [Dátum: 12. December 2014.] Available on the Internet: http://www.honeyd.org/index.php.

4. LEVICKÝ, Dušan. *Kryptografia v komunikačnej bezpečnosti.* Košice : Elfa s.r.o., 2014. ISBN 978-80-8086-235-0.

5. POPA, Marius. *Journal of Mobile, Embedded and Distributed Systems - JMEDS. Techniques of Program Code Obfuscation for Secure.* [Online] 2011. [Dátum: 12. December 2014.] Available on the Internet: http://www.jmeds.eu/index.php/jmeds/article/view/Techniques-of-Program-Code-Obfuscation-for-Secure-Software/pdf.

6. LOUDA, Pavel. *IT NEWS. Nastáva koniec šifrovania cez AES?* [Online] 21. August 2011. [Dátum: 28. November 2014.] Available on the Internet: http://www.itnews.sk/spravy/bezpecnost/2011-08-21/c142645-nastava-koniec-sifrovania-cez-aes-najdene-zranitelnosti-tomu-nasvedcuju...

7. Collberg, Christian - Nagra, Jasvir. *informIT. What Is Surreptitious Software?* [Online] 11. August 2009. [Dátum: 14. Október 2014.] Available on the Internet: http://www.informit.com/articles/article.aspx?p=1380912&seqNum=4.

8. Carrier, Brian. *Open Source Digital Forensics.* [Online] 2015. [Dátum: 25. Február 2015.] Available on the Internet: http://www.sleuthkit.org/index.php.

9. Zelix KlassMaster HEAVY DUTY PROTECTION. *Java Class Obfuscator Features.* [Online] Zelix, 2015. [Dátum: 12. Január 2015.] http://www.zelix.com/klassmaster/classObfuscator.html.

10. Wireshark. [Online] 2015. [Dátum: 25. Február 2015.] https://www.wireshark.org/about.html.

11. Stack Exchange. *Weirdest obfuscated "Hallo World!".* [Online] Stack Exchange, 2. Marec 2014. [Dátum: 25. Apríl 2015.] http://codegolf.stackexchange.com/questions/22533/weirdest-obfuscated-hello-world.

12. *Snort.* [Online] Cisco, 2015. [Dátum: 12. Január 2015.] https://www.snort.org/#get-started.

13. Science Direct. *Advanced obfuscation techniques for Java bytecode.* [Online] 2. August 2002. [Dátum: 12. December 2014.] http://ir.nctu.edu.tw/bitstream/11536/26885/1/000220336900001.pdf.

14. Sandbox (computer security). [Online] 27. Február 2015. [Dátum: 15. Marec 2015.] Available on the Internet: http://en.wikipedia.org/wiki/Sandbox_(computer_security).

15. *Rootkit.* [Online] 12. Február 2015. [Dátum: 15. Február 2015.] http://en.wikipedia.org/wiki/Rootkit.

16. *Obfuscation* (software). [Online] Wikimedia Foundation, Inc., 21. Január 2015. [Dátum: 22. Január 2015.] http://en.wikipedia.org/wiki/Obfuscation_(software).

17. *Jshrink.* [Online] EASTRIDGE TECHNOLOGY, 2012. [Dátum: 20. November 2014.] Available on the Internet: http://www.e-t.com/jshrink.html.

18. ITnetwork.cz. *Programujeme jednoduchou hru v Javě: Logik.* [Online] ITnetwork. [Dátum: 25. Apríl 2015.] Available on the Internet: http://www.itnetwork.cz/tutorial-java-hra-logik.

19. Independent Test of Anti-Virus Software. *File Detection Test of Malicious Software.* [Online] 22. Apríl 2014. [Dátum: 25. Apríl 2014.] Available on the Internet: http://www.av-comparatives.org/wp-content/uploads/2014/04/avc_fdt_201403_en.pdf.

20. ESET Endpoint Riešenia. *Vlastnosti z pohľadu IT špecialistu.* [Online] ESET. [Dátum: 8. Máj 2015.] Available on the Internet: http://static1.esetstatic.com/fileadmin/Images/SK/Docs/Datasheet/ESET-Endpoint-IT-perspektiva.pdf.

21. *Cyber Security Products.* [Online] NiKSUN, 2015. [Dátum: 12. Február 2015.] Available on the Internet: https://www.niksun.com/product.php?id=33.

22. *Cuckoo Sandbox.* [Online] 2014. [Dátum: 22. November 2014.] Available on the Internet: http://docs.cuckoosandbox.org/en/latest/introduction/what/.

23. *Computer Security.* [Online] August 2006. [Dátum: 22. November 2014.] Available on the Internet: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

SPLUNK AND ITS UTILIZATION IN ARMED FORCES

Ján VASIL

Consultant: Assoc. Prof. RNDr. Ľubomír Dedera, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Department of Informatics,
Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: In our paper we were focused on fastly growing section of informational security and its importance in Armed forces. We started with theoretical definition of terms commonly used in our paper as big data and log management and we tried to show the growing importance of this section in environment of the Armed forces. Then we described introducing into Splunk, which is software we used, and its interface and explained principle of its work. In the end we tried to find the way in which we could use this software in Armed forces and we tried to suggest possible implementation in order to improve relations between armed forces and informational security.

Keywords: splunk, big data, log management, armed forces

BIBLIOGRAPHY

1. ZADROZNY, P. - KODALI, R.: *Big Data Analytics Using Splunk: Deriving Operational Intelligence from Social Media, Machine Data, Existing Data Warehouses, and Other Real-Time Streaming Sources*. Apress, 2013.
2. BUMGARTNER,V.: *Implementing Splunk: Big Data Reporting and Development for Operational Intelligence.* Packt Publishing, 2013.

SECTION
MANAGEMENT, ECONOMICS
AND LOGISTICS

THE ANALYSIS OF LEVEL OF FINANCIAL LITERACY OF PROFESSIONAL SOLDIERS OF THE ARMED FORCES OF THE SLOVAK REPUBLIC AND THE OPTION OF POSSIBLE OF INCREASING THE FINANCIAL LITERACY

Nikola BEZOUŠKOVÁ

Consultant: Eng. Soňa Jirásková, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: Nowadays, the society requires from people much more than just the general literacy, such as reading, counting and writing. Unfortunately, money plays a central role in the world today. If people do not want to be the slaves to money, it is necessary for them to understand and know how to handle money and not to let money to control people. There is the place for financial literacy. (And that is the reason why financial literacy should be taken into consideration in these days.)

The aim of the financial literacy is the ability to take care of the finances in order to be able to provide good conditions for themselves and relatives. The financial literacy mainly focuses on people and their ability to orientate in the sphere of money, to differ between the financial products, to provide enough money for themselves in the retirement age, to know how to make right financial decisions, to choose the most advantageous offer, to avoid the problems in the financial sector and to be prepared for unexpected situations which could cause their own bankruptcy.

Researches of financial literacy of the population of the Slovak Republic (from the years 2007, 2011 and 2012) show that the level as well as the index of financial literacy of the Slovaks have very low rates. We analysed the current level of financial literacy of professional soldiers of The Armed Forces of the Slovak Republic and compared it with the level of financial literacy of population of the Slovak Republic which was measured by Slovak Banking Association. The work points out to professional soldiers´ weaknesses in the field of finance and shows their consumption patterns and financial behaviour that are compared to the results obtained from the surveys of the Foundation Partners and of the financial institution ING.

At the end of the survey we tried to ascertain the interest of professional soldiers in financial education and the ways they would like to learn. From the analysis of the results obtained from the survey, we suggested possible solutions to improve the financial literacy of professional soldiers in the Armed Forces.

Keywords: literacy, financial literacy, professional soldiers, level of financial literacy, increasing the financial literacy, The Armed Forces of the Slovak Republic

BIBLIOGRAPHY

1. BELEŠOVÁ, M. 2013. *Relative literacy in society*. UIPS, Bratislava, Slovak Republic, 2013. 60 p., ISSN 1335-5864.
2. KOVALČÍKOVÁ, Z. – SMOROŇ, L. – STRENK, R. 2011. *Basic of financial literacy*. MPC, Bratislava, Slovak Republic, 2011. 68 p., ISBN 978-80-8052-375-6.
3. KYIOSAKI, R. T. 2008. Increase your financial IQ. In *MOTÝĽ: financial magazine*. Bratislava, Slovak Republic, 2008, ISBN 978-80-89199-88-4.

4. *National standard of financial literacy version 1.* 2014.

5. SZOVICS, P. 2012. *Quo vadis financial literacy?* In *BIATEC: specialist bank´s magazine*. Bratislava, Slovak Republic, 2011, NBS, ISSN 1335-0900.

Presentations:

1. SLOVAK BANK ASSOCIACION, *Financial literacy in Slovakia – 2007*. In*tlacovespravy.files.wordpress.com* [online]. 2007. Available on the Internet: http://www.viacakopeniaze.sk/files/vapucebnica/finacnagramotnost-prieskum-2007.pdf>

2. PARTRERS GROUP NADATION. *More than third Slovaks have low level of financial literacy*. In *Partnersgroup.sk* [online]. 2012. Available on the Internet: https://www.partnersgroup.sk/viac-ako-tretina-slovakov-ma-nizku-financnu-gramotnost

3. MRÁZOVÁ, R. *Financial education, how Slovaks care about their finance?* In *tlacovespravy.files.wordpress.com* [online]. 2011. Available on the Internet: http://www.viacakopeniaze.sk/files/vapucebnica/finacnagramotnost-prieskum-2007.pdf>

FUNDING OF DEFENCE OF SLOVAK REPUBLIC

Tatiana FALISOVÁ

Consultant: Eng. Viera Frianová, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The present paper deals with the issue of funding of defence. It discusses defence, state security and armed forces, which are generated in order to perform tasks of defence. The first part is focused on the economy of defence, defence spending, their classification and analysis in the period from the year 2002 before Slovak republic became the member of the North Atlantic Treaty Organization, to the present. The second part includes information about funding of defence in accordance with the state budget and the budget of the Ministry of Defence of the Slovak Republic. This part also consists of allocate efficiency defence funding in terms of the Model 2010 of Armed forces of Slovakia and Long-Term Development Plan - Model 2015 and also indicators of technical efficiency. The final part deals with new ideas of funding defence and with comparing funding of defence of the world leading countries.

Keywords: defence, security, military, defence economics, defence spending, defence funding, the state budget, the budget of the Ministry of Defence, the allocate efficiency of defence funding, technical efficiency defence funding, new ideas of funding defence.

BIBLIOGRAPHY

1. BENČ, V. 2003. *Ekonomické aspekty členstva v NATO.* Prešov : Vydavateľstvo Rokus, 2003. 95 s. ISBN 80-89055-36-2.
2. BEŇOVÁ, E. - NEUBAUEROVÁ, E. 2007. *Ekonomika verejného sektora.* Bratislava : MERKURY spol. s r.o., 2007. 144 s. ISBN 978-80-89143-48-1.
3. BIELA KNIHA O OBRANE SLOVENSKEJ REPUBLIKY. 2013 [online]. [cit. 2015-03-20]. Dostupné na internete: <http://web1.mod.gov.sk/ine/BKO/dokumenty/BKO2013_plne_rozlisenie.pdf>.
4. IVANČÍK, R. 2012. *Alokačná a technická efektívnosť financovania obrany v Slovenskej republike.* Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika, 2012. 144. s. ISBN 978-80-8040-444-4.
5. IVANČÍK, R. - KELEMEN, M. 2010. *Obrana štátu: ekonomika, plánovanie a financovanie obrany.* Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika, 2010. ISBN 978-80-8040-410-9.
6. IVANČÍK, R. - NEČAS, P. Obranné výdavky Ozbrojených síl SR v rámci modelov 2010 a 2015 – plány a realita. In *Politické vedy* [online]. 2011, roč. 14, č. 1. Dostupné na internete: <http://www.fpvmv.umb.sk/userfiles/file/1_2011/IVANCIK_NECAS.pdf.>
7. NEČAS, P. - IVANČÍK, R. 2011. *Globalizácia, obrana a bezpečnosť.* Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2011. 190 s. ISBN 978-80-8040-425-3.
8. ŠEVČÍK, V. 1999. *Ekonomika a obrana štátu*. Praha, AVIS, 1999.

CURRENT ROLE OF SERVICES IN LOGISTICS AF SR

Natália MIŠEKOVÁ

Consultant: Assoc. Prof. Eng. Miroslav Školník, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The work deals with the task of logistics services in the context of the reorganization and transformation of Logistics of the Armed Forces. The initial analysis of the place, role and importance of logistics maintenance services in the Armed Forces. Further addressed the status of logistics services in AF SR is currently focusing on service provisioning. Based on the analysis, and past experience suggests solutions and take concrete actions for the future. The aim of this work is to propose a solution to the problems of logistics services in AF SR with emphasis on provisioning service in the context of their transformation and adaptation to the current situation at the moment.

Keywords: logistics OS SR, logistics services, food services, optimization of logistic services in the Armed Forces

BIBLIOGRAPHY

1. ŠKOLNÍK, M. - MORONG, S. *Vojenská logistika. Základy vojenskej logistiky a materiálového manažmentu.* Vysokoškolská učebnica. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2013. 198 s. ISBN 978-80-8040-485-7.
2. JIRÁSKOVÁ, S. - ŠKOLNÍK, M. *Outsourcing v Ozbrojených silách Slovenskej republiky.* Vedecká monografia, 1. vyd. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2011. - 150 s. ISBN 978-80-8040-424-6.
3. *MO SR. Logistická doktrína OS SR. Doktrína OS SR sign. SVD 40*. Bratislava 2010.

THE ECONOMIC ASPECTS OF QUALITY OF LIFE OF PROFESSIONAL SOLDIERS

Daniela MLYNÁROVÁ

Consultant: Eng. Viera Frianová, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: Comprehensive social security, family and lifestyle of professional soldiers of the Armed Forces of the Slovak Republic are factors that significantly determine his quality of life. The starting points for the issue of social security are the rules that govern the civil service and directly affect the quality of life of professional soldiers. Existing research on issues of quality of life indicate that the quality of life of professional soldiers is tracking and monitoring mainly focused on the sociological area. But just social security is still a major attraction for entry into the armed forces. Many times these expectations are met, but in practice we witness the opposite outcome. That is why the aim of this paper to analyse the area of quality of life in economic terms on the basis of the survey and look at the field of social security through the eyes of professional soldiers.

Keywords: the quality of life of professional soldiers, social security, survey

BIBLIOGRAPHY

1. ÁRENDÁŠ, M. *Makroekonómia I.* Nitra, 2007. 273 s. ISBN 978-80-8069-914-7.
2. LISÝ, J. – kolektív. *Ekonómia –všeobecná ekonomická teória* . Banská Bystrica : Iura edition, 1998. 507 s. ISBN 80-88715-81-4.
3. *Slovensko-poľský zborník štúdií a článkov „Kvalita života v kontextoch globalizácie a výkonovej spoločnosti“.* Filozofická fakulta Prešovskej univerzity v Prešove, 2002, ISBN 80-8068-087-6.
4. HERMANOVÁ, E. *Koncepty, teórie a meraníkvality života*. Praha : Sociologické nakladateľstvo, 2012, ISBN 978-80-7419-106-0.
5. SOJKA, L. *Kvalita pracovného života a súvisiace konštrukty.* Prešov : Fakulta manažmentu Prešovskej univerzity, 2007. 150 s. ISBN 978-80-8068-652-9.
6. MARTEL, J. – DUPUIS, G. *Quality of Work Life: Theoretical and Methodological Problems, and Presenatation of New Model and Measuring Instrument.* Social Indicators Research, 2006, 368 s. ISBN 1573-0921.
7. *Zborník anotácií a elektronických verzií príspevkov z medzinárodnej vedeckej konferencie „Životný štýl a rodina vojenského profesionála*“. Liptovský Mikuláš : Katedra humanitných vied a jazykov AOS, 2007, ISBN: 978-80-8040-328-7.

POLISH SEA PORTS AND MACROECONOMIC INTERDEPENDENCE AND COOPERATION THE ECONOMIES OF V4 GROUP

Lucyna SZACIŁŁO

Consultant: Jacek Kurowski, Ph.D., MA Paweł Krekora

The National Defence University, Warsaw, Poland

Abstract: The paper will present the current situation of Visegrád Group's energetic systems. It will also present the economic priorities of the current Slovakian presidency in 2014-2015 and its connections with the development opportunities of the use of Polish sea ports in Poland. In particular, the role of the ports of Gdańsk, Gdynia and Szczecin-Świnoujście will be stressed. The paper will discuss the strategic location of Poland, which is a great advantage thanks to which sea ports can become the base for goods transported inside the Visegrád Group. The changes observed in sea ports will be shown: the investments connected with new road and railway connections, the modernisation and the simplification of customs procedures. The paper will also outline the perspective of the development of the river Oder as the waterway connecting the south with the ports of Szczecin and Świnoujście.

Keywords: energetic system, economic priorities of the Slovakian presidency, Polish sea ports

BIBLIOGRAPHY

1. Available on the Internet: http://www.umsl.gov.pl/pliki/politykamorska2020.pdf (13.04.2015).
2. http://www.visegradgroup.eu/documents/presidencyprograms/20142015slovak#_6.%20INFRASTRUCTURE (13.04.2015).
3. http://morzaioceany.pl/inne/archiwum/14-porty-morskie/1936-to-b%C4%99dzie-rekordowy-rok-polskich-port%C3%B3w-morskich.html (13.04.2015).
4. http://www.portgdansk.pl/about-port/general-info (13.04.2015).
5. http://www.portalmorski.pl/porty-i-logistyka/porty-terminale-polskie/36912-wielkie-inwestycje-w-porcie-gdansk (13.04.2015).
6. http://www.port.gdynia.pl/en/about-port/basic-data (13.04.2015).
7. http://tvn24bis.pl/wiadomosci-gospodarcze,71/morski-port-gdynia-wyda-na-inwestycje-ponad-737-mln-zl,398007.html (13.04.2015).
8. http://port.szczecin.pl/files/port/Port_Handbook_2013_2014.pdf (13.04.2015).
9. http://www.rynekinfrastruktury.pl/wiadomosci/porty-w-szczecinie-i-swinoujsciu-chca-lepiej-wspolpracowac-z-czechami-17634.html (13.04.2015).
10. http://www.port.szczecin.pl/pl/aktualnosci/porty-polskie-zachcaj-czeskich-partnerw-do-wsppracy (13.04.2015).

SECTION

SOCIAL SCIENCES

NATIONAL AND INTERNATIONAL SECURITY

ROLES OF RECONNAISSANCE UNITS (SQUAD, PLATOON) IN PROVISION OF FIRE SUPPORT

Alexander BOTOŠ

Consultant: Eng. Lubomír Belan, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: This work is aimed to activities of reconnaissance squads and platoons of mechnaized and artillery forces during provision of fire support. In the first chapter I characterize these units, their goals, assignment, I describe the selected spectre of tasks they fill in said roles. In the second chapter I define thier organization structure of recon units in a mechanized infantry battalion as well as in an artillery battalion of The Armed forces of the Slovak Republic. In chapter three I deal with thier equipment for these tasks – vehicles and also optical and optoelectronical devices etc., and thier capabilities. In the final part, chapter four, I describe the activities of recon units in individual kinds of operations, such as offensive, defensive, stabilizing and enabling activities.

Keywords: reconnaissance, fire support, mechanized infantry, artillery, technologies and equipment of recon units

BIBLIOGRAPHY

1. HEADQUARTERS, DEPARTMENT OF THE ARMY: *Reconnaissance and Scout Platoon FM 3-20.98.* August 2009.
2. NORTH ATLANTIC TREATY ORGANIZATION : *NATO Indirect Fire Systems Tactical AArtyP-5(A).* 2010.
3. *VELITEĽSTVO POZEMNÝCH SÍL OZBROJENÝCH SÍL SLOVENSKEJ REPUBLIKY: Prieskumná čata. Služobná pomôcka SPG-2-6/Sprav.* Trenčín 2010.
4. *VELITEĽSTVO POZEMNÝCH SÍL OZBROJENÝCH SÍL SLOVENSKEJ REPUBLIKY: Spravodajstvo, prieskum a sledovanie v pozemných silách SPG-2-1/Sprav.* Trenčín 2008.
5. *UNITED STATES AIR FORCE: Targeting. Air Force Doctrine Document 2-1.9.* 8 June 2006.
6. HEGYI, R. *Současné poznatky z procesu targetingu na taktickém stupni.* Univerzita obrany Brno. March 2012.
7. BELAN, L. *Proces palebného ničenia v etapách zisťovania, napadnutia a vyhodnotenia cieľov.*
8. *NORTH ATLANTIC TREATY ORGANIZATION: NATO Glossary of abbreviations Used in NATO Documents and Publications AAP-15(2010).*
9. MAJCHÚT, I. *Delostrelecký prieskum.* (PowerPoint presentation) Katedra bezpečnosti a obrany.
10. *VELITEĽSTVO POZEMNÝCH SÍL OZBROJENÝCH SÍL SLOVENSKEJ REPUBLIKY: SPG-3-22/Del.*
11. *Artillery regulations Del-1-2, Del 6-3, Del 55-31.*

TACTICAL DEMOLITION TARGED AS PART OF BARRIER

Šimon BRIGANT

Consultant: Assoc. Prof. Eng. Peter Spilý, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš,
Slovak Republic

Abstract: The work contain short introduction to issue of obstacles construction as one of the tasks of engineer support in the area of operations. The main part is devoted to design a method for demolition of a real bridge as a tactical obstacle. The process of creating demolition plan is based on military standard Žen-2-6/s. It's dedicated to recon and creating demolition plan. When creating demolition plan, it must be considered type of object, placing charges, creating firing circuit and position of the demolition guard. The work describes composition of demolition guard. It describes different techniques when we have a lot of time and in lack of time. For demolition of different parts of construction, different variants were made based on used explosives.

Keywords: tactical demolition target, barrier, charge, demolition plan, demolition guard, firing circuit

BIBLIOGRAPHY

1. Žen-2-3 *Vojenský predpis o ženijnom prieskume a o ženijnej podpore spravodajstva*. 2012.
2. Žen-2-6 *Trhaviny a ničenie*. 1982.
3. Žen-2-7/1 *Vojenský predpis o zatarasovaní*. 2013.
4. Žen-2-9/s *Ženijné práce všetkých druhov vojsk* (Q-528).
5. Žen-2-8 Metodika výcviku malých ženijných jednotiek skupín oddielov. 2009
6. MALINA, Z. *Vojenské dopravní stavby II.* Brno : Univerzita obrany, 2007.
7. SPILÝ, P. *Trhaviny a ničenie (Zbierka príkladov)*. (Q-990). 1997.
8. SPILÝ, P. *Uzol zátarás*. Liptovský Mikuláš : Vojenská akadémia, 2000.

ANALYSIS AND EVALUATION OF TRAINING RISKS

Tatiana FALISOVÁ

Consultant: Eng. Ondrej Kredatus, Ph.D.

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: The aim of the present paper is to describe the development and definition of risk and also of the risk management. Nevertheless, the main part of this paper is about application of risk management into armed forces, which consist of identifying potential training risks, analysis and evaluation of them and also make recommendations to reduce their occurrence.

The present paper is divided into four chapters. The first part deals with the historical development of risk and risk management, the second is about the definition of risk and process of risk management, the third is focused on identifying potential training risks and also includes their risk management process. The final chapter comprises recommendations for risk reduction in training.

Keywords: risk, risk management, training risk, analysis of training risk, evaluation of training risk.

BIBLIOGRAPHY

1. REITŠPÍS, J. a kol. 2004. *Manažérstvo bezpečnostných rizík*. Žilina : Edis, 2004. 296 s. ISBN 80-8070-328-0.
2. SMEJKAL, V – RAIS, K. 2003. *Řízení rizík*. Praha : Grada Publishing, 2003. 263. SBN 80-247-0198-7. Knižnica AOS ZF 28218.
3. STN 01 0380: 2003: *Manažérstvo rizika.*
4. STN ISO 31000: 2011: *Manažérstvo rizika. Zásady a návod.*
5. ŠIMÁK, L. 2006. *Manažment rizík*. [online]. Žilina : Fakulta špeciálneho inžinierstva Žilinskej univerzity, 2006. 116 s. [cit.25.11.2014] Dostupné na internete: http://fsi.uniza.sk/kkm/old/publikacie/mn_rizik.pdf>
6. VARCHOLOVÁ, T. – DUBOVICKÁ, L. 2008. *Nový manažment rizika*. Bratislava : Ekonómia, 2008. 196 s. ISBN 978-80-8078-191-0.

ACTIVITY ANALYSIS OF CROWD IN CIVIL RIOTS

Jakub MURČEK

Consultant: Npor. Eng. Michal Hrnčiar

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: Life today is far from simple. Every day we hear of natural disasters, technically unstable conveniences of today, the economic problems, life-threatening terrorist attacks, riots that shook the world.

The discontent of the population on Earth is getting greater and greater. People complain about the wrong decisions of the governing bodies, the financial problems with which no one helps them, the social inequality between equals and the many other problems which are creating every day. Dissatisfaction is often so great that it degenerate into civil riots.

Civil riots are activities of dissatisfied groupings of the population which wants some changes. Civil rights allow residents to congregate, that mean to create civil groups- crowds.

Crowds can be a tremendous force which depends on the size and the will of the people by attempting to change. In military operations groupings of the population which are unheard and ineffective from the beginning often grows into civil riots where can go even for a life.

Where incites violence, destroying property, where is bloodshed ther is need of the intervention of forces. Police forces are in most cases insufficient to repel riot, so to stabilize them there is need to add protection of military forces.

Military forces have a protective role in the stabilization activities like crowd control, thus controlling and eliminating residents who are involved in civil riots. Activities of crowd in civil riots has long query and quite problematic issue in solution of stabilization activities. Military protection forces must be prepared to face the armed crowd and therefore it tactically trained. Psychological aspects are also key point to understand the crowd, searching for crowd leaders and their elimination. The crowd is often uncontrolled and it is difficult for military protection force to stop civil riots which are accompanied by violence on innocent bystanders, property and also on military and police forces. Crowd on violence used many resources to intensify the damage.

Failure in analyzing the activity of the crowd when civil riot may lead to a disaster of unprecedented proportions. Stabilizing activities in which military forces are involved, must therefore be properly oriented in this issue, and must be able to act effectively against it because it appears at the world more and more.

Keywords: operations, riots, crowd, residents, military forces, protection, violence

BIBLIOGRAPHY

1. *VDG-30-01-01/Oper. Postupy a spôsoby vykonávania stabilizačných aktivít*. 23. august 2010.
2. *FM 3-19.15. Civil disturbance operations*. 18. apríl 2005.

THE ANALYSIS OF THE ROLES OF THE SLOVAK REPUBLIC ARMED FORCES IN THE SOLUTION OF CRISIS SITUATIONS IN THE SLOVAK REPUBLIC

Jakub SASARÁK

Consultant: Prof. Eng. Vojtech Jurčák, CSc.

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: A paper deals with role of the Slovak republic armed forces in domestic crisis management. Aim of a paper is to conduct an analysis of the roles of the Slovak republic armed forces in the solution of crisis situations in Slovak republic. The study is divided into three main parts. In first part a paper outlines roles of the Slovak armed forces according to law 319/2002 about the Slovak republic defence. In this part of a paper every single task of the Slovak republic armed forces is briefly analyzed. In the second part, paper deals with analysis of the deployment of the Slovak republic armed forces in assistance operations to domestic crisis management. Analysis is conducted in timeframe of last three years, from 2012 to 2014. Slovak republic armed forces deploy troops to domestic crisis management operations independently or with cooperation with Slovak police force or Fire and rescue brigade. Analysis is conducted from three points of view. Firstly it analyzes types of tasks conducted by Slovak republic armed forces. Secondly it analyzes types of operations to which Slovak republic armed forces were deployed. Thirdly it analyzes types and frequency of use of military vehicles. The third part of the paper deals with military training. There is conducted analysis of the military training of Slovak armed forces for tasks following from domestic crisis management. A military training is performed in two ways. As cooperative training with the Slovak police force, the Fire and rescue brigade or other organizations. Second way the military training is performed is independently as military training of soldiers. In the conclusion a paper compares training with a deployment in recent three years and proves if the military personnel were trained for crisis situations in which they were deployed.

Keywords: Slovak armed forces, crisis situations, domestic crisis management, military training

BIBLIOGRAPHY

1. HALAJ, J. 2013. *Plánovanie a použitie ozbrojených síl Slovenskej republiky v kontexte domáceho krízového manažmentu:* [Záverečná práca]. Akadémia ozbrojených síl v Liptovskom Mikuláši. Vyšší veliteľsko-štábny kurz Centra vzdelávania. Vedúci záverečnej práce: plk. Ing. Ľubomír KUBEK. Liptovský Mikuláš : AOS, 2013. 39 s.
2. ANDRASSY, V. – GREGA, M. 2013. *Didaktické postupy riešenia úloh v oblasti krízového manažmentu*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2013. 141 s. ISBN 978-80-8040-484-0.
3. ŠIMÁK, L. 2004. *Krízový manažment vo verejnej správe*. Žilina : FŠI ŽU, 2004. ISBN 80-88829-13-5.
4. ŠIMÁK, L. a kol. 2005. *Terminologický slovník krízového riadenia*. Žilina : FŠI ŽU, 2005. ISBN 80-88829-75-5.

5. *Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.*
6. *Zákon č. 129/2002 Z. z. o integrovanom záchrannom systéme.*
7. *Zákon č. 171/1993 Z. z. o Policajnom zbore.*
8. *Zákon č. 315/2001 Z. z. o Hasičskom a záchrannom zbore.*
9. *Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky.*
10. *Zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu.*
11. *Zákon č. 42/1994 Z. z. o civilnej ochrane obyvateľstva.*

NON-LINEAR WARFARE

Gergő SZABÓ

National University of Public Service, Faculty of Military Sciences and Officer Training
Hungary, 1083, Budapest Ludovika tér 2.

Abstract: This paper deals with the Crimean crisis, especially focusing on the new type of warfare, which the Russian soldiers executed during their operations. This type of warfare, some call it non-linear, hybrid or asymmetric, has to be examined properly, since it emerged as a new threat, besides the failed states and terrorism, on which we have been focusing in the last decade.

The non-linear war and its usage during the crisis in Ukraine has to be considered as a sinister sign to all Middle-European and Baltic countries, in short, the post-soviet region of Europe. The Russian government's and Putin's communication usually deals with the resurrection of the glorious pan Slavic empire, or the creation of the Eurasian Union, with Russian leadership of course. This has to implicate the reviews of the individual countries national security policies and The Washington Treaty.

However there is another side of the coin. We have to consider how, when and where the NATO can use these procedures during our peacekeeping missions, or during an offensive campaign. Although this topic is huge, during this paper I will show the characteristics of this new type of warfare, which may give food for thought for future evaluations.

Keywords: asymmetric warfare, non-linear war, hybrid war, Crimea, Ukraine, Russia

BIBLIOGRAPHY

1. BERZINS, J. (2014. 10 22). *National Defense Academy of Latvia.* Forrás : National Defense Academy of Latvia: Available on the Internet: http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx
2. BOGDANOV, T.&. (2014. 11 02). *Times of Change*. Forrás : A total absence of effort: Available on the Internet: http://www.thetoc.gr/eng/opinion/article/a-total-absence-of-effort
3. GALEOTTI, M. (2015). *'Hybrid War' and 'Little Green Men': How it works and how it doesn't.* Bristol, United Kingdowm.
4. GERASIMOV, V. (2014. 11 02). *Moscow's Shadow*. Forrás : Russian non linear war: Available on the Internet: http://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/
5. NATO Strategic Communication Centre of Excellence. (2014. 10 13). *NATO Strategic Communication Centre.* Forrás: NATO StratComm COE: Available on the Internet: https://nllp.jallc.nato.int/IKS/Sharing%20Public/NATO%20StratCom%20COE%20Research%20on%20Information%20Campaign%20against%20Ukraine.pdf
6. PUTIN, V. (2014. 10 24). *President of Russia*. Forrás : Kreml Archive: Available on the Internet: http://archive.kremlin.ru/eng/speeches/2005/04/25/2031_type70029type82912_87086.shtml
7. Russian Government. (2014. 10 15). *Russia's National Security Strategy to 2020.* Forrás : Russia's National Security Strategy to 2020: Available on the Internet: http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020

8. SUTYAGIN, I. (2015. March). *Russian Forces in Ukraine.* London, United Kingdom.
9. *The Ministry of Foreign Affairs of the Russian Federation.* (2014. 10 20). MFA of Russia. Forrás : MFA of Russia: Available on the Internet: http://www.mid.ru/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/89a30b3a6b65b4f2c32572d700292f74?OpenDocument

IRAN AND ITS INFLUENCE ON SECURITY ENVIROMENT IN THE MIDDLE EAST

Alena ŠVORČÍKOVÁ

Consultant: Prof. Eng. Vojtech Jurčák, CSc.

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Abstract: This thesis carries out an analysis of Iranian role as regional player in the Middle East and its relationships with selected states in the region of the Middle East.

This thesis is divided into 8 chapters. The first chapter is focused on Iranian relations with Iraq. The second chapter is concentrating on analyze of Iranian relations and interests in Saudi Arabic, the third one describes relations between Iran and Lebanon.

The fourth chapter analyzes Iranian relations in Gulf monarchies. The fifth one carries out and analysis of Iranian relations and interests in Syria, the sixth chapter considers on relations between Iran Turkey and the seventh on analyze of complicated relations between Iran and Israel. The last one analyse an impact of nuclear programme on Iranian relations with the countries of the Middle East region.

Keywords: Iran, Israel, Middle East, Iranian nuclear program, Saudi Arabic, Gulf monarchies, Syria, Lebanon, Turkey, Iraq

BIBLIOGRAPHY

1. BAER, Robert. *Jak naložit s ďáblem*, Praha : Volvox Globator 2010. 317s. ISBN 978-80-7202-755-7.
2. BOUCHAL, Martin, eds. Irák. In *Současný Blízky východ*, Brno : Barrister Principal 2011, s. 154. ISBN 978-80-87474-45-7.
3. BURGROVÁ, Helena, eds. Státy Zálivu. In: *Současný Blízky východ*, Brno : Barrister Principal 2011, s. 188-201. ISBN 978-80-87474-45-7.
4. EICHLER, Jan - LAML, Roman. *Bezpečnostná politika v dobe globalizácie*. Skalica : Stredoeurópska vysoká škola v Skalici, 2010, 176 s. ISBN 978-80-89391-14-1.
5. EICHLER, Jan. *Mezinárodní bezpečnost na počátku 21. století*. Praha : AVIS 2006, 303s. ISBN 80-7278-326-2.
6. JEŽOVÁ, Michaela, eds. Izrael a Palestinská autonomní správa. In *Současný Blízky východ*. Brno : Barrister Principal 2011, 118-133s. ISBN 978-80-87474-45-7.
7. MACHÁČEK, Štěpán. *Írán a arabští šíité*. 2008, 20 s.
8. ŠABACKÁ, Yvona. *Konflikt a politika velmocí na Blízkém východě. Libanon-bitevní pole velmocí.* Plzeň : Aleš Čeněk, 2011. 409 s. ISBN 978-80-7380-298-1.
9. TOMKOVÁ, Alena, eds. *Současný Blízky východ*. Brno : Barrister Principal 2011, s. 162-174. ISBN 978-80-87474-45-7.
10. VEJRYCH, Jaromír, eds. Saúdská Arábie. In *Současný Blízky východ*. Brno : Barrister Principal 2011, s. 177-179. ISBN 978-80-87474-45-7.

11. CILEČKOVÁ, Jitka. *Íránská zahraniční politika vůči Spojeným státům americkým za prezidentú Chatámího a Ahmadínežáda*. Brno : Bakalárska práca: Masarykova univerzita, 2010, 36 s.
12. CHENG QIU. *Mocenské ambice Íránu a jeho nukleární program*. Plzeň : Bakalárska práca: Západočeská univerzita v Plzni, 2012, 49 s.
13. KARTALOVÁ, Petra. *Irán a Saudská Arábia ako regionálne mocnosti na Blízkom východe*. Praha : Diplomová práca: Univerzita Karlova v Praze, 2013, 93 s.
14. KOVAŘÍK, Michal. *Postupy odradenia potenciálne jadrového Iránu*. Brno : Magisterská záverečná práca: Masarykova univerzita, 2012, 93 s.
15. ROLEČEK, Ondřej. *Íránský jadrový program jako bezpečnostní dilema*. Praha : Bakalárska práca: Vysoká škola ekonomická, 2014, 33 s.
16. ŠVORČÍKOVÁ, Alena. *Príčiny vzniku súčasných nepokojov v Líbyi a Sýrii.* Skalica : Bakalárska práca: Stredoeurópska vysoká škola v Skalici, 2012, 57 s.

REBEL WAR - A NEW GOD OF THE 21ST CENTURY

Przemysław ZERA

Consultant: Marzena Żakowska, MA

National Defence University, Poland, 00-910 Warsaw, al. Gen. A. Chruściela 103

Abstract: The pace of technological progress and changes in the international environment after the 2nd World War caused the necessity of developing new methods of warfare and strategic actions. Apart from Liddell Hart's theory of the indirect approach, Beaufre's theory of deterrence and Brodie's nuclear strategy, there is also a rebel war concept elaborated by Evgeny Messner. This concept hasn't been widely known until now, but it's constantly gaining importance. The aim of this article is to present the main assumptions of rebel wars and to identify their basic means of combat and defense. Moreover, the author attempts to create a model of a new commanding-headquarters institution in the state structures that would meet the requirements of speed and elasticity of actions in the rebel wars.

In view of the above, the author tries to find an answer to the following questions:

1. What are the main assumptions of the rebel war theory?
2. What means of attack and defense can be identified on the basis of the conflict in Eastern Ukraine?

Furthermore, the article shows the likely evolution of rebel wars in the 21st century.

Keywords: security, war, Messner, Ukraine, Russia, separatism

BIBLIOGRAPHY

1. KRAJ, K. Wojny asymetryczne czy miatieżewojna Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku. In *Bezpieczeństwo. Teoria i praktyka*, K. Budzowski (ed.), Cracow 2012, vol. 3, p. 33-41. ISSN 1899-6264.
2. SAWA-CZAJKA, E. Rebel-war in Ukraine. In *Confrontation and Cooperation: 1000 Years of Polish-German-Russian Relations*.
   Available on the Internet:
   http://www.degruyter.com/view/j/conc.2014.1.issue-1/conc-2014-0004/conc-2014-0004.xml, access: 16.04.2015.
3. SYKULSKI, Ł. Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera. In *Przegląd Geopolityczny*, 2015, vol.11, p. 103-113. ISSN 2080-8836.
4. SYKULSKI, Ł. Wojny buntownicze – wprowadzenie do koncepcji Jewgienija Messnera. Część I. In *Geopolityka*, [06.10.2014]. Available on the Internet: http://geopolityka.net/leszek-sykulski-wojny-buntownicze-cz-1/, access: 15.04.2015.
5. TRYBULSKI, Ł. Pomoc za reformy. Ukraina dostanie 17 mld dolarów kredytu od MFW. In *NaTemat*. Available on the Internet:
   http://natemat.pl/100615,pomoc-za-reformy-ukraina-dostanie-17-mld-euro-kredytu-od-mfw, access: 20.04.2015.
6. WIĘCŁAWSKI J. Russians in Latvia - the problem of status and civic rights of Russian inhabitants of Latvia.In *Forum Politologiczne*. Available on the Internet:

http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-1cca23ed-0b3f-4ec9-99ac-70e4a360ff6d/c/05-08.pdf, 22.04.2015.

7. *The EU and Russia: before and beyond the crisis in Ukraine*.
   Published by the Authority of the House of Lords (Great Britain),
   http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/115/115.pdf, 17.04.205
8. Available on the Internet:
   http://in.rbth.com/articles/2011/02/07/post-terrorism_syndrome_12133.html, 15.04.2015
9. *Ukraine crisis: Timeline,* Available on the Internet:
   http://www.bbc.com/news/world-middle-east-26248275, 20.04.2015
10. *'Maidan snipers trained in Poland': Polish MP alleges special op in Ukraine to provoke riot*.
    Available on the Internet:
    http://rt.com/news/251961-ukraine-maidan-snipers-poland/, 23.04.2015
11. '*Ukrainian neo-Nazis switch from theory to practice' – Russian diplomat.*
    Available on the Internet:
    http://rt.com/politics/252317-ukraine-nazi-dolgov-russia/, 23.04.2015
12. *Poroszenko w niemieckiej prasie: Rosja wspiera separatystów.* Available on the Internet: http://www.tvn24.pl/wiadomosci-ze-swiata,2/poroszenko-w-niemieckiej-prasie-rosja-wspiera-separatystow,426477.html, 17.04.2015
13. Available on the Internet:
    https://www.msw.gov.pl/ftp/OCK/dokumenty_Prawo_MPH/1907_18_X_III_konwencja_haska.pdf, 19.04.2015
14. *Secretary General: Situation in Ukraine is critical, NATO supports peace effor.* Available on the Internet:
    http://www.nato.int/cps/en/natohq/news_117319.htm, 18.04.2015

Sponsors „Students´ Scientific Conference 2015 – V4 GROUP“

SLOVAK ELEKTROTECHNICAL SOCIETY, Liptovský Mikuláš, Slovak Republic

Slovak Electro-technical Society is voluntary, independent, non-political and social organization, which stands behind and develops interests of individuals and groups including all the areas of electrical engineering. This support concerns education, consulting activities, the gathering and exchange of information in the field of electrical engineering.

Town Liptovský Mikuláš

Sponsors thank you for their support!

THE ARMED FORCES ACADEMY

of General Milan Rastislav Štefánik
Liptovský Mikuláš, Slovak Republic

ABSTRACTS

„Students´ Scientific Conference 2015 – V4 GROUP“
26th MAY 2015

Issued by: The Armed Forces Academy of General Milan Rastislav Štefánik,
Liptovský Mikuláš, Slovak Republic

Number of pages: 59
Number of copies: 50

ISBN 978-80-8040-507-6